POL00401626

Post Office Risk and Compliance Committee Agenda

Date
13 March 2018

Start Time	Finish Time
13.00 hours	16.00 hours

Location
1.19 Wakefield, Finsbury Dials

Present	In Attendance		Apologies
Jane MacLeod (Chair)	Johann Appel	Richard Williams (5.1)	Debbie Smith
Paula Vennells	Jonathan Hill	Deana Herley (5.1)	
Al Cameron	Michael Passmore (3 & 4.1)	Ashish Singh (5.2)	
Mark Davies	Jenny Ellwood (4.3)	Barbara Brannon (8.1)	
Rob Houghton	Sally Smith (4.4, 4.4.1 & 5.2)	Clare D'Netto (7.1)	
Martin Kirke	Keith Maple (4.4 & 4.4.1)	Nicholas Spicer (7.2)	
Owen Woodley	Mick Ebsworth (4.6 & 9.3)	Mark Dixon (9.1)	
Tom Moran (On behalf of DS)	Jules Harris (4.6, 7.2 & 9.2)	Mick Mitchell (9.3 & 9.4)	
Sarah Koniarski (Secretary)	Ian Holloway (5.1)	Tim Armit (10.1 & 10.2)	

Agenda Item	Action Needed	For ARC	Purpose	Lead	Time
1. Welcome and Conflicts of Interest			Members to declare any conflicts of interest.	Chair	13.00 – 13.05 (5 minutes)
2. Minutes and Action Lists	Approval		To approve the minutes of the meeting held on 18th January and update on actions.	Chair	
3. Internal and External Audit Procurement Plan	Questions & Noting	✓	Verbal update on the plan for procuring internal and external audit services.	Michael Passmore / Johann Appel	13.05 – 13.10 (5 minutes)
4. Key Operational Risks	Discussion & approval		To review the management of key operational risks and agree for onward submission to the ARC.		13.10 – 13.50
4.1 Financial Reporting Controls		✓		Michael Passmore	(5 minutes)
4.2 FS Conduct Risk Update		✓		Jonathan Hill	(5 minutes)
4.3 Change Risk Update		✓		Jenny Ellwood	(5 minutes)
4.4 Financial Crime Risk Update		✓		Sally Smith	(5 minutes)
4.4.1 Product Risk: Gift Card				Keith Maple	(5 minutes)
4.5 IT Risk Update		✓		Rob Houghton	(10 minutes)
4.6 Cyber Security & Information Assurance Update		✓		Mick Ebsworth / Jules Harris	(5 minutes)

CONFIDENTIAL

POL00401626

Post Office Risk and Compliance Committee Agenda (cont.)

Agenda Item		Action Needed	For ARC	Purpose	Lead	Time
5.	**Risk Update**					13.50 – 14.20
	5.1 Risk Placemat, Including an Update on Risk Exceptions and the Rollout of the Placemat	Questions & Noting	✓	To review progress on the rollout of the Placemat.	Richard Williams / Deana Herley / Ian Holloway / Owen Woodley / Tom Moran / Jonathan Hill	(20 minutes)
	5.2 Financial Crime Pilot			To review the progress of the pilot.	Ashish Singh / Sally Smith	(10 minutes)
6.	**Internal Audit**					14.20 – 14.35
	6.1 Audit Report	Questions & Noting	✓	To note the Internal Audit Report and Internal Audit Plan for onward submission to the ARC.	Johann Appel	(15 minutes)
	6.2 Audit Plan 2018/19		✓			
7.	**Updates for Noting**					14.35 – 14.55
	7.1 GDPR Programme Update	Questions & noting	✓	To note the GDPR Programme Update.	Clare D'Netto	(10 minutes)
	7.2 Compliance with Payment Card Industry Data Security Standards	Questions & noting	✓	To receive an update on compliance with PCI DSS.	Nicholas Spicer / Jules Harris	(10 minutes)
8.	**Compliance**					14.55 – 15.00
	8.1 Procurement Compliance Reporting	Noting		To review the Procurement Compliance report and forward view.	Barbara Brannon	(5 minutes)
9.	**Policies for Approval**					15.00 – 15.30
	9.1 Treasury Risk Management Framework, Policies and Authorities	Approval	✓	To agree for onward submission to the ARC.	Mark Dixon	(10 minutes)
	9.2 Document Retention and Disposal Policy	Approval	✓	To agree for onward submission to the ARC.	Jules Harris	(10 minutes)
	9.3 IT Security Policy	Approval	✓	To agree for onward submission to the ARC.	Mick Mitchell / Mick Ebsworth	(5 minutes)
	9.4 IT Disaster Recovery Policy	Approval	✓	To agree for onward submission to the ARC.	Mick Mitchell	(5 minutes)

CONFIDENTIAL

POL00401626

Post Office Risk and Compliance Committee Agenda (cont.)

Agenda Item		Action Needed	For ARC	Purpose	Lead	Time
10.	**Business Continuity** 10.1 Business Continuity Planning 10.2 Business Continuity Policy	Noting Approval	✓ ✓	To agree the BCP report and Business Continuity Policy for onward submission to the ARC.	Tim Armit	15.30 – 15.50 (20 minutes)
11.	**Governance** 11.1 RCC Effectiveness Review 11.2 Update on Terms of Reference for RCC / ARC	Noting Noting		To review and agree the committee's performance against its terms of reference. Verbal update on a review of the terms of reference.	Chair	15.50 – 15.55 (5 minutes)
12.	**Updates from Subsidiaries** 12.1 POMS RCCC Minutes	Noting		To receive the minutes of the POMS RCC meeting held on 31 January 2018.	Chair	15.55
13.	**Any Other Business**				Chair	15.55 – 16.00
	Close					16.00

CONFIDENTIAL

POL00401626

Post Office Limited
Risk and Compliance Committee Meeting

MINUTES OF A MEETING OF THE RISK AND COMPLIANCE COMMITTEE (THE "COMMITTEE") OF POST OFFICE LIMITED (THE "COMPANY") HELD ON 18 JANUARY 2018 AT 20 FINSBURY SREET, LONDON EC2Y 9AQ AT 1.00PM

Present:	Jane MacLeod	Chairman	
	Paula Vennells (PV)	Group Chief Executive	
	Al Cameron (AC)	Chief Financial and Operations Officer	
	Debbie Smith (DS)	Chief Executive, Retail	
	Rob Houghton (RH)	Group Chief Information Officer	
	Martin Kirke (MK)	Group HR Director	
	Mark Davies (MD)	Group Communications, Brand & Corporate Affairs Director	
	Martin Edwards (ME)	Group Strategy Director	
In Attendance:	Johann Appel (JA)	Senior Manager, Internal Audit	
	Ashish Singh (AS)	Interim Head of Risk	
	Owen Woodley (OW)	Managing Director, Post Office Money	
	Jane Fahey (JF)	Deputy Company Secretary	
	Sally Smith (SS)	Head of Financial Crime	3.3
	Jules Harris (JH)	Head of Information Protection and Assurance	*3.8 & 4*
	Clare D'Netto (CDN)	GDPR Programme Manager	*4*
	Chris Russell (CR)	Data Protection Officer	*4*
	Richard Williams (RW)	Senior Risk Manager	*5*
	Barbara Brannon (BB)#	Procurement Director	*6 & 7*
	Ben Foat (BF)	Legal Director	*9*
	Mark Dixon (MD)	Head of Treasury, Tax and Insurance	*11*
Apologies:	Nick Kennett	Chief Executive – Financial Services & Telecoms	

ACTION

by telephone

1. WELCOME, INTRODUCTION AND CONFLICTS OF INTEREST

1.1 The Chairman welcomed DS, Chief Executive, Retail, to the meeting.

2. MINUTES AND ACTION LIST

2.1 Minutes of the meeting of the Board held on 8 November 2017 were approved and authorised for signature by the Chairman.

2.2 The Action List Status Report was noted as accurate. Save for the following, there were no actions due which had not been addressed in advance of the meeting or through the meeting papers:

(a) 1789 – Compliance Requirements: The Chairman advised that discussions were now underway with HMRC on the impact of likely enhanced anti money laundering ("AML") and fit and proper requirements. PV stressed the importance of ensuring this action was

POL00401626

closed by the next meeting; and

(b) 1788 – Financial Crime Risk assessment: The Chairman confirmed that the Financial Crime workshops for Product Managers ("PMs") had been held, however the PMs had yet to complete the follow-up work. **DS agreed to raise the matter with the relevant PMs.** **DS**

3. KEY OPERATIONAL RISKS

3.1 Financial Services Conduct Risk

The Financial Services Conduct Risk Update was noted.

AC highlighted inconsistencies in risk ratings between this report and the Company's financial performance pack presented in other governance forums. The Chairman explained that this was due to lack of alignment in the metrics used to produce the reports and agreed on the importance of consistent reporting.

3.2 Change Risk

The Change Risk Update was noted.

The Chairman advised that Carla Stent, Chairman of the Company's Audit, Risk and Compliance Committee ("ARC") had requested further detail as to the lessons learned from Change activity over the past three years, and a forward view as to where the principal risks would arise. The paper should be updated to reflect this request.

AC invited the Committee to submit any additional comments on the content of the paper to him in advance of the ARC.

SS joined the meeting.

3.3 Financial Crime Risk

SS noted that her report included the Money Laundering Reporting Officer annual review for 2017 which addressed various statutory and regulatory requirements. SS advised that due to the size and complexity of the Post Office network, and the diverse range of products and services provided in both face to face and digital environments, the key financial crime risk control was staff training and awareness. The current training model was inefficient, and while work was underway with Learning and Development to address this, further support from the Group Executive ("GE") and senior leadership population would be required in order to drive completion rates.

RH submitted that it was not sufficient to address this risk through education alone, and that, in order to address the root cause, systems needed to be redesigned to incorporate the right controls. SS responded that no system could entirely address the risk due to the complexity of the network. Therefore, education would remain the key control. PV challenged this, stating that while the issues caused by the network structure were large in scale, they were not necessarily complex. The launch of HGNT would help ensure that agents complied with financial crime-related requirements. In addition, she submitted that there were certain products which should be reviewed to ensure that the benefits they brought to the business outweighed the associated financial crime risk.

In response to a question from DS as to where the legal accountability lay for

POL00401626

financial crime compliance, the Chairman explained that it was her accountability to ensure that there were effective systems and controls to prevent money laundering and counter terrorist financing. However, on a day-to-day basis, responsibility for implementing these controls lay with the business. Training was one aspect of this, as was having processes to ensure products were designed with fraud prevention in mind. Agents were contractually obliged to comply with Post Office rules. She added that twenty agents had recently been suspended for failure to comply with these rules. In response to a further question from DS as to the position of the risk environment, the Chairman clarified that cases of non-compliance were mostly historical. However, as the management information ("MI") in this area had been largely developed over the past two years, it was not possible to provide a definitive, long-term assessment as to whether the risk environment was improving.

SS advised that under requirements introduced during 2017, the Company would be required to demonstrate the fitness and propriety of all agent entities to HMRC. In response to a question from DS as to how compliance with these requirements would be demonstrated, SS explained that this would be achieved through reporting metrics currently under development.

AC queried whether the resourcing and budget required for the recommendations outlined in the paper had been planned for with sufficient detail. JM advised that a detailed project plan had been prepared which was funded to the extent necessary. SS highlighted the importance of ensuring Product Information Packs were complete to demonstrate a full risk assessment. **OW agreed to follow up with the PMs in question.** **OW**

The Committee noted the Money Laundering Reporting Officer's (MLRO) annual report on compliance with The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 and The Terrorism Act 2000, which was included in the report.

SS left the meeting.

3.4 IT Risk Update

The IT Risk Update was noted.

3.5 Financial Reporting Controls

The Financial Reporting Controls Update was noted.

3.6 Business Continuity and Crisis Management

The Business Continuity and Crisis Management update was noted.

In response to a query from AC as to whether sufficient resources were being provided to this crucial area, the Chairman advised that resourcing requirements over the next twelve months were currently under review.

3.7 Health and Safety

The Health and Safety Update was noted.

JH joined the meeting.

POL00401626

3.8 **Information Protection and Assurance**

JH introduced the Information Protection and Assurance Update. AC submitted that while the need to improve the management of data was critical, it was important to ensure that all data management needs were consolidated into one programme. In response, the Chairman advised that all programmes related to data were aligned.

RH commented that the control improvement actions to mitigate insider threat and external malicious attack, as detailed in the appendix to the paper, were somewhat vague. He suggested that GE members be assigned responsibility for identifying owners for the various categories of data, and the actions required to increase the Company's maturity level in this area. **JH agreed to develop a draft proposal.** **JH**

MK requested that **the appendix to the paper be amended to reflect the fact that the HR Director was accountable for, rather than the owner of, the Joiners, Movers and Leavers ("JML") programme.** **JH**

PV requested that **the appendix be updated to provide further detail on how the control improvement actions outlined would be applied in practice.** **JH**

CDN and CR joined the meeting.

4. GDPR PROGRAMME UPDATE

The Chairman introduced the General Data Protection Regulation ("GDPR") Update. She advised that a GDPR training session would be provided to the ARC on the 29 January 2018, and that the matters covered in this paper would form the basis of that session.

CDN explained that the GDPR programme had from inception flagged that it was unlikely to achieve full compliance by May 2018. Instead the programme has taken a risk-based approach to achieve 'effective compliance'. New activity would be compliant on or before 15 May 2018. In addition, remediation of existing activities which were high risk/high priority would be completed by May 2018.

RH highlighted that the challenge to achieving effective compliance by the May 2018 deadline was in meeting change lead times. There was still uncertainty as to what needed to be achieved and when, and consequently whether the necessary operational and technical changes could be delivered in time. For those instances where the requirements were known, it was not clear that the programme was progressing sufficiently quickly to deliver them. **He requested that a clear articulation of the "known unknowns" be prepared, including details of the key stakeholders, and where prioritisation calls may be required.** PV challenged this position, querying whether the volume of change required by the programme between now and May, which was incremental to the existing change agenda, was truly significant. The Chairman advised that it was not, with most of the change involving marketing activity. However, remediating legacy issues would take another approximately 12-18 months following the deadline. **CDN/CR**

POL00401626

MK highlighted that there was a lack of awareness of the issues raised by GDPR across the business **and asked the programme team to consider how they could drive understanding.** **CDN/CR**

JH, CDN and CR left the meeting. RW joined the meeting.

5. RISK UPDATE

RW introduced an update on the Risk Placement, including an update on Risk Exceptions. Rollout of the Risk Placemat was on track to be completed by June 2018. Since the November 2017 meeting, the approach had been further rolled-out within Financial Services and Retail. In parallel, a methodology was being created to test the integrity, and formalise the governance framework, of principal risks for post-Placemat implementation.

The Committee reviewed the current Risk Exception Status and commented on the following in particular:

(a) AC advised that an IT solution for the risk of loss of data/service due to the RPA software running on stand-along desktop machines was still being awaited; and

(b) RH advised that he would need to determine the extent to which Salesforce software was being used across the business prior to making any decision on contract renewal. He expressed frustration at the fact the contract was due to expire on 29 April 2018, which did not give sufficient time for transition, should that be determined the correct option. AC commented that while he was aware of the issue, he had not until now been aware of the April deadline. **He would work with Barbara Brannon to ensure early escalation of these matters going forward. PV requested that RH bring a report on the use of Salesforce across the organisation to GE.** If it were concluded that the software was used exclusively by Customer Relationship Managers ("CRMs"), then she was content to carry any risk until the Company's strategy with regard to CRMs was finalised. **BB** **RH**

RW left the meeting. BB joined the meeting.

6. COMPLIANCE

6.1 Procurement Compliance Report

BB presented the Procurement Compliance Report. She reported that since the last meeting in October 2017 there had been a total of seven non-compliant contract awards, with a total value of GBP9,388,000. Three of these were currently pending imminent contract signature. During that period, a number of large value procurements had been completed and brought into compliance, bringing the overall value down from GBP19 million in October 2017 to GBP15 million in January 2018.

The Committee expressed concern at the level of non-compliance detailed in the report. AC queried whether instances of non-compliance were being escalated to the GE in a sufficiently timely manner. The Chairman submitted that there seemed to be a relaxed culture within the business regarding procurement compliance and

POL00401626

that more could be done to address this. BB responded that while there was room for improvement, it was not necessarily a matter of the business being apathetic where compliance was concerned. There were large parts of the business which were very proactive in working with Procurement and who had a clear understanding of their requirements and the lead times involved. However, there were other part of the business who, for a variety of reasons, found articulating their requirements more challenging and therefore decision-making proved difficult. AC reiterated his request that such instances be escalated earlier.

7. POLICIES

7.1 Supplier Relationship Management

BB recalled for the Committee that, in order to help evidence good supplier management, she and the Chairman had been given an action to create a Supplier Relationship Management Policy (the "Policy"). In doing so, they had endeavoured to create an easy-to-follow guide which defined the minimum standards to manage the day-to-day supplier relationship once the supplier is on board and providing services. She explained that between now and the end of March 2018, Procurement would work the business to create supplier relationship terms, and a timetable would be signed off by each GE member as to how mandatory activities would be delivered over the next 12 months. This would involve identifying the tools and systems to evidence that the required degree of oversight existed. The Committee discussed the merits of Traction system, noting that while it would be relatively simple and cost-effective, it did not hold any data, and merely provided a system to acknowledge completion of the tasks assigned. After discussion, it was agreed in principle that Traction be utilised.

Subject **to a request from RH that the policy be amended to standardise role titles**, the Committee approved the policy. It was agreed that the policy did not require further approval by the ARC. **BB**

BB left the meeting.

8. AUDIT

8.1 Internal Audit Report

The Committee noted the Internal Audit Report.

JA advised that reports for four Internal Audit reviews were currently being drafted or cleared through management. These included reviews of compliance with the Banking Framework and AML compliance for MoneyGram. With regard to the Banking Framework review, a number of areas, namely Information Protection, Data Security, and Business Continuity, required significant improvement in order to demonstrate compliance. The Chairman commented that an assumption had been made at the time of signing the Banking Framework that the requirements under the agreement had been clearly communicated to the relevant teams, which had not been the case. However, the changes required to demonstrate compliance were not material. AC stressed the importance of taking the lessons learned from this, **and requested that a copy of the full report be circulated to the Committee.** After discussion, it was agreed that that the **JH**

POL00401626

Banking Framework report should be submitted for consideration at the March 2018 ARC. **PV requested that OW provide his view on the report from a Post Office Money perspective.** **OW**

JA reported that audit actions were generally being completed on time and 107 actions had been completed year to date, which demonstrated an improvement in the cultural approach of the business. As at 31 December 2017, 36 actions remained open, two of which were overdue. These were being tracked closely.

BF joined the meeting.

9. DEEP DIVES

9.1 Annual Legal Risk Review

BF introduced the Annual Legal Risk Review for 2017 (the "Review"). He outlined the main legal risks for Post Office as follows:

(a) Contract Management
Improvements had been made over the last 12 months to the contracts management and procurement processes, through the introduction and enhancement of a number of controls. These included the enhancement of a central repository of contracts utilising the existing Bravo procurement system. However, there remained further work to enforce a compliant culture in the business. AC advised that it had been agreed earlier in the meeting that Traction would be used to assist with overseeing compliance with contractual terms, and that the Review should be updated to include this.
PV challenged the language used in the Review concerning the number of material arrangements in which services were being provided without a written contract in place. While she agreed that it was unacceptable for there to be no written contract in place, the Review did not detail the significant progress that had been made in managing down the number of such contracts. **AC added that the actions being taken to mitigate any risk arising from the remaining cases should also be clearly spelled out.** **BF**

(b) Competition Rules
There needed to be better understanding of the potential implications of commercial activities, such as acquisitions or joint ventures ("JVs"). The legal department ("Legal") had developed Compliance Guidance and FAQs to support operational managers in understanding this risk, together with bespoke training.

(c) Corporate acquisitions and JVs
Corporate M&A knowledge was dependent on a few core individuals. Legal was developing a Corporate Acquisition Checklist and challenge process aimed at enhancing risk management of these projects.

(d) Litigation
As a result of the Postmaster litigation, the recovery of agent losses and prosecutions have become significantly more challenging, thereby

POL00401626

increasing the risk that the deterrent effect of such recovery actions or prosecutions will be diminished. In addition, there was a risk of default judgments due to Legal not being notified of service of proceedings received in the network. Proper communications were required to ensure documents were scanned and emailed to Legal promptly.

(e) Branding and IP Enforcement
While basic controls were in place, such as cease and desist letters, brand infringements largely went unchallenged. Further enhancement could be achieved through a formal process with appropriate funding. PV responded that these cases should be dealt with on a case by case basis. If a significantly serious instance, or increase in infringement cases were seen, Legal should escalate appropriately.

BF advised that Legal's focus for 2018/19 Legal would centre on enhancing the legal maturity of Post Office through the introduction of enhanced controls, and the delivery of further training to assist managers to better understand core areas of legal risk and develop necessary processes.

10. HORIZON SCANNING

10.1 FCA Report –Ageing Populations and Financial Services

The FCA Report on Ageing Populations and Financial Services was noted.

10.2 Legal and Regulatory Horizon Scanning

The Legal and Regulatory Horizon Scanning report was noted.

MD joined the meeting.

11. INTEREST RATE SWAP UNDER NEW POCA CONTRACT

11.1 Mark Dixon recalled for the Committee that at the July 2017 Board meeting the Group CFOO, following ARC approval, was authorised to execute an interest rate swap, if considered advantageous. A paper setting out the rationale for the transaction, an update on pricing, and how to manage the risks associated with swap execution, was subsequently presented to the ARC in September 2017. He reported that as approval had now been received from the Department of Business, Energy and Industrial Strategy and HM Treasury to enter into an interest rate swap for the purposes of hedging its floating rate exposures linked to the POca cash balances, approval would be sought to do so at the upcoming ARC. The current pricing levels for the swap were then outlined.

After discussion, the Committee noted the paper for onward submission to the ARC.

POL00401626



Post Office Limited
Risk and Compliance Committee Meeting

12. PAPERS FOR NOTING

12.1 Minutes from the meetings of the POMS RCC held on 11 October 2017, 29 November 2017 and 19 December 2017 were noted.

12.2 The EUM Programme Update was noted.

12.3 The SuccessFactors Risk Exception Report was noted.

12.4 JM **agreed to circulate an update on Jointers, Movers and Leavers following the meeting.** **JM**

13. ANY OTHER BUSINESS

13.1 There being no other business, the Chairman closed the meeting.

....
Chairman **Date**

POL00401626

POL Risk and Compliance Committee
Action List

Status Report as at: 06/03/2018

Meeting Date	AP ref	ACTION	Action Owner	Due Date	STATUS	Open/ Closed
18/01/2018	**3.3**	**Financial Crime Risk** - The importance of ensuring Product Information Packs were complete to demonstrate a full risk assessment was highlighted. OW agreed to follow up with the PMs in question.	Owen Woodley	13/03/2018		Open
18/01/2018	**4**	**GDPR Programme Update -** (a) A clear articulation of the Programme's "known unknowns" to be prepared, including details of the key stakeholders, and where prioritisation calls may be required. (b) The Programme team to consider how they could drive understanding of the issues raised by GDPR across	Clare D'Netto	13/03/2018		Open
18/01/2018	**8.1**	**Internal Audit Report** - Owen Woodley to provide his view on the Banking Framework Report from a Post Office Money perspective.	Owen Woodley	13/03/2018		Open
18/01/2018	**9.1**	**Annual Legal Risk Review** - the actions being taken to mitigate any risk arising from the remaining cases (of material arrangements in which services were being provided without a written contract in place) to be clearly spelled out in the Review.	Ben Foat	13/03/2018		Open
08/11/2017	**1801**	**Business continuity testing** - Test Bolton before the implementation of SuccessFactors and Chesterfield by the financial year end	Tim Armit	02/05/2018	Bolton to be tested by end of April 2018.	To close
08/11/2017	**1800(b)**	**IT DR plans** - Provide an update on IT Disaster Recovery plans	Mick Mitchell	02/05/2018	Included in March agenda.	To close
13/09/2017	**1789**	**Compliance requirements -**Discuss impact of likely enhanced AML & fit & proper requirements with the relevant stakeholders in Government	Jane MacLeod/ Patrick Bourke/ Mark Davies	13/03/2018 (next update)	In light of the new challenges from HMRC regarding retention of customer ID, together with Patrick Bourke we are looking to set up stakeholder meetings with HMRC shortly.	To close
20/07/2017	**1781**	**Insurance Distribution Directive -** Provide a briefing on the potential training requirements of the IDD in order to consider the future compliance burden against capacity in the branch network	Jonathan Hill	18/01/2017	Update at November RCC: Network and Learning team currently looking at this. Will have a year to implement. Update on progress due at January RCC.	Open
09/03/2017	**1773**	**RCC Terms of Reference** - to be reviewed and updated based on changes in PO structure	Jane MacLeod	13/03/2017	Verbal discussion at March meeeting.	To close

POL00401626

Actions Update

Author: Company Secretariat Meeting date: 13 March 2018

Executive Summary

Context

Further to the actions list published with the Risk and Compliance Committee agenda on 7 March 2018 supplementary information has been supplied. Accordingly an updated actions list is provided for the committee's reference.

Input Sought

1. The committee is asked to review the revised actions list and comment on the updates contained therein.

Appendices

1. Risk and Compliance Committee Actions List Updated 12 March 2018
2. GDPR Programme Update in Response to Action 4

POL00401626

1. Risk and Compliance Committee Actions List Updated 12 March 2018

Meeting Date	AP ref	ACTION	Action Owner	Due Date	STATUS	Open/ Closed
18/01/2018	**3.3**	**Financial Crime Risk** - The importance of ensuring Product Information Packs were complete to demonstrate a full risk assessment was highlighted. OW agreed to follow up with the PMs in question.	Owen Woodley	13/03/2018	Packs have been completed.	To close
18/01/2018	**4**	**GDPR Programme Update** (a) A clear articulation of the Programme's "known unknowns" to be prepared, including details of the key stakeholders, and where prioritisation calls may be required. (b) The Programme team to consider how they could drive understanding of the issues raised by GDPR across the business.	Clare D'Netto	13/03/2018	The GDPR Programme Manager has provided an overview of the known unknowns and actions to drive understanding which is annexed to this actions tracker.	To close
18/01/2018	**8.1**	**Internal Audit Report** - Owen Woodley to provide his view on the Banking Framework Report from a Post Office Money perspective**.**	Owen Woodley	13/03/2018	Owen had a look at the report and did not have anything further to add.	To close
18/01/2018	**9.1**	**Annual Legal Risk Review** - The actions being taken to mitigate any risk arising from the remaining cases (of material arrangements in which services were being provided without a written contract in place) to be clearly spelled out in the Review.	Ben Foat	13/03/2018		Open
08/11/2017	**1801**	**Business Continuity Testing** - Test Bolton before the implementation of SuccessFactors and Chesterfield by the financial year end.	Tim Armit	02/05/2018	Bolton to be tested by end of April 2018.	To close
08/11/2017	**1800(b)**	**IT DR plans** - Provide an update on IT Disaster Recovery plans.	Mick Mitchell	02/05/2018	Included in March agenda.	To close
13/09/2017	**1789**	**Compliance requirements -** Discuss impact of likely enhanced AML & fit & proper requirements with the relevant stakeholders in Government.	Jane MacLeod/ Patrick Bourke/ Mark Davies	13/03/2018 (next update)	In light of the new challenges from HMRC regarding retention of customer ID, together with Patrick Bourke we are looking to set up stakeholder meetings with HMRC shortly.	To close
20/07/2017	**1781**	**Insurance Distribution Directive -** Provide a briefing on the potential training requirements of the IDD in order to consider the future compliance burden against capacity in the branch network.	Jonathan Hill	18/01/2017	Update at November RCC: Network and Learning team currently looking at this. Will have a year to implement. Update on progress due at January RCC.	Open
09/03/2017	**1773**	**RCC Terms of Reference** - to be reviewed and updated based on changes in PO structure.	Jane MacLeod	13/03/2017	Verbal discussion at March meeting.	To close

POL00401626

2. GDPR Programme Update in Response to Action 4

Known/Unknowns	Impact & decision	Stakeholders	Actions to drive understanding
IT Remediation costs for suppliers to comply with the updated DP clauses and security standards	Cost – potential impact on agreed budget for 2018/19	CIO / Systems Owners	1. Requires an accurate/documented view of the personal data processes and relevant controls, including the ability /processes to delete data. ○ *The Programme is experiencing blockers to getting this from IT suppliers. This has been well documented via the programme governance. The remediation is that the Programme Director and Systems PM are going to focus on a couple of key suppliers to understand how we can remove these.* 2. Contracts updated with the DP clauses and schedules including the Schedule of Processing and Security Schedule (by May 2018). ○ *A process for Assurance will be established by May 2018 which will result in gaps for remediation being identified which will continue beyond May 2018.*
Costs of data deletion to complete with retention schedules	Cost – as above	CIO / Systems owners	1. PO's Document Retention policy and retention schedules is currently outside scope of the GDPR Programme and is a key dependency. Therefore a business case will be raised via the GDPR programme to address this. • *The programme is currently assessing the existing processes and capability for suppliers to delete data when this comes into force.*
Unstructured data We don't know where all the unstructured data is on POL, POMS and suppliers systems	Scope & cost	CIO / Business Owners	1. Work with suppliers to identify the location of the data on their systems. We have asked this via the original questionnaire but information received is incomplete. IT help required to push this forward and this may incur a cost – see above. 2. The Business Functions work stream is assessing where this is on PO systems – for high risk areas. 3. POL could invest in a tool to search for data and delete based on a POL retention policy (see above re: dependency), but cost is dependent on the size of the data if unknown. 4. Education will be key, so data will be on One Drive and Share-point otherwise we can't scan and delete.
Suppliers Information on Bravo is out of date and incomplete so we know we don't know all the contracts, including non-IT suppliers, software licences and this will impact on our ability to remediate contracts and but also puts us at risk as a result of our failure to maintain an up to date inventory and / or if there is a data breach for an unidentified vendor.	Scope	Contract Owners	1. Email going out to GE/GE-1 on 12/3 to identify a single point of contact to help us pick up some of the smaller contracts, not currently held on Bravo or visible to the Team. 2. The Programme is also working with IT and Procurement on this, however there will be a requirement for tighter controls for new IT vendors and software in BAU. 3. We have engaged a Contract PM who will drive this forward.

POL00401626

Financial Reporting Controls

Author: Danielle Goddard Sponsors: Micheal Passmore, Al Cameron Date: 13 March 2018

Executive Summary

Context

The purpose of this paper is to update the RCC on the status of the Financial Reporting Controls Framework (the FRC), the most recent control self-assessment results (January 2018), current areas of focus, and the progress made on the second phase of the project.

Questions addressed in this report

1. What is the current status of the FRC?
2. What testing is being performed over the FRC?
3. What is the status of the additional scope of the FRC?
4. What other controls changes are being implemented?
5. What actions are being taken in response to the control points raised in EY's FY16/17 audit report?
6. What additional work is planned for FY17/18 year end?

Conclusions

Current status of the FRC
The number of controls has increased from 303 at end December 2017, to 326 at end January 2018. Most of the increase relates to 18 new controls over Success Factors (after the January go live). The framework continues to be self-assessed on a monthly basis within the TrAction online self-assessment tool and results are monitored.

Of the 326 controls at end January 2018, 255 (78%) were issued for self-assessment. 250 (98% of those issued for self-assessment) were operating effectively. Of the remaining 5 controls, 2 related to new controls where work is required to formalise the evidence of the control for the next self-assessment, 1 relates to a monthly process and risk review which will be completed for the next self-assessment due to a change in ownership, and the remaining 2 are under review with the control owners.

Of the 71 controls not issued for self-assessment at the end of November, 59 were not due to be operated in the period. The remaining 12 controls were in remediation, with workaround controls in place or remediation in progress.

PwC's comments over spreadsheet controls have been fully implemented.

Strictly Confidential

POL00401626

Testing performed
Internal sample testing is now being performed by the FRC team; 186 controls have been tested to date, the results are detailed within section 2.2 of this paper. Of the 186 controls tested, 148 were operating effectively, 18 had insufficient evidence, 13 were not operating effectively, and 7 were in remediation. All 13 ineffective controls have since been remediated, and 15 of the 18 with insufficient evidence have been resolved (with the remaining 3 in progress). In addition to this, communications have been issued to remind control owners how to appropriately evidence controls in line with best practice.

PwC began further independent testing in February and are currently finalising the results of the 74 controls they selected for testing.

EY selected 33 controls to walkthrough, and are in the process of testing those which they can rely on for audit purposes.

Additional scope of the FRC
5 Masterdata processes are complete, the 9 remaining Masterdata processes are expected to be complete by end June 2018 (extended from May 2018 due to recent work over Success Factors, ART and CWC Masterdata).

FSC Transaction Correction controls are now being self-assessed on a monthly basis; further work commenced in March to analyse the balance sheet accounts relevant to FSC, and to ensure that the appropriate in-depth reconciliations and controls are in place.

Other controls changes and improvements
18 new controls have been added to the self-assessment process in relation to Success Factors. There are still some control recommendations being closed in relation to Success Factors; these will be complete by the year end or workaround controls in place where necessary.

Interim controls continue to operate over POLSAP journals. Work is being performed as part of Back Office Transformation ('BOT') to ensure that strong automated controls are in place once POLSAP processes migrate into CFS.

A full cash count is planned for Belfast cash centre at transition from POLSAP to CWC. There was a full cash count performed at all cash centres in February; the Glasgow and London counts are required to be re-performed, this is planned for March 2018 and Finance will attend both locations.

Closure of the FY16/17 control points raised by EY is in progress. Progress against each item is detailed in Appendix 2 of this paper.

Input Sought

The RCC is asked to note the progress made and comment on the priorities.

POL00401626

The Report

1. What is the current status of the FRC?

1.1 The FRC is self-assessed by control owners on a monthly basis, with results monitored by the FRC Manager. The table below summarises compliance in January 2018.

January 2018 - Total controls	**326**	
Less: Controls in remediation	(12)	
Controls not due to be operated due to frequency	(59)	
Total population for self-assessment	**255**	**78%**
Self-assessed and operated effectively	250	98%
Self-assessed but not operated effectively	5	2%
No self-assessment submitted	0	0%

1.2 The total number of controls continues to expand for changes and improvements in processes, and the additional scope of the project. 29 incremental controls have been added, and 6 controls removed since the last update to RCC; the new controls relate to 18 controls over Success Factors (after the January go live), and 11 other new controls.

1.3 Of the 326 controls at end January 2018, 255 (78%) were issued for self-assessment. 250 (98% of those issued for self-assessment) were operating effectively. Of the remaining 5 controls, 2 related to new controls where work is required to formalise the control or control evidence for the next self-assessment, 1 relates to a monthly process and risk review which will be completed for the next self-assessment due to a change in ownership, and the remaining 2 are under review with control owners.

1.4 Of the 71 controls not issued for self-assessment at the end of January, 59 were not due to be operated in the period. The remaining 12 controls were in remediation; remediation is expected to be complete by year end except where reliant on BOT implementation (although workaround controls are in place where this is the case).

1.5 The implementation of PwC's recommendations over spreadsheet controls is now fully complete and a sample review control will be performed going forwards. The recommendations related to the implementation of a summary control sheet, separation of inputs and outputs, and password protection; these have been applied across the full population of critical spreadsheets.

POL00401626

2. What testing is being performed over the FRC?

2.1 Internal sample testing of controls is being performed by the FRC team. 186 controls have been tested to date. Of these 186, 148 (80%) were 'green' (control operating effectively), 18 (10%) were 'amber' (deemed to be operating effectively but not appropriately evidenced), 13 (7%) were 'red' (not operating effectively), and 7 (4%) were in remediation. The testing results by process are summarised below.

2.2 All 13 red controls have since been remediated and now deemed as operating effectively. Of the 18 amber controls, 15 are now deemed as being evidenced appropriately and the remaining 3 are being followed up. In addition to this, communications have been issued to remind control owners how to appropriately evidence controls with examples of best practice.

Process	Controls tested	Control in remediation	Controls operating effectively	Controls with insufficient evidence for audit purposes	Controls not operating effectively
Bank & Cash Management	27	0	23	4	0
Bill To Cash	13	0	13	0	0
Client Settlement	1	1	0	0	0
Fixed Assets	17	2	7	6	2
Payroll	44	0	39	3	2
Procure To Pay	16	0	14	2	0
Project Accounting	5	0	2	0	3
Record To Report	33	0	27	2	4
Settlement Process	10	1	9	0	0
Stock	2	0	2	0	0
Tax	12	3	6	1	2
Treasury	6	0	6	0	0
Total	**186**	**7**	**148**	**18**	**13**

2.3 PwC are performing further independent testing of the controls framework and have selected a sample of 74 controls for testing. The sample selected includes controls from each process; some of the controls selected have been internally tested by the FRC team. PwC are currently completing their testing and will report their results in due course.

2.4 As part of the external audit, EY were provided with a list of key controls from the framework. EY selected 33 controls to walkthrough and are in the process of testing those which they can rely on for audit purposes.

POL00401626

3. What is the status of the additional scope of the FRC?

3.1 The scope of the FRC was extended to cover; Masterdata, Finance Service Centre ('FSC') processes, Agents' Debt, Agents' Remuneration, Cash Management and Forecasting, and POMS.

3.2 5 Masterdata processes have now been completed. Vendor, Customer, GL, Payroll and Employee Masterdata controls are in TrAction being self-assessed on a monthly basis. The remaining 9 Masterdata processes are expected to be complete by end June 2018 (extended from May 2018 due to recent work over Success Factors, ART and CWC Masterdata).

3.3 Key controls over the FSC Transaction Correction process are now part of the monthly self-assessment process. An additional piece of work commenced in March to analyse the FSC balance sheet accounts; this will include mapping the balance sheet accounts back to the relevant FSC process and ensuring that risks and controls have been documented for each of these processes, and alongside this reviewing the balance sheet reconciliations in place to ensure completeness and robustness.

3.4 Mapping of risks and controls over the Agents' Debt process has also commenced in March.

4. What other controls changes are being implemented?

4.1 Interim authorisation controls continue to operate over POLSAP journals. A monthly 10% sample check is performed; one exception was noted for January 2018 and retrospective authorisation is being obtained. Work is being performed to develop automated controls as part of BOT (refer to section 4.5.5 of this paper).

4.2 A bi-annual full cash count (at all cash centres) control has been added to the framework. Cash count instructions and templates have been issued by Finance to the cash centre managers.

4.3 Full cash counts took place at all cash centres in February 2018; with Finance attendance at Birmingham and external audit attendance at London and Glasgow. It has been deemed necessary for London and Glasgow to re-perform their counts, as counts were completed prior to the time that external audit were advised to arrive on site. The counts have been rescheduled for 16 and 17 March 2018 and for both sites a Finance representative and external audit representative will attend.

4.4 Work is in progress over Fixed Asset controls, including a review of all AUCs >£500k to ensure that no material live projects remain in AUC. This is substantially complete and will be fully complete for end March 2018. A quarterly review will be implemented going forwards. Further work is being performed to ensure appropriate controls over additions, disposals and physical verification prior to year end.

POL00401626

4.5 There are a number of projects which the FRC team have engaged with to ensure existing controls are adapted or new controls are documented:

4.5.1 New controls have been documented over the new HR system Success Factors which went live in January 2018; 18 new controls were live for the January self-assessment, and 8 existing controls were adapted. A number of IT General Controls have also been documented in respect of Success Factors, which have been reviewed by the IT Controls team for inclusion within the IT Controls Framework.

4.5.2 31 new controls have also been documented in respect of Agent Remuneration Transformation ('ART'); these have been loaded into TrAction to be performed for the February self-assessment (performed in March).

4.5.3 Review of CWC controls is still in progress; there are a number of outstanding controls actions which are expected to be completed during March 2018. Some lower risk outstanding actions will remain for completion by June 2018 go live.

4.5.4 The Back Office Transformation team continue to work closely with the FRC team to ensure an appropriate control environment is in place over all process changes and migrated processes. Business process documents and control matrices are being reviewed and signed off by the relevant business owners, the FRC team and the Finance Director, POL.

4.5.5 The FRC team are engaged in the building of automated user access controls in CFS; this will minimise the user access risk when POLSAP processes are migrated to CFS. The BOT team are performing the analysis required to design these user access controls so that they can be formally signed off and built prior to go live in June 2018. The controls will ensure that all manual journals are centrally processed where possible, and there is a closed environment for any manual transactions which cannot be centralised (e.g. transaction corrections, file uploads, settlements, and other high volume processes which are transitioning from POLSAP to CFS).

5. What actions are being taken in response to the control points raised in EY's FY16/17 audit report?

5.1 Actions and deadlines are being tracked for each Management Letter Point raised by EY (refer to Appendix 2). A detailed status update is included in Appendix 2.

5.2 All items are expected to be completed prior to end March 2018 with the exception of item 2.18 which cannot be resolved until Back Office Transformation go live.

5.3 There are three items which are behind target but are expected to be completed by year end:

5.3.1 Item 2.8 Bill payments revenue; the required analysis has been performed to determine the correct income accrual required. A paper was provided to EY at

POL00401626

the prior year end and this is currently being updated to reflect the current position. This is expected to be resolved by end March.

5.3.2 Item 2.19 Management of SAP privilege accounts; EY recommended changes to two specific SAP privilege accounts. The DDIC account has been locked by Accenture as recommended, however the TMSADM account password has not been changed as Accenture have advised against this; this will be discussed with EY prior to end March.

5.3.3 Item 2.20 Changes approval; the IT team have discussed with Atos the evidence retained for changes that require CAB approval, and we believe this is sufficient evidence of approval. A discussion will be held with the EY IT audit team before end March 2018.

6. What additional work is planned for FY17/18 year end?

6.6 The following work is in progress or planned to be performed for FY17/18 year end:

6.6.1 Finance Directors have been notified that their Balance Sheet review files for P11 and P12 should include auditable evidence to accompany the reconciliations for any line item >£250k; the evidence will be reviewed centrally and questioned appropriately P11 and P12 Balance Sheet review meetings.

6.6.2 Annual controls are being performed prior to year end where they are not specific to P12, in order to identify any potential issues and allow internal testing of annual controls prior to year end.

6.6.3 Cut-off reminders have been issued to Finance prior to year end, and teams will be reminded of this in the Balance Sheet review meetings. Unrecorded liabilities review will be performed in the weeks prior to and after the year end date.

POL00401626

Appendix 1 – January 2018 CSA results by process

Controls		Control Gaps				Control Owners		January 2018 CSA Results (submitted February 2018)				
Process	Total controls	Control gaps	H/M/L risk gaps			Owner Assigned	No owner assigned	Controls operated effectively	No self assessment submitted	Not operated due to agreed frequency	Self-assessment submitted but control not operated	Controls to be set to live
			H	M	L							
Bank & Cash Management	31	0	0	0	0	31	0	31	0	0	0	0
Bill To Cash	41	0	0	0	0	41	0	34	0	5	2	0
Control Environment	38	2	0	1	1	38	0	30	0	4	2	0
Fixed Assets	22	2	0	0	2	22	0	17	0	3	0	0
Payroll	64	0	0	0	0	64	0	57	0	7	0	0
Procure To Pay	27	0	0	0	0	27	0	18	0	9	0	0
Project Accounting	10	1	0	1	0	10	0	5	0	4	0	0
Record To Report	44	5	0	4	1	44	0	24	0	14	1	0
Settlement Process	16	1	0	0	1	16	0	10	0	5	0	0
Stock	5	1	0	1	0	5	0	4	0	0	0	0
Tax	20	0	0	0	0	20	0	12	0	8	0	0
Treasury	8	0	0	0	0	8	0	8	0	0	0	0
	326	**12**	0	7	5	**326**	**0**	**250**	**0**	**59**	**5**	**0**

POL00401626

Appendix 2 – Status of EY control findings from FY16/17 audit

Observation		Control issue	Business efficiency	Priority	POL Owner(s)	POL deadline	Status	Comments
2.1.	Assets under construction project monitoring	✓	✓	High	Tom Woodhouse	25-Mar-18	In progress	An AUC review is substantially complete, and is expected to be fully complete by end March 2018.
2.2.	Asset under construction additions	✓	✓	High	Tom Woodhouse	25-Mar-18	In progress	The AUC review will be performed quarterly from end March 2018.
2.3.	Fixed asset disposals	✓	✓	Medium	Tom Woodhouse	25-Mar-18	In progress	The business case template has been updated to identify disposals. A review of the masterplan report is in progress in order to identify branch closures and assess completeness of disposals; this will be complete by end March 2018.
2.4.	Ongoing management of the FAR		✓	Medium	Tom Woodhouse	25-Mar-18	In progress	Accenture have been engaged to assist with processing bulk changes through the SAP asset register. There has been delay due to system restraints but this is expected to be complete for year end.
2.5.	Branch postcodes		✓	High	Tom Woodhouse	25-Mar-18	In progress	A review of the different sources of data is in progress.
2.6.	Revenue commission rates	✓	✓	High	Danielle Goddard	31-Jan-18	Complete	Product manager review of all billing rates has been co-ordinated by Finance and is complete; this exercise will be performed quarterly from end March 2018.
2.7.	Revenue third party information		✓	High	Danielle Goddard	25-Mar-18	Complete	A third party audit control is now live; three third party audit visits have been performed to date and a plan for FY18/19 is currently being drafted.
2.8.	Bill payments revenue	✓		High	Danielle Goddard	28-Feb-18	In progress	Calculations have been completed and a paper is currently being drafted for external audit.
2.9.	Network cash internal audit	✓		High	Russell Hancock, Danielle Goddard	31-Jan-18	Complete	Cash counts were held in February 2018 at all cash centres with instructions and templates issued by Finance, and Finance attendance at one site. Reperformance of counts for Glasgow and London will take place in March 2018 with Finance attendance at both. A plan is in place for future bi-annual counts; Finance oversight and attendance will continue.
2.10.	Network cash counts	✓		High	Russell Hancock, Danielle Goddard	31-Jan-18	Complete	See comments above regarding Finance attendance at cash counts. A policy regarding sealed cages has been included in the count instructions.
2.11.	Pension discount rate		✓	Medium	Micheal Passmore	25-Mar-18	In progress	Pension assumptions will be discussed in March 2018; planning meetings have been held with external advisors in line with normal year end procedures.
2.12.	Financial statements preparation		✓	Low	Danielle Goddard	25-Mar-18	Complete	A new Sharepoint site (with restricted access) has been set up and all FY16/17 and FY17/18 support to date has been saved here.
2.13.	New accounting standards		✓	High	Briony Tristram	25-Mar-18	Complete	Initial report has been submitted to the ARC and discussions will be held with external audit as part of their audit requests. Project is in progress.
2.14.	Timely deactivation of leavers' accounts	✓		High	Matthew Warren, Tracy Wilkes	31-Jan-18	Complete	Weekly leavers control is now being evidenced.
2.15.	Approval of third party created user accounts	✓		High	Matthew Warren, Tracy Wilkes	25-Mar-18	Complete	Steria have been instructed not to create new user accounts without POL approval; a sample check has been performed with no issues noted.
2.16.	Improvement in the periodic user access review process	✓		Medium	Matthew Warren, Tracy Wilkes	25-Mar-18	In progress	Two bi-annual user reviews will have been completed by end March 2018.
2.17.	Segregation of incompatible duties within the manage change process	✓		Medium	Rebecca Barker	25-Mar-18	In progress	This is under review as part of the IT Controls Framework.
2.18.	Direct access to make changes to SAP - SCC4 security settings	✓		Medium	Max Jacobi	30-Jun-18	In progress	This is expected to be resolved after BOT implementation.
2.19.	Management of SAP privilege accounts	✓		Medium	Matthew Warren	31-Jan-18	In progress	EY's recommendations have been discussed with Accenture; the DDIC account has been locked as advised. Accenture have advised that changing the TMSADM password is not advised as it could affect service; this will be discussed with EY in March 2018.
2.20.	Changes approval		✓	Medium	Rebecca Barker, Max Jacobi	28-Feb-18	In progress	Evidence of change approval is being maintained through the CAB process; this process will be discussed with EY prior to year end.
2.21.	Audit of third party providers		✓	Low	Rebecca Barker	28-Feb-18	Complete	EY's recommendation has been noted for any future contract negotiations.

POL00401626

Financial Services Conduct Risk Update

Author: Jonathan Hill

Meeting date: 13 March 2018

Executive Summary

Context

1. This paper updates the Committee on current risks and actions in respect of conduct risk. One of the key risks on the FS Risk register (also reflected in the Post Office and POMS risk registers) relate to conduct risk. Conduct risk in the regulated financial services context refers to risks to customers from poor product design, distribution and selling processes as well as those risks relating to poor product fulfilment.

Questions this paper addresses

2. This paper provides an update on the key conduct risks and how they are being managed.

Conclusions

3. Conduct risk is within risk appetite. The February BoI risk dashboard highlights 17 green, 4 amber and 1 red rating on its dashboard. For POMS the data reported in February was 16 green, 0 amber and 3 red.
4. The common red rating theme from POMS and BoI identified through mystery shops is that colleagues are not following the approved introductory processes. Separately POMS had a red metric for a higher incidence of upheld complaints because of issues surrounding delivering the free £50 gift card for Over 50s Life cover but this is outside of Post Office's control.

Input Sought

5. The Committee is asked to note these developments.

POL00401626

The Report

Key risks, governance and management information

6. Conduct risks are measured and reviewed by FS&T Risk together with our Principals on an on-going basis and management information is provided on the key risk areas. These are reviewed at the BoI-Post Office Customer and Conduct Risk Committee (CCRC) and POMS-Post Office Joint Compliance Committee (JCC), which meet monthly.
7. In the new financial year Post Office FS&T Risk will be working with BoI, POMS and the LRG team to take on and further develop the dashboards as the first line for Conduct Risk.

Current risks and issues

Mystery Shops

8. FS&T Risk has undertaken counter mystery shops of FS products. This has highlighted a failure in branches to follow the introductory sales processes.
9. Encouragingly, close to 100% of our shopping results confirmed that the mystery shopper was not pressurised to take out a product 'there and then'. The shopper was given time to read the product literature.
10. We are taking the product managers and training team through our findings so they can understand which areas need improving so that the introduction/sales process is as easy as possible to follow, whether this be via a Post Office counter or a tablet.
11. A key conformance weakness in the sales process is the provision of the 'summary box leaflet' with each savings application. We are deploying series of activities to help improve this performance. This includes reducing the number of different savings packs (with improved designs), improving the ordering processes for branch savings materials, monthly communications and working with the BoI Business Controls Team to help support conformance.

Out of date product literature in branch

12. We have identified that there is a high frequency of 'out of date' product literature out in branch or behind the counter available to give to customers.
13. FS&T Risk have been working with Network and Supply Chain (including the branch user forum) on solutions. The key actions taken include updated communications through a new branch focus article supported by an updated monthly checklist to enable branches to understand all the FS literature that is current. This has received good feedback from the network.
14. We are also piloting a new branch checklist to be deployed by the end of March for Branch Managers/Postmasters to use, working with the Network Gateway team.

Vulnerable Customers

15. The Post Office ARC approved the updated Vulnerable Customers policy in September 2018, with both Kevin Gilliland and Nick Kennett sponsoring and Tom

POL00401626

Wechsler and Jonathan Hill as policy owners. The policy recognises that Post Office already does a large amount to support vulnerable customers (and there are many examples in the 'One' communications). Nevertheless we have challenged ourselves to identify gaps and possible solutions.

16. A key area of our work has been to listen to key stakeholders and, in liaison with the Public Affairs team, we have linked up with Mind, Age UK, Sense and the Alzheimer's Society. We have also liaised with BoI and UK Finance (including joining two of their working groups on vulnerability) and reviewed FCA/Ofcom guidance as vulnerability is a key focus area for the regulators.

17. To date we have not identified any large gaps in our approach but there are always potential areas of improvement we can consider. For example:

- POMS is developing dementia training for its Glasgow contact centre, working with the Alzheimer's Society.
- We have asked the Alzheimer's Society to review Post Office Vulnerable Customers training that we include in various training courses to give feedback on how this could be improved
- We are looking at how we as an organisation/individuals might be able to become a Alzheimer's Society "Dementia Friend" and also what support we can give to our own people impacted by dementia.
- We need to improve our website to better organise the current vulnerability information, strengthen information on how to avoid scams and publish our vulnerability approach to meet Ofcom vulnerability requirements
- Sense has offered a resource to 'road-test' new propositions such as the customer hub
- Operational improvements have been identified to the provision of alternative forms of product information e.g., type talk, large print information

18. We will conclude the full report for the May RCC and ARC.

Regulatory agenda items previously highlighted.

Insurance Distribution Directive

19. This key piece of legislation will come into force on 1st October 2018. This covers a number of key requirements including:

- New disclosure wording requirements,
- A customer's best interest rule and
- A requirement to demonstrate that those involved or overseeing insurance mediation can demonstrate competence and are trained with 15 hours of CPD.
- POMS is driving the project on this which will require wide FS&T Risk and Network engagement.

Further FCA Consultation Papers on Senior Manager and Certification Regime (SM&CR).

20. The FCA released three Consultation Papers (CPs) in December covering this topic with the implementation timetable still unclear for intermediaries such as POMS. In previous papers the FCA had acknowledged that SM&CR did not apply to ARs, but said it would bring out a further CP covering ARs. However, in these CPs the FCA states that the regime will not apply to ARs. This is because the FCA has acknowledged the Financial Services Act 2016 does not give it the powers to do this.

POL00401626

21. Therefore, the responsibility rests with the Principal firm to ensure the activities of the AR remain compliant. POMS is driving a project to implement these requirements, supported by Post Office HR and FS&T Risk.

FCA Mission Our Future Approach to Consumers Paper (issued November 2017)

22. The FCA outlines its mission in respect of consumers, recognising the changes in technology and the characteristics and changing demographics of consumers. In all markets the FCA wants to see consumers being able to access the products they need, for the market to deliver high quality good value products and services and for there to be financial inclusion. But the FCA recognises that it does not have the mandate to ensure access to financial services for all but it will intervene under its public sector equality duty if it sees discrimination against vulnerable customers.

23. It aims for partnership working with the industry and others to achieve its objectives recognising that in some areas (such as vulnerable customers) it has been able to make good progress with industry engagement rather than rules and regulation.

FCA Financial Lives Study 2017-issued October 2017

24. Based on nearly 13,000 face-to-face and online interviews, Financial Lives is the regulator's tracking survey on consumers and finance. The paper can provide some useful data on our key markets and the challenges that might be raised by the FCA in the future. This paper has been shared with the Post Office Money team

FCA published findings from the Ageing Population Project-Occasional Paper no 31 issued September 2017

25. A report was provide at the previous committee

FCA focus on culture and performance management guidance.

26. This is an ongoing theme in the FCA's business plan and regulatory approach to ensure an appropriate customer centric culture is embedded in firms.

General Data Protection Regulation

27. The General Data Protection Regulation (GDPR) ushers in an enhanced legal regime for the collection, processing and storage of personal data from 25th May 2018. A comprehensive risk review and programme is underway in Post Office, with appropriate training being provided to personnel. The Post Office and BoI GDPR teams are working together.

FCA Strategic Review of Retail Banking

28. Further to the FCA's review, it is now seeking to improve its understanding of the state of competition and conduct in retail banking markets at a pivotal time of change. We await first publication of the information in mid-August 2018.

Jonathan Hill
Head of FS&T Risk & Regulation

POL00401626

BOI Post Office Money branch distribution - February 2018

Risk ratings

January risk ratings and how they compared to December

Red rated MS shops	▲
Red rated CRM shops	◀▶
Red rated counter shops	◀▶
Black rated MS shops	◀▶
MS mutiple red/black shops	◀▶
A or B rated mortgage cases	◀▶
D rated mortgage cases	◀▶
MS meeting QAT benchmark	◀▶
Distribution complaints	◀▶
Mis-selling complaints	◀▶
Conduct survey results	▼
Mystery shopper experience	◀▶
NPS survey results	
Branch product knowledge	◀▶
Branch regulatory knowledge	◀▶
Specialist/CRM knowledge	◀▶
Branch advertising reviews	▲
Advertising compliance issues	▲
Social media compliance issues	◀▶
Savings cancellations	◀▶
Competent specialists	◀▶
Supervisor spans of control	◀▶
BOI supervisor reviews	◀▶

Performance measured in January

Risk ring and overall performance rating



Based on the weighted cumulative outcome of the KRIs we measured in January, the overall risk rating is Amber.

Green rated KRIs



Amber rated KRIs



Red rated KRIs



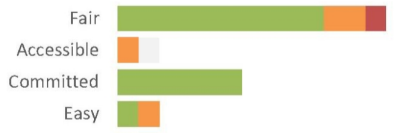
This month we were within tolerance for 21 out of the 22 KRIs we measured. 17 of our KRIs were rated green and 4 of our KRIs were rated amber. One of our KRIs was rated red. In comparison, in December we exceeded tolerance in 2 of our KRIs and in November we exceeded 3 of our tolerances. On average, in each month between August and January, we were within tolerance in 20 of the KRIs we measured and exceeded tolerance in 2.

January v December ratings

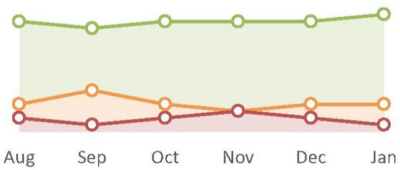
◀▶	15
◀▶	2
◀▶	1
▲	2
▲▼	2
▼	0

One KRI remained red, one KRI moved out of red and no KRIs fell to red.

Performance against our FACE commitments



Distribution of KRI risk ratings between August 2017 and January 2018



Exceptions and key trends

CRM mystery shops - Savings shops are still resulting in red ratings, with 9 out of 52 (17.3%) being red rated in the 3 months to the end of January 2018. This rate has remained steady over the previous 3 months. A detailed action plan was submitted to C&CRC at the January 2018 meeting and will continue to be monitored.

Counter shops - The Red rated KRI relates to counter-staff savings mystery shops completed across the DMB, agency and multiple networks by both BOI and Aba during the three months ending January 2018. 26 of the 59 shops completed (44.1%) were rated red. The shops related to introductory conversations and the red ratings were caused by staff making comments or taking actions which could have been deemed as suggesting the suitability of a particular course of action and/or failing to provide a summary box leaflet.POL have prepared a detailed breakdown of the MI which is due to be presented to C&CRC in February with recommended actions included. A targeted campaign of counter mystery shops has since been planned for early 2018.

Branch Advertising Reviews - Whilst only one BOI branch review was rated 'red' in January 2018 for displaying out-of-date marketing literature and/or not following display instructions, POL continue to investigate what process and control improvements could be made to ensure out-of-date literature is less likely to remain in the public domain across the network. There was one material financial promotion issue recorded in January in relation to the online Summary Box Leaflet which was published with an old approval number displayed. There was one in-branch social media breach, where a branch uploaded details of a credit card offer without the corresponding link to T&Cs.

Conduct Survey Calls - Due to the low volume of calls made in Jnauary (5), the data has been skewed. No new issues were identified.

Mystery Shopper Experience - Whilst the results have remained steady over recent months, a full review of the question set completed by the mystery shopper is to be reviewed to ensure the questions fully reflect an introductory conversation.

◀▶ Remained green ◀▶ Remained amber ◀▶ Remained red ▲ Improved to green ▲ Improved to amber ▼ Fell to amber ▼ Fell to red

BOI Group classification : **Red** (Confidential) - distribute only with sender's permission

POL00401626

Joint Conduct Committee (JCC) - Network Distribution Scorecard

Jan-18

Risk ratings

January risk rating and how they compared to December		
●	Branch net sales vs complaints	◀▶
●	% of branch complaints upheld	◀▶
●	FOS cases upheld	◀▶
●	Red rated MS VMS shops	▼
●	Red rated CRM VMS shops	▼
●	Black rated MS/VMS shops	◀▶
●	Non VMS observations	◀▶
●	Branch monitoring red ratings	◀▶
●	Home cancellations	◀▶
●	Travel cancellations	◀▶
●	Life cancellations	◀▶
●	Over 50s cancellations	◀▶
●	Branch sales - errors	◀▶
●	MS mandatory training	◀▶
●	CRM mandatory training	◀▶
●	T&D record checks	◀▶
●	On the job observations	◀▶
●	NPS results	◀▶
●	CES results	◀▶
●	Reportable incidents	◀▶

Key	
●	green
●	amber
●	red
●	not measured this month
◀▶	remained green
◀▶	remained amber
◀▶	remained red
▲	improved to green
▲	improved to amber
▼	fell to amber
▼	fell to red

Performance measured in January

Overall performance rating	Green rated KRIs	Amber rated KRIs	Red rated KRIs	KRIs not measured
AMBER	16	0	3	1

Based on the weighted culmative outcome of the KRIs we measured in September, the overall risk rating is AMBER.

This month we were within tolerance for 18 out of the 19 KRIs we measured. 16 of our KRIs were rated green, 0 of our KRIs was rated amber and 3 of our KRIs were rated red. In comparison with December there were no changes in the number of KPIs measured and achieved. In the last six months (August - January) we have averaged an achievement rate of 85.4% of the total KRIs measured within this period which results in an amber rating.



This month we were within tolerance for 11 out of the 13 KRIs we measured. 11 of our KRIs were rated green, 1 of our KRIs were rated amber and 1 of our KRIs were rated red. In comparison with August there was no change in the number of KPIs measured and achieved. In the last six months (April - September) we have averaged an achievement rate of 84.4% of the total KRIs measured within this period which results in an amber rating.

Key headlines and trends

Summary - January saw a deterioration in our key risk metrics. Of particular concern is the VMS scores. Whilst this relates to low volume, the failure rate is worrying and we should be seeing a higher level of monitoring given the volumes of transactions performed. The introduction of non-VMS observations should be key to providing this additional level of assurance.

POL00401626

Change Risk Update

Author: Jenny Ellwood Sponsor: Tim White Meeting date: 13 March 2018 (RCC)

Executive Summary

Context

This report provides an update on the delivery status of the Change Portfolio, the key risk themes under management and the risks we think RCC and ARC should have visibility of.

Questions addressed in this report

- What is the current change portfolio delivery status and key delivery challenges?
- What are the current top portfolio risks?
- What are the types of portfolio risks and how has this mix changed?

Conclusion

1. The project delivery and risk status (which is an amalgam of the status of individual programmes) remains 'Red' due to a number of contributing factors. In particular dDelivery challenges still remain in a number of Programmes these include Customer Hub, GDPR, Transaction Simplification, Mercury (HNGT lite) and Back Office Transformation.

2. The current portfolio risks which we consider should be given visibility at RCC and ARC are: i) GDPR: Contracts, ii) Late delivery of Change leading to increased costs and reduced benefits and iii) EUM effectiveness. There are currently **28** risks within the Portfolio. MI is shown as an Appendix.

3. The late delivery of change risk is also one of the group reported risks and work on this continues to be led by the newly formed Strategic Portfolio Office. The inaugural Investment Committee was held at the end of February. This is one of the first steps in improving the change process ensuring that where funding is allocated to change it is aligned to the Post Office Strategy and is given to the Programme in stages on proof of delivery of key milestones/agreed value.

4. At the moment the Portfolio holds a mix of portfolio-wide risks and some key Programme risks. The number of portfolio risks have seen a net increase of **+4** from November 2017. This is reflected in the current aggregated risk severity score of **260**. This score has been incrementally increasing since September.

Input Sought

The Committee is asked to note the slight deterioration of the portfolio risk position since the last ARC, the top risks being faced, how they are being managed and mitigated and to advise on any additional areas/topics that should also be taken forward.

POL00401626

The Report

What is the current delivery status of the Change Portfolio and key delivery challenges?

1. At the end of February 2018, the overall Post Office change portfolio status was 'Red'. There were 3 key programmes which reported Red from a risk dimension:
   - Customer Hub: as it continues negotiations with FRES around the development of APIs, the new Customer App and migrating existing customers on to this.
   - GDPR: as it continues to work towards reaching 'effective compliance' by end of May 2018' see paragraphs 4-7.
   - Transaction Simplification: there is a risk the programme continues its development work in the absence of an agreed negotiating position with RMG on receipt printer quality.

2. Discussions continue around our appetite to further reduce agents' pay and we are monitoring the following programmes:
   - Project Mercury: The proposition is being reviewed with Spar and there are a number of 'show stopping' restrictions which will require negotiation with RMG. In addition, the development of the APIs is taking longer and is more expensive than first thought. For this reason HNGT lite proposition is being reconsidered. The development work will not be wasted as it is core for HNGT.
   - Back Office Transformation: The programme is facing a number of delivery risks with both POLSAP migration and the Cash Processing work streams. Both of which were due to go live in June 2018 and under a full replan. Further details on the risk and the delay that POLSAP migration creates on DR Testing is provided in the IT risk update paper.
   - IT Networks: This programme is continuing to roll out the new networks and is targeted to reach 6,500 branches by the end of March. Despite the difficult weather conditions there hasn't been any major impact on the Network Migration/Branch Counter refresh schedule this week.

What are the top risks currently being managed within the Portfolio and what is the performance of risk management based on the mitigation plans?

3. There are currently **28** open risks being managed at a Portfolio level, a net increase of **+4** from the last time this was reported to ARC in November 2017. The current portfolio risks which we consider RCC and ARC should be given visibility of are: i) GDPR: Contracts, ii) Late delivery of Change leading to increased costs and reduced benefits and iii) EUM effectiveness:

General Data Protection Regulations (GDPR)

4. The GDPR comes in to force in May 2018. The Programme has from inception flagged that it was unlikely to achieve full compliance by May 2018. Instead the programme has taken a risk based approach to achieve 'effective compliance' which is defined as all new activity and remediation for existing high risk/priority activities will be completed. However, there is still much to do to reach 'effective compliance' by the commencement date of the legislation.

POL00401626

5. A number of our 3rd party suppliers, in their role as 'data processors', are now subject to increased accountabilities. Controllers need to understand who has access to their personal data and ensure appropriate due diligence is undertaken on suppliers, vendors and processors. This is a significant risk for Post Office owing to historic issues with contract management. Contracts with many suppliers do not contain appropriate governance provisions, even for existing data protection obligations. There is therefore a lack of shared understanding of processing responsibilities. In many cases documentation is not sufficient to comply with GDPR.

6. The GDPR Programme is addressing this using a risk based approach. A high level assessment has been done and an external legal firm has been appointed to work with business stakeholders and relevant 3rd parties to deliver compliance, based upon a graded and suitable risk based approach.

7. This approach is in line with the guidance the Programme has received from the Department of Culture, Media & Sport (DCMS) which sponsors the Information Commissioner's Office (ICO). The latter have also made a number of public statements stating that securing full regulatory compliance will be a long haul and preparations will be ongoing beyond May 2018. The ICO have emphasised that they will adopt a proportionate approach subject to organisations' self-reporting potential breaches, being able to demonstrate effective accountability arrangements are in place and, finally, proactively engaging with them to resolve issues. A recent survey from Deloitte indicated that overall, only 15% of organisations surveyed expect to be fully compliant by May 2018, with the majority instead targeting a risk-based, defensible position.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
GDPR Contract Risk	Risk that the GDPR programme cannot deliver what is defined as "Effective Compliance" by 5/2018 because of difficulties: • in establishing what the universe of 'material' and 'non material' contracts is, and to obtain all current versions, • that current controller to processor contracts do not provide sufficient governance of suppliers obligations • with a lack of up to date core documentation on the personal data suppliers process and lack of clarity of their processing responsibilities.	16 I/L: 4:4	• Validation of the 'material' contracts via GE • Validation of 'non-material' value contracts list via GE • P-Suite to include GDPR compliant clauses for new commercial agreements • Renegotiation of Existing contracts	Complete 15 March Complete Ongoing	12 I/L: 4:3

Late Delivery of the Change Plan

8. This update follows on from the update provided in January, where the root causes were highlighted. PA Consulting are continuing with their review of the way the Post Office manages change and is seeking to make, by the end of March 2018, recommendations for improvement. This includes developing mitigations to tackle these key root causes. Additionally, this work currently involves validating the design of the high-level target Change Operating Model (including the Strategic Portfolio Office), building a phased transition plan and identifying implementing and delivering Quick Wins.

POL00401626

9. A key component of the new approach is the creation of a Post Office Investment Committee (IC). This commenced in February and is chaired by Rob Houghton. Its purpose is to review and make investment decisions on both the in-flight and pipeline change initiatives. It will also have a role in making strategic interventions to in-flight work, as required.

10. PA have already made some suggestions around some low effort, high impact improvements, which include development of:
    - criteria to assess all new projects against, to determine the level of control that should be applied, depending upon size and complexity
    - a revised delivery framework application which is flexed for less complex programmes
    - clear and robust mandatory gate requirements,
    - improved / creation of best practice templates aligned to the delivery framework and gate requirements
    - a Delivery RACI and clarification of role requirements for key personnel, ensuring there is a common understanding of who does what, and when

11. The above recommendations are all key mitigations and will help reduce the late delivery risk. PA are also looking at providing Agile insight into the Target Operating Model deliverables. Change Risk and Assurance will develop an Agile assurance approach and plan which will be agreed with Internal Audit.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
Late Delivery of Change	Our change is delivered late, risking costs and benefits or has unintended consequence	15 I/L: 3:5	• Transfer the executive sponsor of change to Rob Houghton / Tim White • Implementation of a Strategic Portfolio Office (SPO) and recommend the Target Operating Model which should be in place. • Create a new Investment Committee – develop TOR, attendees, roles and responsibilities. • Develop a project prioritisation methodology, which prioritises those initiatives that contribute the most to the PO's strategy and financial objectives • Build a phased transition plan to implement the new strategic portfolio office and processes (including the introduction of an agile delivery and governance process).	Complete End Mar 18 Complete End-March 18 End-March 18	6 I/L: 2:3

Enhanced User Management (EUM)

12. To date the Programme have rolled out the new identity solution to 1700 branches, within current gating approval to go to 4000 branches. The current planning assumption is that the design enhancements approved at POL Board in January will be implemented in June, although the Fujitsu release date has not yet been confirmed. If Fujitsu and the programme do not hit the June slot, this will impact our ability to deploy the training controls in July as we need the system functionality to allow branches to regain access to Horizon in near real time once they have completed their training to avoid significant operational issues including unexpected branch closures. This risk is being carefully managed and we expect confirmation of the release date in March.

POL00401626

13. The main outstanding risk is the efficacy of data capture from branches as this is a manual process involving branch by branch data verification. Through close working with the Common Services programme, steps have been taken to improve the communication to branches, using memoview rather than letters as this is a more certain way to ensure the message is seen and read.

14. Additionally, a simpler data collection process using Horizon will be implemented in late March. The current mitigating action of collecting data from 500 branches per week to achieve 300 branches per week of clean data will continue. If the improvements lead to better response rates, this will inform our ability to achieve an improved beat rate, but this won't be known until April 2018 at the earliest. An independent assurance review is planned in March/April 2018 to test the confidence in this new data collection process as well as the progress made by Fujitsu ahead of a confirmed release slot.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
EUM	There is a risk that EUM does not perform as expected due to • being unable to collate accurate data from agents • POL staff/agents not having an individual email address which can be used to communicate logins and training information **(resolved)** • Agents not being able to access SuccessFactors via the internet/browser solution **(resolved in new design)** This all leads to our inability to address the key business goal, which is for POL to prove to its client that persons transacting on its behalf are suitably qualified and vetted.	**12** **I/L: 4:3**	• Liaise with Common Services programme regarding data capture. Agreed ramp up request of data to 500 branches and improvements in data capture process and alternative communication process. • Build Horizon/SF learning interface in EUM to enable both systems to be available for agents to complete their training. • Uplift Branch standards resources to support branch migration to using the new Smart IDs and securing training compliance.	Mar-May 18 Ongoing Ongoing	**9** **I/L: 3:3**

15. ARC also requested an update on the SuccessFactors Programme. Payroll went live in January 2018, and this has gone well, with no material over or under payments. The project is currently undertaking post go-live support, preparing for transition to BAU later in March 2018 and agreeing contractual 3rd line support with Accenture, who want unlimited liability in respect of TUPE cases. Hyper care arrangements are still in place and will remain until the knowledge transfer is completed.

16. The SuccessFactors project is now moving towards formal closure. However, there will remain some activities outstanding from the approved Risk Exception Notice, in relation to single sign-on and 'bring your own device'. A corporate solution to resolve these is targeting delivery in June 2018. Design documents have been produced and a supporting business case updated. The action owner confirms that although there will be significant progress made by this date, if not fully successful then access to SuccessFactors must be limited to Post Office corporate devices. This would mean that front line employees, for example, having to book annual leave/access payslips through their depot/branch manager's PC. There will also be multiple employees accessing their personal and sensitive data from a shared computer, which could give rise to additional risk of data leakage.

POL00401626

17. A full list of the **28** active portfolio risks is shown as an Appendix.

What are the types of portfolio risks and how has this mix changed?

18. In November 2017, there were **24** portfolio level risks (October 2017 data). This was the last time we formally reported on this data to ARC. The current total is **28** which has been subject to churn in that (since October 2017) **5** risks have been opened (GDPR contracts, DPO Bandwidth, HR SAP decommissioning, HNGx & New Receipt Printer and Late Delivery of Change) and **1** risk closed (Operational Impact of Generic Training Expiry Dates).

19. An illustration on how the mix of risks at portfolio level continues to flex and shows the open portfolio risks by severity is shown on the following page.

RAG Impact/Likelihood	Minor (1)	Moderate (2-4)	Major (5-11)	Significant (12-19)	Critical (20-25)	Total
February 18	0	4	14	10	0	28
January 18	0	4	13	10	0	27
December 17	0	4	13	10	0	27
November 17	0	4	12	8	0	24
% of total (current period)	0%	14%	50%	36%	0%	100%
Number of New Risks in last period						5
Number of Emerging Risks in last period						1
Number of Closed Risks in last period						1

Figure 1: Please note the minor/moderate risks are managed at a local level and not escalated to the Portfolio view.

POL00401626

Appendix: Change Portfolio risks, supporting metrics and mitigation plan dynamics

The Portfolio

	Risk Title	Nov ARC	Mar ARC	Grid Ranking CURRENT	Grid Ranking TARGET
1	GDPR Contracts		✓	16	12
2	Complex Portfolio Planning & IT Management	✓		16	8
3	HNGx & New Receipt Printer	✓		16	2
4	ISDN removal from Branch estate[1]			15	8
5	Late Delivery of Change		✓	15	6
6	DPO Bandwidth Risk			12	4
7	Delivery of elements of the Change Plan	✓	✓	12	9
8	EUM Effectiveness	✓	✓	12	9
9	IT Change Operating Model			12	8
10	Data Risk			12	8
11	GDPR			12	8
12	ITBNA Incumbent Supplier Proactive Engagement - BT			9	4
13	IT Vendor Renegotiations			9	9
14	IT Delivery Capability			9	6

[1] To be closed in the next reporting cycle

POL00401626

	Risk Title	Nov ARC	Mar ARC	Grid Ranking CURRENT	Grid Ranking TARGET
15	Unintended consequences on Operational Performance - Process			9	6
16	Adverse Impact of Change/ Organisational Change on Agents			9	6
17	Accounting & Reconciliation			8	8
18	Financial risk - Benefits/Revenue Realisation			8	6
19	Availability of Key Skills and Knowledge			6	6
20	Responsible use of public funds			6	1
21	Strategy & Design: Conflict between current BaU and Transformation activities			6	3
22	Reputational Damage - Media risk			6	4
23	Reputational Damage - Political stakeholder risk (local government)			6	4
24	Decommission of HR SAP			5	1
25	Deployment of Non-Compliant Solutions/Systems - (Breach of LRC reqts)			4	4
26	Reputational Damage - Political stakeholder risk (national government)			4	4
27	Poor coordination of change communications with stakeholders and employees			4	4
28	Model Office Testing Capacity/ Resilience			3	2

POL00401626

The Churn

The table below details the number of risks open and closed over the last rolling 12 months.



Figure 2: A comparison of open/closed risks (by month)

Risk Weighting

Each portfolio risk has a weighting score calculated by multiplying their impact/probability scores. When added together this provides a cumulative portfolio score which currently stands at **260**.

The overall risk severity has oscillated since February 2017 when it was **18**% than it is now albeit it has been incrementally increasing since September 2017. The risks continue to be monitored in line with the change portfolio risk review process.

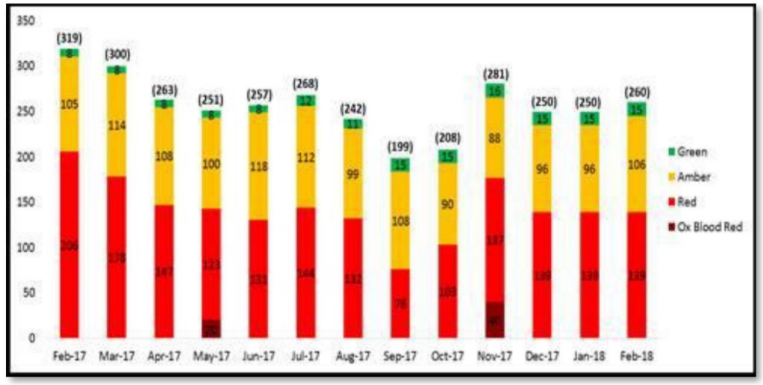


Figure 3: Current cumulative portfolio risk weighting score by month

Figures 4 and 5 illustrate the anticipated impact of a reduction in the number of active risks over the next 6 months will have on the residual risk weighting.

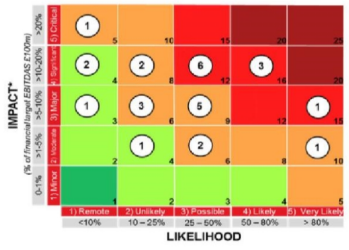


Figure 4: Current portfolio risk weighing (Feb 2018)

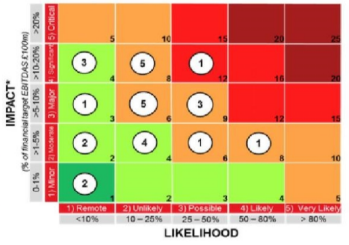


Figure 5: Target portfolio risk weighting (Feb 2018)

POL00401626

Financial Crime Risk Update

Author: Sally Smith | Sponsor: Jane MacLeod | Meeting Date: 13th March 2018

Executive Summary

Context

This paper updates the Risk and Compliance Committee on financial crime risks relating to Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) and Anti-Bribery and Corruption and compliance with The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 and The Terrorism Act 2000.

Questions this paper addresses

- What are the key AML and CTF risks within Post Office Ltd and are there any significant gaps or weaknesses in the Post Office's compliance with its regulatory obligations under the Money Laundering Regulations (MLRs)?
- What is the current position with the post HMRC Audit Bureau de Change remediation project
- What is the current position with financial crime risk assessments.
- Are the minimum control standards in the Post Office's Anti-Bribery and Corruption and Whistleblowing Policies being effectively applied?

Conclusion

1. The project team are progressing with the work needed to comply with the new Fit & Proper requirements, but there is still significant work to meet the June 2018 deadline and to ensure that the ongoing framework is robust.
2. There have been further delays with the Bureau de Change remediation projects with implementation of the data warehouse solution pushed back to the beginning of March, meaning that the new reports have not yet been built and tested. The eKYC, PEPs and Sanctions solution is progressing for April implementation, however, HMRC have now verbally advised that our interim solution for cash transactions over £2k is not acceptable, and we are due to meet with them on 12th March to discuss.
3. Risk assessment work continues, although there are a number of new or updated Product Information Packs that remain outstanding, and these are being chased.
4. There have been no issues with Gifts & Hospitality reporting since the communication in January. The volume of Whistleblowing reports received via various channels has increased, although further communication and awareness activities are planned throughout 2018.

POL00401626

Input Sought

The R&CC is asked to review this report and consider whether further actions should be undertaken.

The Report

Compliance with MLRs

5. The pre-penalty notice in respect of Regulations 19 and 20 relating to the Bureau de Change product was received on the 8th January 2018 for the sum of £344,766 and this has been paid.

6. Annual training content for Network and back office staff is being drafted and is due to be delivered 4th – 30th May 2018. There are still 4 branches that have not completed their training from last year and second remedy letters have been sent to them. If they still remain non-compliant, the contracts team will need to escalate.

7. We continue to liaise with HMRC on the new Fit & Proper tests, and have sent them an initial data set split out by Multiples, Sole Trader Agents, Limited Company Agents, and direct employees who are now captured. There is significant work still to do to complete the gaps in data, especially the identification of Directors and Beneficial owners. Other activity that needs to be completed includes documenting the policy and processes to cover on-boarding and periodic vetting/self-declarations, training and defining events that would require fit and proper status to be reviewed.

8. HMRC have written to all Large Traders at the end of February to emphasise that the deadline for responses with the information they require is the 25th June 2018 (i.e. one year after the new regulations came into force). Whilst Post Office will have identified all individuals that are subject to the Fit & Proper regime, there will still be gaps in some of the data fields as these are obtained from agents, directors and beneficial owners. Our HMRC supervisor has indicated that this is acceptable, but we will raise again with them when we meet in March.

9. Non-conformance issues in the Network in January and February 2018 included 38 incidents identified at 38 branches.
    - 17 branches identified were Directly Managed Branches and/or WH Smith Multiples and these have been addressed by the Financial Crime Team and escalated to Network as appropriate. A number of these instances relate to breaches that we deem 'unavoidable' – i.e. not the same clerk, day or time that the customer is transacting.
    - 15 branches remain on the non-conformance watchlist following the new ID thresholds and are manually monitored monthly.
    - 1 new branch was added, and none were removed.

10. The volumes of suspicious activity reports (SARs) have increased slightly in January and February 2018. The increase volume on internal SARs submitted by the AML team has contributed to this rise in overall SARs, these predominantly are in relation to Bureau de Change.

POL00401626

11. The Financial Crime Team were previously concerned that SARs in relation to MoneyGram and potential vulnerable customers had decreased since the introduction of MoneyGram's new ID capture portal, and this was resulting in branches assuming transactions were genuine because the customer was still willing to complete the transaction. In January and February we have seen a steady increase in SARs relating to this issue and the Financial Crime Team have planned communications to increase the networks awareness.

Bureau de Change remediation project status

12. HMRC have responded verbally to the letter sent in January setting out our approach for transactions over £2000. Whilst they accept that for transactions paid by card the proposal is sufficient, they have stated that our proposal for cash transactions, whereby the clerk will need to confirm on Horizon that the photo ID and the customer are the same individual, is in breach of regulation 40, which requires us to retain a copy of the ID.

13. They have requested a meeting with us to discuss, which is scheduled for the 12th March. We are taking further legal advice on the regulations and looking at what options may be available to avoid the need to retain copy documentation.

14. The eKYC, PEPs and Sanctions capability has progressed to testing and should be live in April, but the exact date is yet to be determined. Post Office have been advised that the Government Document Checking Service cannot be used for one-off transactions, only where re-usable credentials are established, so this element cannot be applied until the new Customer Hub and Identity service is achieved later in 2018.

15. The new data warehouse delivery has slipped but is due to go live week commencing 5th March. The new reports can then be built and tested, and HMRC are due to review these in Chesterfield on 21st March. The reports cannot be finalised until the PEPs and Sanctions checking goes live. Once the new reports have been built, the operational team in Chesterfield will need to parallel run against the current report to ensure they are working.

Financial Crime Risk Assessment

16. Work on risk assessment continues as BAU, and Appendix A gives full updates on the status of Product Information Pack completion and re-assessment work. Completion of the Banking Framework Services Product Information Packs is critical if the risk assessment work is to meet the end of March deadline from the recent Internal Audit report.

17. We have identified managers within Retail and Financial Services & Telecoms that require financial crime risk assessment training, and will be looking to roll out sessions in the new financial year.

18. As part of the work the Risk team are doing on the Risk and Controls Matrix, we are piloting a methodology to ensure that there is appropriate oversight of financial crime as a principal business risk.

Anti-Bribery and Corruption (ABC) update

13. Following further communications sent out in January after the Oct-Dec quarterly report, there have not been any significant issues identified in Gifts & Hospitality reporting. However, an issue was identified with the new

POL00401626

expenses tool relating to the 'external entertainment' category, and this now references that any external entertainment claimed must have been reported and approved via the Gifts & Hospitality Tool. A quarterly review of entertainment expenses data is going to be compared against the central Gifts & hospitality register from the end of the current quarter.

Whistleblowing update

14. The volume of Whistleblowing reports is improving, and further regular communications are planned for 2018.

15. 13 reports were received between January and February, and 11 of these named a Post Office branch. 6 were classified as fraud and 1 as money laundering. The majority of Fraud reports were submitted via Grapevine or the Speak Up line and were in relation to theft carried out by a Postmaster, Agent Assistant or an employee. 2 reports alleged thefts from vulnerable customers. All reports are investigated with recommendations made and followed up

Regulatory updates

16. The update relating to the Fifth Money Laundering Directive in the January report remains current.

17. The new Sanctions and Anti-Money Laundering Bill introduced on 18th October 2017 has been reviewed. There are two key areas it is designed to address:

    - enable the UK to continue to implement United Nations (UN) sanctions regimes and to use sanctions to meet national security and foreign policy objectives; and
    - enable anti-money laundering and counter-terrorist financing measures to be kept up to date, helping to protect the security and prosperity of the UK and continue to align the UK with international standards

    There are no significant impacts for Post Office.

18. Following the National Risk Assessment that was published at the end of October 2017, HMRC has published a review of anti-money laundering compliance in money service businesses (MSBs). This is mostly aimed at money transmitters operating via an agency model, but covers some generic areas. The review identified good practices to assist with a risk-based approach and reduce vulnerability. The document has been reviewed and there are no significant areas that impact Post Office business.

External threats

19. There have been no new issues since the January 2018 report.

POL00401626

Appendix A

Risk Assessment and Product Information Pack update

Due for reassessment in the next two months

Product/Service	PIP initially received	PIP due for review and update	Month FCT will re-assess risk	RAG status	Comments
Gift Cards	July 17	July	September	RED	Following an incident in October 2017 the PIP needs to be updated
Bill Payments	October 17	October	December	RED	Following an incident in October 2017 the PIP needs to be updated
Postal Orders	April 17	April	June	Not yet due	
Travel Insurance	May 17	May	July	Not yet due	
Business Insurance	May 17	May	July	Not yet due	
Home Insurance	May 17	May	July	Not yet due	
Car Insurance	May 17	May	July	Not yet due	
Motorcycle Insurance	May 17	May	July	Not yet due	
Van Insurance	May 17	May	July	Not yet due	
Pet Insurance	May 17	May	July	Not yet due	
Drop & Go	May 17	May	July	Not yet due	

Due from November 2017 Product Manager Workshop

Product/Service	Month PIP Due	Completed PIP received?	Month FCT scheduled to re-assess residual risk	RAG status	Comments
Partner Banking Framework	February	No	March	RED	PIP has not been received to date. This will cause the audit action risk assessment to be delayed
Identity Services	March	No	May	Due March	Draft has been received and reviewed. Awaiting amendments.
Savings Products	March	No	May	Due March	Draft has been received. Awaiting review
Credit Card Products	March	No	May	Due March	
Pre-Paid Cards	March	No	May	Due March	
Mortgages	March	No	May	Due March	

POL00401626

Product/Service	Month PIP Due	Completed PIP received?	Month FCT scheduled to re-assess residual risk	RAG status	Comments
Loans	March	No	May	Due March	
Life Insurance Products	March	No	May	Due March	Draft has been received and reviewed. Awaiting amendments.
Telecommunications products	March	No	May	Due March	
National Lottery	March	No	May	Due March	

POL00401626



Identification and Management of Risk :Gift Card

Keith Maple

March 2018

POL00401626

Situation at the end of 2016 indicated high risk and lack of control

Initial Financial Crime Risk assessment completed in September 2016 concluded high residual risk (10.24) and a control rating of only 14%

WHY?

- No evidence to show the product was effectively managed
- No immediate evidence of a signed contract
- No evidenced or demonstrable understanding of contract obligations or evidence that POL were complying with financial crime policies and applicable legislation OR if POL needed to be registered with the FCA
- Nothing that provided an overview of the risks to which POL could be exposed
- No framework for enabling the effective management of Gift Card
- No evidence of branch training being required or executed
- No evidence of monitoring of possible fraud

POL00401626

Gift Cards do have inherent risks

- The product is Anonymous
- The product can be bought with cash which increases the anonymity
- They can be sold to commercial customers

BUT

Something needed to be done to reduce the risks that could be addressed

The conduit for the solution was the completion of a **Product Information Pack** to;

- outline Gift Card's risks, processes, obligations and procedures
- provide an overview of the risks to which Post Office Ltd might be exposed
- provide the framework to enable the effective management of Gift Card

POL00401626

June 2017 risk has been reduced from high to moderate with control of risk at 75%

Financial Crime Risk Reassessment completed in June 2017 produced a reduction in residual risk from 10.24 to 3.04 **moving from high to moderate risk**

WHY?

- Thistle worked with Legal, Risk and Governance and the POL Gift Card Product Manager to ensure the necessary controls are in place to mitigate the risk of financial crime. The framework for this is the Completed Product Information pack
- Contractual obligations and POLS contractual position were clarified and understood and confirmation that POL, as a distributor for GVS, are not required to be registered with the FCA
- Recognition that Postmasters are required to follow the overarching POL polices to report suspicious behaviour, AML etc. Training uses Gift Card examples including purchases of multiple cards.
- Confirmation that GVS have procedures in place to detect fraud including being able to block cards. This is supplemented by POL Financial Crime analysing reports of sales by branch and acting on "suspicious" behaviour

POL00401626

June 2017 until now

- The Financial Crime Team have honed their analysis to pinpoint possible irregular behaviours in branches and have investigated, actioned and in some circumstances helped to re-educate staff in branches
- There is a greater understanding of the features of the product, its flows and the contextual and contractual arrangements and obligations within the Product Team. There is also a closer relationship with GVS after going through the Product Information Pack process
- It has been highlighted by GVS that, that in some circumstances, the cards can be reloaded. Early investigations indicate that though this should not happen at all the incidence is very low. GVS and POL are currently working on a remediation plan
- One lesson learned from this is that if the Product Information Pack had been developed at the inception of the product over 10 years ago then any subsequent 'Memory loss' may have been avoided as the product ownership changed hands .

POL00401626

IT Risk Update

Author: Rebecca Barker Sponsor: Rob Houghton Meeting date: 13th March 2018

Executive Summary

Context

This report provides updates on the IT Risk landscape within Post Office; the key projects within the IT risk area; and details on the remediation activities for the risks identified as outside our risk tolerance.

Questions addressed in this report

1) What is the current IT Risk Landscape?
2) What is the existing progress of the remediation activities planned for the risks outside of the Risk Tolerance?
3) What is the progress against the key activities in Risk Management?

Conclusion

We remain outside our risk appetite in key operational areas, especially the Fujitsu supported infrastructure estate. However infrastructure related change programmes intended to reduce these risks over time are in progress.

The Branch Network refresh project, which will address the risk to replace ageing kit and move from Fujitsu to Verizon is on schedule to complete by the 31st March 2018. Despite the difficult weather conditions there hasn't been any major impact on the Network Migration/Branch Counter refresh schedule.

Following delays within the Cash Management Processing project, POLSAP Migration is now planned for 1st September 2018. This revised date impacts our DR programme, and our Fujitsu failover test needs re-planning (originally planned for August), as the risk is too high to perform the failover whilst POLSAP remains in operation on the existing Fujitsu infrastructure. We need to assess when the Failover test can be planned with minimal impact to service.

We continue to reduce and mitigate the risk of cyber-attacks and security breaches with the Security Operations Centre (SOC) programme. DDoS protection is live, protecting our website service. Firewall assurance is live, improving our understanding of our security perimeter and allowing us to reduce the risk of attacks. Certificate management is in progress, and once fully operational, this SOC component will remediate Certificate Management risks.

An improvement plan is in progress to reduce the risk of loss of service to Swindon stores: the activities over the next four weeks will focus on improving Disaster Recovery plans and increasing the support wrap provided by our Suppliers.

Input Sought

The RCC is requested to note the progress made, and provide feedback on the report.

Strictly Confidential

POL00401626

The Report

What is the current IT Risk Landscape?

1. At the end of February 2018 there are currently 52 open risks being managed within IT, this has increased slightly from January, this is as a result of improved risk insight with our suppliers. No known risks have materialised to issues. Six risks remain outside our risk tolerance and are detailed in section 3 (see also Appendix 1 for the high level tube map).
2. The number of risks outside tolerance is reducing over time, and IT are running key programmes which will mitigate our overall risk and bring us within risk appetite, these include;
    - Horizon Data Centre Refresh (HDCR): The HDCR Programme is moving applications off very old infrastructure onto new. We are currently testing all Banking and Payment services interfaces for the Banking and Payment services migration in Q1 2018. All business critical migrations will be completed by Q1 2018. The programme will complete in Q2.
    - Branch Network Refresh: 9,393 branches have migrated. Work continues with Verizon to improve the Verizon secondary service, ensuring that the strongest secondary connection is prioritised. Migration is still on course to complete by end March 2018.
    - SOC (Security Operations Centre): Firewall Assurance Service is live, covering the four major tower providers which represents over 85% of the current estate. The Security Incident & Event Monitoring (SIEM) service will be in place for the four major towers, starting from end April 2018. Improved Certificate Management is currently being introduced, increasing secure trusted connections to be electronically established. Risk and controls functionality will be provided via the Archer platform scheduled to be in place by end March 2018. SOC is on plan to be fully commissioned from July 2018 when Verizon will take on operational management.
    - DDoS (Distributed Denial of Service attacks): There have been no DDoS attacks since end November. For increased protection, a proof of concept of a DDoS protection product, Distil, has been initiated and is protecting the live website today. The output and level of protection afforded will be reviewed throughout March to determine ongoing requirements.
    - BYOD (Bring Your Own Device): BYOD will be materially rolled out by the end of March. All obsolete Windows mobiles phones need to be replaced and this will occur by end April, enabling the protected service to be fully adopted. The closure of exposure of non-corporate devices requires a multi-layered approach and as such requires significant communications to colleagues to ensure they understand differences in business behaviours. Office 365 lockdown will be end April once we have replaced the windows phone estate.
    - Horizon Counter Refresh: Branch counter transition stretch target for exit of HNGX is Aug-18 (commercial deadline is 31/3/19). Working with Computacenter (and other partners) to agree plan to accelerate delivery to meet this target. The programme is now rolling out the new Epsom 7200 slip and receipt printer, which we expect will reduce the volume of calls regarding printer failures and improve service availability.

POL00401626

- IT Disaster Recovery: The DR Framework and IT DR policy target sign date is 13/03/2018, planning for 2018 DR testing is well progressed. Monthly IT Service Continuity Meetings are in place. Recovery Time (RTO) and Recovery Point Objectives (RPO) have been documented for Computacenter, Verizon and Accenture. We expect to complete documentation of RTO and RPO's for all Tier 1 suppliers by 23rd March. This will allow us to meet our commitment in closing the actions with the PWC Banking Framework Audit by the 31/03/2018.
- Cyber Security Vulnerability: A new zero day chip vulnerability known as Spectre or Meltdown exists affecting all chips in computer systems. We review our position against these vulnerabilities regularly and have applied protective patching where available. There are no known publicly exploits of this vulnerability that require remediation, however we continue to be vigilant and to patch all our environments to the latest security levels to ensure we are protected. There have been no major IT Security incidents since December 2017 on our estate.

How are the remediation activities progressing for the risks outside tolerance?

3. The risks below are currently sitting outside risk tolerance; with the potential to significantly impact service availability, compliance, regulatory requirements.

- POLSAP
- Horizon Datacentre Failover
- GDPR
- PCI
- Stock Services
- Accenture Resilience

4. POLSAP: POLSAP Services will be migrated by September, this date has moved from June due to delays in the migration of Cash Processing. Additional hardware blades have been purchased to mitigate risks. The revised date of September will probably result in the Fujitsu Failover Test being postponed from the August bank holiday. (See point 5 for additional information).

Risk Title	Risk	Curr. RAG	Mitigation Plan	Due date	Target RAG
POLSAP Legacy Systems	Failure to ensure all components are fully supported by the appropriate levels of adequate technology, hardware, whilst programme activities are in progress, may lead to a loss of service within Supply Chain and Finance Teams, resulting in service unavailability, financial loss, reputational damage and Security Vulnerabilities.	20 I/L 5:4	1. POLSAP Processes migrated to core finance. 2. Cash Processes migration to Belfast. 3. POLSAP Hosting Contract Extension – period April 1st to December 31st 2018. 4. IPSEC Tunnel Failover – Exploring MSEG options with Verizon. – REN has been raised. 5. Network Upgrade to core final planning stages. Fujitsu have confirmed that Tests plans are underway. The Live dates are being planned. Data Centre work	1.01/09/2018 2 19/03/2018 3.31/03/2018 4.Ongoing 5.In progress	9 I/L 3:3

POL00401626

Risk Title	Risk	Curr. RAG	Mitigation Plan	Due date	Target RAG
			and the network is in progress. 6. SAP Application Support 7. Reviewing the purchase of 2 additional blades for additional contingency.	 6.Complete 7.Complete	

5. Horizon Datacentre Failover Test: As a result of the new migration date of September for POLSAP, the Fujitsu failover test needs re-planning (originally planned for August), as the risk is too high to perform the failover whilst POLSAP remains in operation on the existing Fujitsu infrastructure. We need to assess when the Failover test can be rescheduled with minimal impact to service.

Risk Title	Risk	Curr. RAG	Mitigation Plan	Due date	Target RAG
Horizon Datacentre Failover Test	Failure by Post Office IT to ensure that a full Disaster recovery test is carried out on a regular basis in line with contractual agreements, may lead to being unable to restore primary servers and services not being restored in a real outage. Resulting in financial losses, reputational damage, and prolonged service interruption.	20 I/L 5:4	1. Ensure that component testing that does not impact the delivery of POLSAP or Horizon Datacentre refresh continues to as planned, this is supported by the DR Framework. 2. Planning in place to support the Full Datacentre refresh takes place in August. First session complete 3. March Planning session – assess when the revised Fujitsu failover can take place.	1.Ongoing 2.In progress 3.w/c 26/03/2018	9 I/L 3:3

6. GDPR: A GDPR programme is in flight, supported by the IT Team. The programme team will provide a comprehensive GDPR update to RCC.

Risk Title	Risk	Curr. RAG	Mitigation Plan	Due date	Target RAG
GDPR	Failure by POL IT to communicate the expectations of GDPR to projects and programmes may lead to products and services being prevented or being delayed from launching, Resulting in delays to operational activity, financial loss and reputational damage.	16 I/L 4:4	To be updated by GDPR team in a separate paper to RCC		8 I/L 4:2

7. PCI Compliance: Engagement is ongoing between the IT Security Team, IPA, IT Risk Management and Vendor Management. We are working closely with Computacentre and Fujitsu to mitigate risks to PCI compliance.

POL00401626

Risk Title	Risk	Curr. RAG	Mitigation Plan	Due date	Target RAG
PCI Compliance	Failure by Post Office to ensure operational activities, IT infrastructure/security and related services are PCIDSS compliant may cause challenges during external audit, require significant remediation activities and attract unbudgeted costs. This may result in a failure to obtain the required certification, breach our agreed banking framework and may lead to a legal/regulatory breach, financial loss and reputational damage	16 I/L 4:4	To be updated by IPA and Payments team in a separate paper to RCC		8 I/L 4:2

8. Stock Services: Swindon Stores are running on an obsolete platform that has limited levels of support in place. Furthermore, robust Disaster recovery processes are not in place and the restoration of any service incidents heavily relies on a single individual within Swindon stores to resolve. The impact of an outage to Swindon Stores not only impacts our estate but the service provided to Royal Mint, DVLA and Royal Mail.

Risk Title	Risk	Curr. RAG	Mitigation Plan	Due date	Target RAG
Stock Services	Failure to ensure all components are fully supported by the appropriate levels of adequate technology, hardware, whilst programme activities are in progress, may lead to a loss of service within Supply Chain and Finance Teams, resulting in service unavailability, financial loss, reputational damage and Security Vulnerabilities.	16 I/L 4:4	1. Business paper submitted to suppliers to request a cost effective proposal for support of: • Infrastructure, Operating systems and Oracle Databases. • Remediation plan to be delivered within 4 weeks of service take over and covering - weak areas of support, reduction in risk, improved, ITSCM/DR , Virtualisation and hosting of the FTP/Reporting Server (Business Objects) and hosting, Alternative solutions for support of the primary service 2. Data Cabling – assessment of site and bring up to standard. 3. Proposal from ATOS to ensure the services and suppliers are integrated with ATOS Incident Management and Change Management processes. 4. Swindon Staff to ensure all issues with PC's and printers	1. 12th March 2.19th March 3.19/03/2018 4.w/c 05/03/2018	8 I/L 4:2

POL00401626

			are reported to the service desk to clear the backlog 5. Review on supporting applications: Galaxy, WCS, Mercia and Capricorn 6. Strategic decision on direction for Swindon Stock Centre	5.w/c 26/03/2018 6.In-progress	

9. Accenture Datacentre Resilience: Verizon are now delivering network services to the Post Office. Verizon provide a pair of resilient connections connecting Accenture Datacentres, Hoff and Kronberg. The last mile into the Datacentres is connected via a single fibre connection. In the event of a disaster, the recovery process is manual and the downtime is unknown. The impact of such an event has increased following the migration of Credence and MDM. Further Services will also be migrated to Accenture over the next 6 months thus increasing the impact.

Risk Title	Risk	Curr. RAG	Mitigation Plan	Due date	Target RAG
Accenture Datacentre Resilience	Failure to ensure adequate infrastructure to support failover of the Core finance systems. Resulting in financial losses, loss of services and reputational damage.	16 I/L 4:4	1. Change request has been submitted to Verizon. 2. Review Verizon Response. 3. Solution to be implemented.	1. w/c 05/03/18 2. date to be confirmed. 3. date to be confirmed	8 I/L 4:2

What is the progress against key activities in IT Risk Management?

10. IT Controls Framework (ITCF): Positive engagement with Control Owners with a high response rate to their self-assessments of the controls due for the month of Jan and Feb 2018 respectively. Control testing is in progress and will be complete on the agreed date 16 March 2018. A number of controls are due for assessment in April and will be tested upon submission. IT will complete 100% test of controls for Tranche 1 by the 1st May. The project team are engaged with the Internal Audit team who are supporting the ITCF programme by carrying out a sense check of several complete controls and will provide informal feedback.
11. IT Risk Transformation: An IT Risk Transformation programme has been established to improve our capability maturity. This includes improvements in risk awareness, IT Risk reporting, and supplier risk management. The IT Controls' Framework implementation to improve control across the IT landscape is in self-assessment phase and on target to finish by end of F17/18.

POL00401626

Next Steps

- Informal testing of 6-10 controls from the ITCF to be carried out in March/April to align with the next RCC update in May.
- High level plan to be submitted to ITLB (IT Leadership Board) w/c 12th March for Tranche 2 of the IT Controls Framework.
- Planning session to be held w/c 26th March with Fujitsu to assess a rescheduled date for Fujitsu Failover.
- Workshop to be held with Change Portfolio Programme to formalise process on risks being transferred to live w/c 19th March 2018.

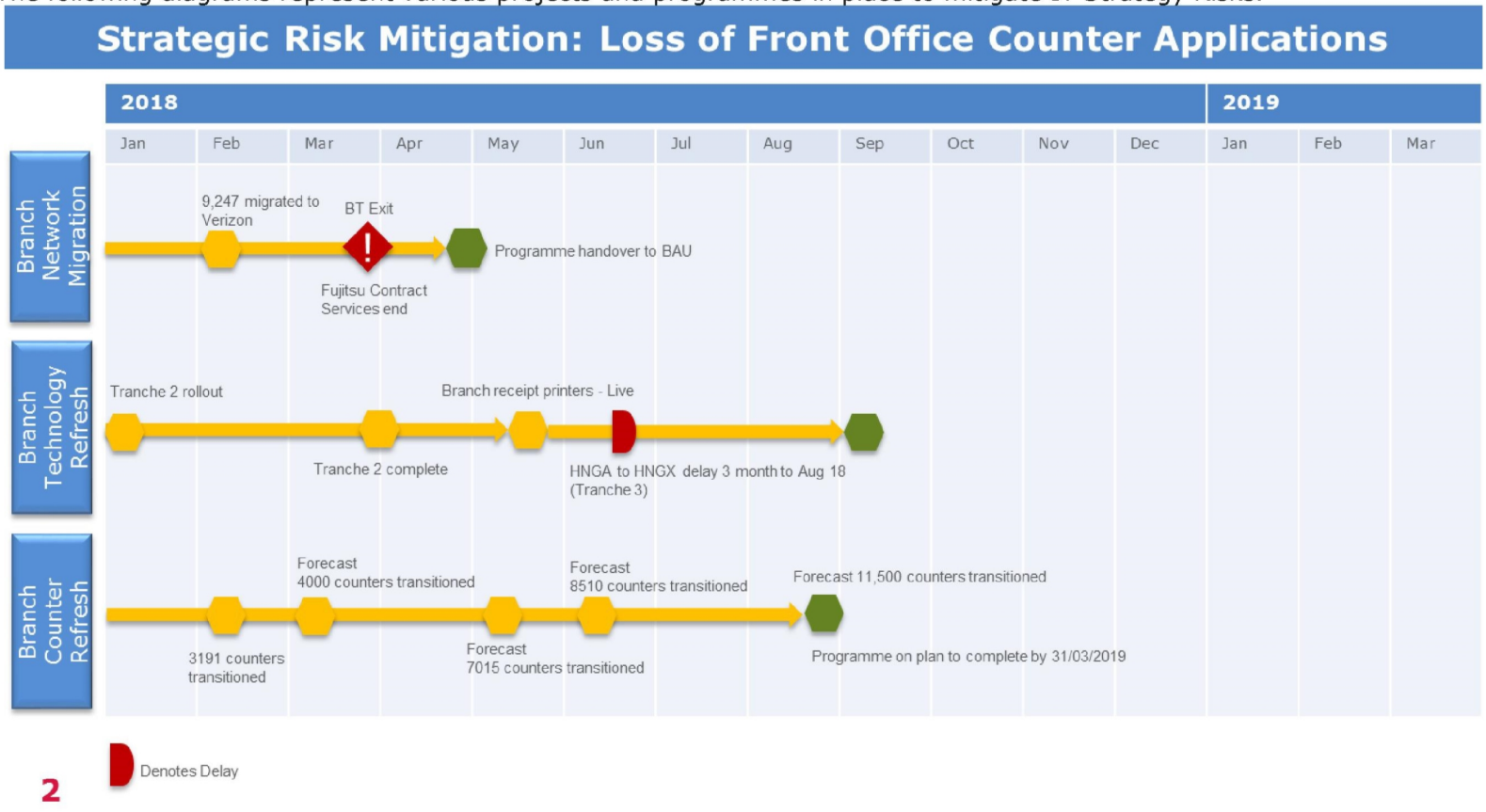
Strictly Confidential

POL00401626

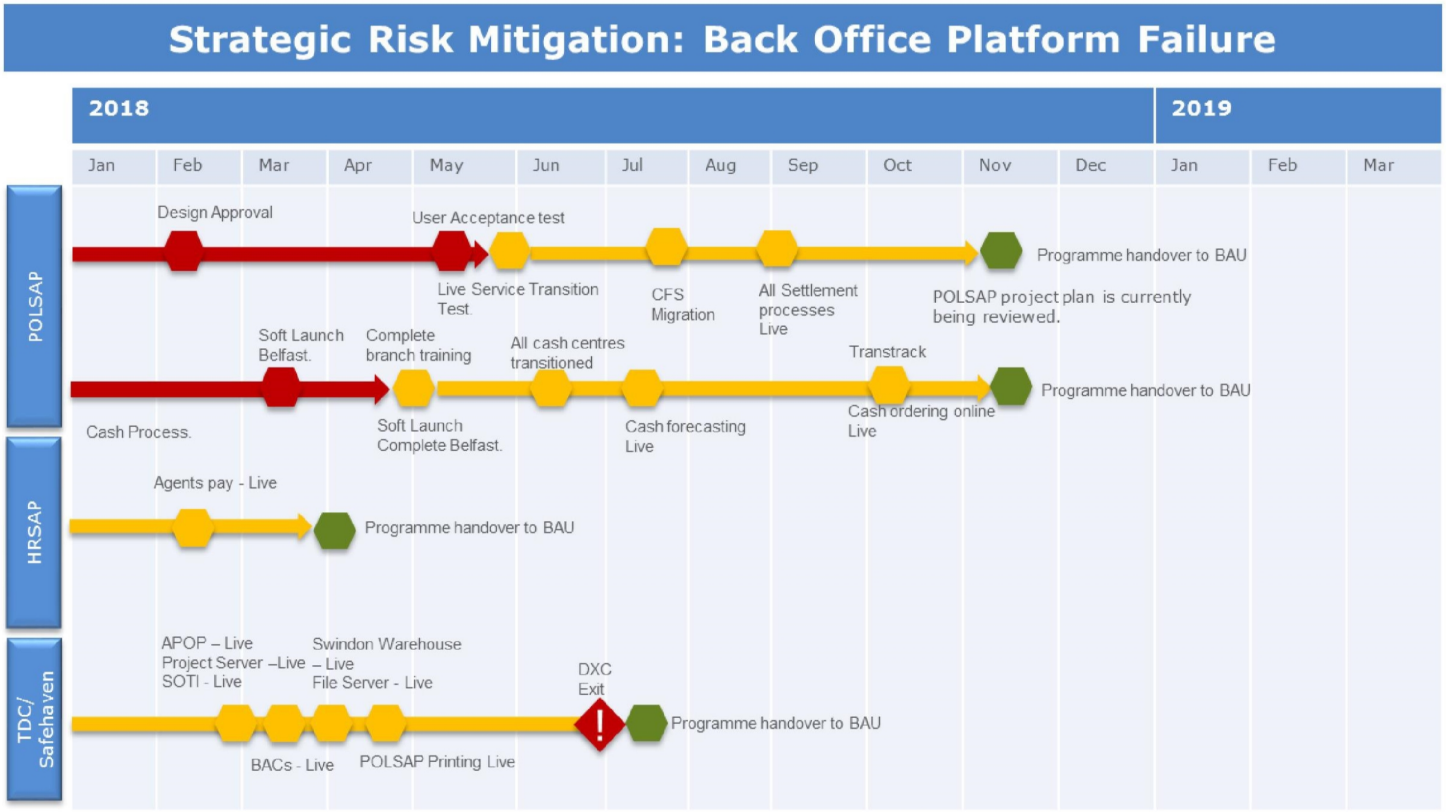
Appendix 1: Risk Tube Map

** updated 20th February 2018*

The following diagrams represent various projects and programmes in place to mitigate IT Strategy Risks.



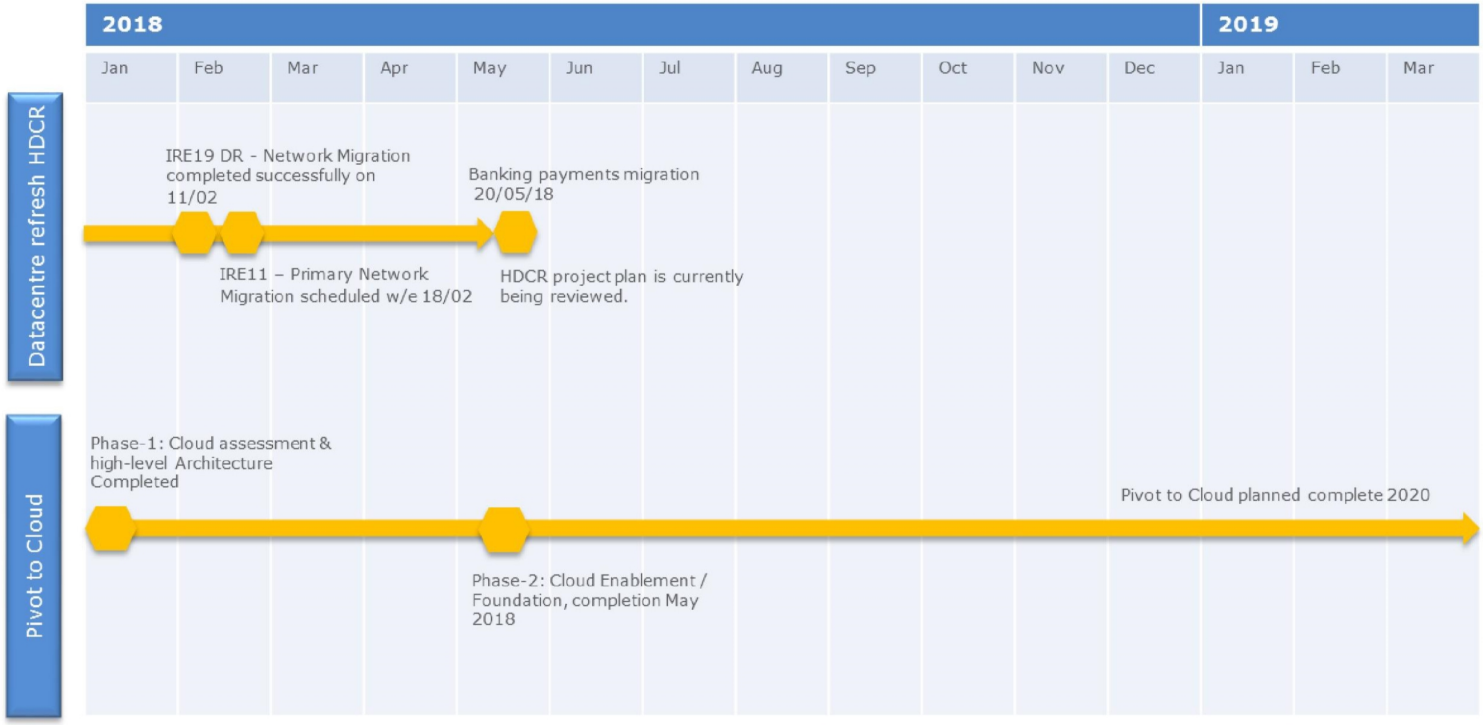
POL00401626



3 NB Credence/MDM Live – Programme Handover 31/03/2018
Swindon Risk Assessment is in progress and will be visible on the Risk Tube map in March

POL00401626

Strategic Risk Mitigation: Horizon Platform Failure

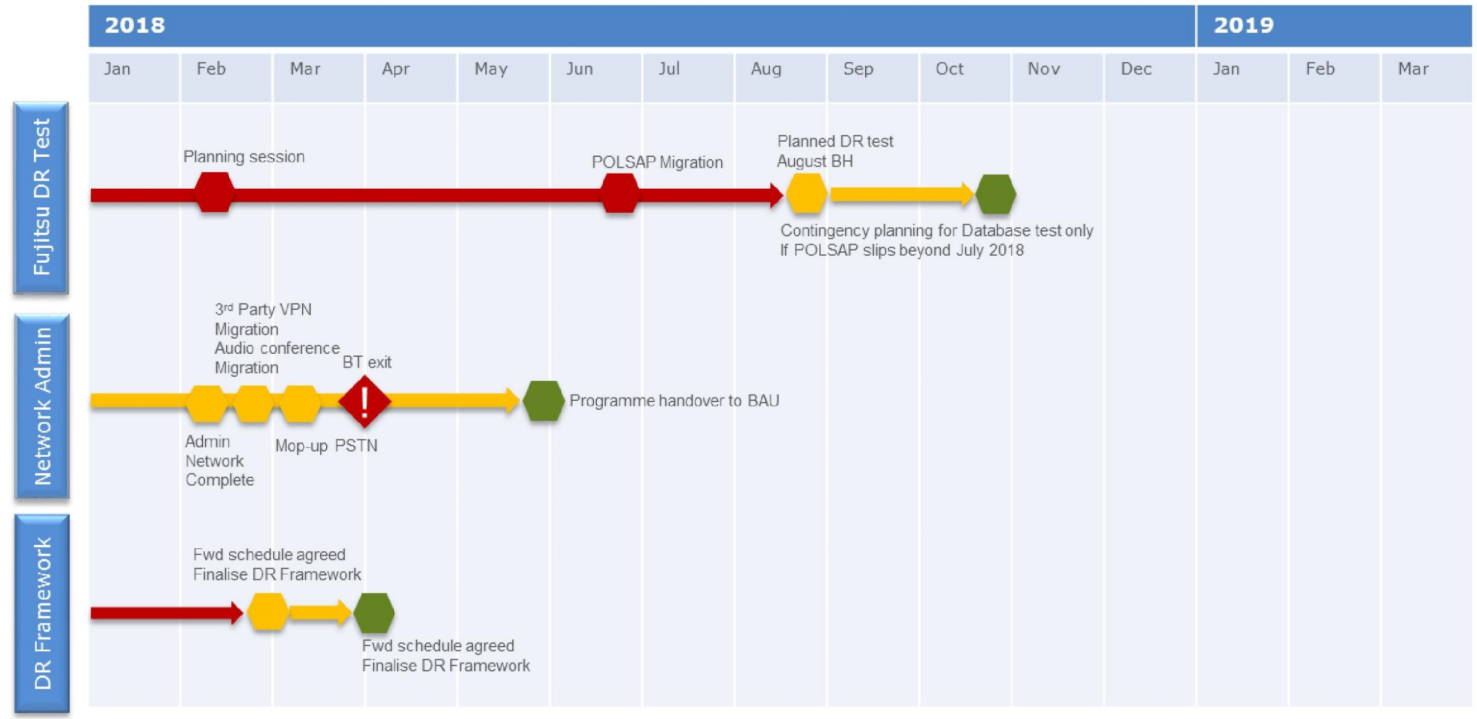


4

Strictly Confidential

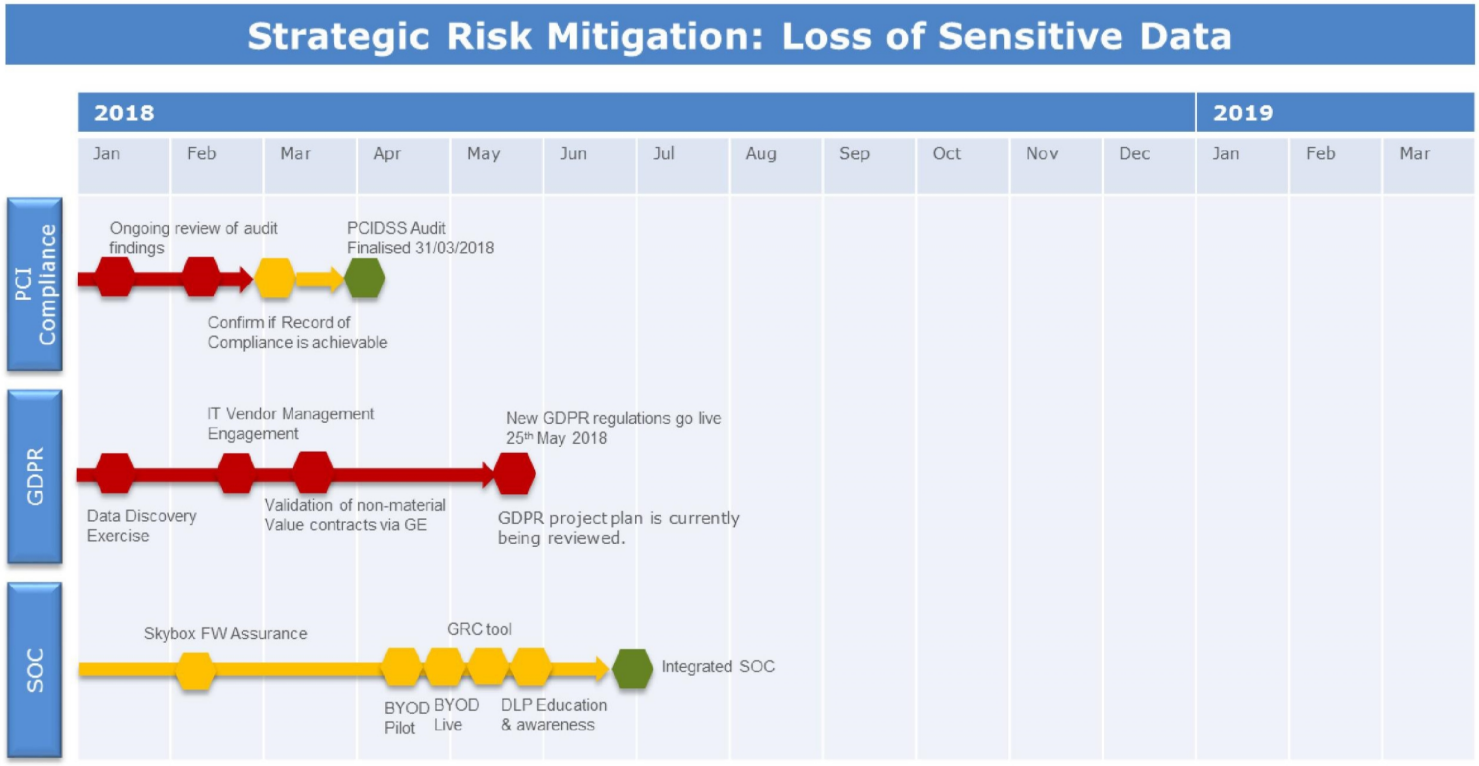
POL00401626

Strategic Risk Mitigation: IT Availability/Ability to Trade



5

POL00401626



Strictly Confidential

POL00401626

Cyber Security and Information Assurance Update Paper

Authors: Mick Ebsworth/Jules Harris Sponsor: Rob Houghton/Jane Macleod Meeting date: 13 March 2018

Executive Summary

Context

In order to discharge its duties, the Board and Audit and Risk Committee (ARC) request regular updates on cyber and data security risk.

This report is to provide an update on CSIA to Risk and Compliance Committee (RCC) and for onward communication to Audit and Risk Committee (ARC).

Questions this paper addresses

- What are the current top risks to Post Office (PO) from an Information Security and Cyber-perspective?
- How would we know if the risk has materialised?
- What is the current status of the remediation against those top risks?
- What steps are taken to keep abreast of the risk threat horizon?
- What will our risk profile look like once all the current plans have been completed?

Conclusion

PO continue to make significant headway with its Information Security Transformation journey, building on Information Security Governance and the Security Transformation Programme.

The initiation of the '24x7x365' Security Operations Centre (SOC) has been awarded to Verizon for implementation. Service augmentation has commenced with the introduction Firewall Assurance, addressing a concern previously raised in the Deloitte report of 2016. The SIEM will consuming system logs in May 2018 and the full service augmentation will complete in July 2018.

Lock down of Office 365 is progressing, BYOD for mobiles is being rolled out, this includes a replacement handset for Corporate users. This will complete in April 2018 enabling unfettered mobile access to the environment to be disabled.

Additionally, technology to protect against phishing attacks and provide awareness training has been procured and is in the process of implementation (Ironscales), as well as technology to manage our digital Certificates, used to enable secure trusted connections to be established (Entrust). Entrust will identify all certificates in use and determine any issues that the certificates may pose to our live service.

POL00401626

IPA is working on improving the ability of people to recognise and react appropriately to cyber threats through increased awareness activities and have recently launched security characters to assist in getting the improving cyber security training to colleagues.

In conclusion, progress is being made and we have defined key next-steps and have realistic plans to deliver enhancements to our security posture throughout 2018. PO still remain below the level of maturity in cyber and information security for a company in a digital age, but our current provision is appropriate for where Post Office are on their digital journey.

Input Sought

The Committee is requested to note this paper.

POL00401626

Report

What are the current top risks to Post Office (PO) from an Information Security and Cyber Perspective?

The risks to our systems and information assets, as with many other organisations, are as follows:

Risk Number	Risk Description
1	External malicious attack
2	Loss of corporate and personal data through leakage across our perimeter
3	Insider threat (which includes accidental events i.e. phishing attacks)
4	IT Availability

How would we know if the risk has materialised?

PO would be aware if a cyber or information security related risk has materialised by:

- System outages or performance outside of accepted operational parameters (E.g. Denial of Service attacks);
- Identification of a breach through our SOC team;
- Ransomware demands;
- Internal incident reporting; or
- 3rd Party Alerts and Reporting.

What is the current status of the remediation against those top risks?

Risk Number	Remediation	Progress Update	Deadline
1, 3	Implementation of 24x7x365 Security Operations Centre (SOC)	Verizon contract has been signed (Jan 18). Service augmentation commenced, and FW Assurance went live 06/02/2018. Full SOC services implementation on track for July 2018.	Complete July 18

POL00401626

Risk Number	Remediation	Progress Update	Deadline
1, 3	Implementation of IronScales	Testing of Ironscales (phishing protection and awareness training) is now complete with full rollout by March 2018	Q4 17/18
2, 3	Data Leakage Prevention	Bring your Own Device – implementation of Microsoft InTune to control some aspects of data leakage. Completed rollout to GE.	Complete.
2, 3		InTune rollout of mobile devices remains in progress. The project has been re-planned to ensure all obsolete (windows) mobiles phones are replaced by end April, enabling the protected service to be fully adopted. Office 365 lockdown has moved to end April.	~~Q4 17/18~~. Q1 18/19
2, 3		Non Post Office owned laptops and access to Post Office E-Mail protection is due to be available from End Feb 18. Rollout to users will be over the following months.	Q1 18/19.
3	IPA Improving Security Awareness Culture	The images have been created and IPA have started their campaign. The questionnaire to determine the current status has also completed.	Complete
4	Data Owners Programme	GE will have been trained in Data Owner responsibilities during March	Complete

POL00401626

What actions remain to be performed?

Risk Number	Remediation	Progress Update
1	Updating of Legacy Systems	Our ageing systems continue to be a challenge to IPA's ability to maintain our certifications, especially to the Payment Card Industry – Data Security Standard (PCI-DSS). IPA, working with our Payments and Banking Services colleagues, are closely monitoring the situation. IT have a number of programmes already inflight to aid in the remediation of this risk.
2, 4	Data Leakage Prevention (DLP)	DLP paper has been submitted with progress being made on email controls to protect against data leakage. Project initiation to commence for other boundary solutions. The paper and plan to be presented at March ISC for approval.
2, 4	Data Classification	PO has had a classification scheme for a long time but colleagues do not habitually adhere to it. In order to implement any data leakage product successfully a sister programme is required to enforce better usage of our classification scheme. The DLP paper mentioned above also covers options for enforcement of data classification.
3	Security Culture	Campaign is underway. Information Security and GDPR awareness days scheduled for March in all support offices.
2,3	2 Factor Authentication	Passwords are recognised as not being secure enough to protect critical assets. Post Office need to better protect our remote access and should therefore implement a second level of protection. IT Security are assessing the impact to the business and a proposal for implementation will be delivered during Q1 18/19.
2, 3	Single Sign-on	IT Security in conjunction with Enterprise Architecture will be assessing the impact to the business during Q1 18/19.
3	Information Security Technical Standards	IT Security are fully committed with operational priorities. This will be revisited Q1 18/19.
1	Protection of postoffice.co.uk domain.	IT Security have identified a need to better protect our domain name to stop abuse of both the website and e-mails we send out to our

POL00401626

Risk Number	Remediation	Progress Update
		customers. Papers will be prepared and socialised Q1 18/19.

What steps are taken to keep abreast of the risk threat horizon?

IPA, IT and IT Security hold monthly risk meetings to:

- Identify new and emerging risks, allocate accountable leads and set milestones/deadlines;
- Review internal and 3rd Party Supplier Information Security Reports against our current risk appetite;
- Update on progress with existing risks and agree future activities;
- Test the validity and performance of existing controls, setting new actions where necessary; and
- Developing KRI to act as early warning systems to generate interventions.

The meetings are chaired by Heads of Department, where a strict governance process is followed to ensure risks are managed in-line with appetite, reviewed cohesively and only tolerated when there is sufficient evidence to suggest that the risk is mitigated.

All activity is recorded on the respective Risk Registers to ensure we have a transparent and auditable process.

The levels of confidence IPA and IT Security have over the levels of protection that our 3rd party suppliers is improving from its previous low position, this is due to the work being carried out through the SOC implementation and the visibility this affords Post Office over technical controls such as Firewalls. Work has been progressing during 2017/18 to set expectations within our critical supplier

What will our risk profile look like once all the current plans have been completed?

Without doubt, the completion of actions to a time and quality that we agree will lower the likelihood of risks materialising and in some cases, lower the impact. The implementation of the Advanced SOC and the fine tuning of alerting as a result of that, will be a significant step forward in protecting PO.

However, it is important to note that addressing impact is more complex due to the ever-changing risk landscape. As an example, having a complete and effective firewall estate may reduce the 'likelihood' of our defences being breached however, if breached, the impact would still remain 'high'.

To address the constant changing risk landscape it is vital that even once actions have been completed, there is a process of 'control re-assessment' to ensure that our defences are relevant and current. IPA, IT and IT Risk fully accept this and periodically reassess controls whether those controls are owned by ourselves of 3rd Party Suppliers.

Monitoring of our performance and the effectiveness of controls in now managed through new Risk Reporting Dashboards.

POL00401626

Risk Placemat, including an update on Risk Exceptions

Author: Richard Williams/Deana Herley Sponsor: Jane MacLeod Meeting date: 13 March 2018

Executive Summary

Context

The purpose of this paper is to provide the RCC with the latest version of the Placemat, which now includes the results from Financial Services & Telecoms (FS&T), POMS and Retail. The Q4 reassessment of risks has been performed with Finance and Operations (F&O) and Legal, Risk & Governance (LRG), with Government and Payment Services (G&PS) and Telecoms also reflected on the Placemat. The paper will also update the RCC on the the final 20% phase of the Placemat approach and a current status of Risk Exceptions.

Questions this paper addresses

- What are the results of rolling out the placemat in FS&T, POMS and Retail?
- What does the Q4 reassessment of risks tell us?
- What are the next steps in rolling out the placemat approach?
- What is the current status of Risk Exceptions?

Conclusion

1. FS&T has identified 155 risks overall, which includes Banking Services, with 8 top FS&T risks (8 red). POMS has identified 82 risks overall with 6 top risks (4 red, 2 amber). To date, as a start Retail has identified 132 risks within each team. Debbie Smith will present the top down view at the next RCC in May.
2. Since the Q3 reassessment, out of 32 top risks, 41% of the F&O risk profile has changed, with better processes and controls leading to reductions in 5 risks, most notably to cash management, client settlement and the appointment of agents. 7 risks have increased in the period and 1 new risk has been identified relating to instability of the NBSC telephony system. For LRG, out of 10 top risks, there has been a slight change in the risk profile, as mitigating actions continue to be progressed. The GDPR risk score has increased due to delay in getting additional team resource due to the very high demand for such technical expertise.
3. The final phase of the Placemat approach will be rolled out in April/May to the teams in IT, HR, Comms, Strategy and Identity Services.
4. There are 3 current Risk Exceptions for noting.

Input Sought

5. The Committee is asked to review and comment on the report.

POL00401626

The Report

What are the results of rolling out the placemat in FS&T, POMS and Retail?

FS&T

6. FS&T has provided a consolidated top down view of their respective risk and controls. A total of 155 risks have been identified, which includes Banking Services, with 8 top FS&T risks (8 red). The highest scoring risks in the profile are as follows:
   - PCI DSS non Compliance for Post Office (5x4 same risk as Banking Services): This risk is scored highly because of the contractual requirements of the Banking Framework. Following a PCI Audit in December, the planned remediation requirements to certification are scheduled to be in place by the end of March 2018, working with the Information Protection and Assurance Team.
   - GDPR Compliance for Telecoms (4x4): Post Office is the data controller for customer data but we are largely reliant on Fujitsu to ensure compliance with GDPR. There is a risk that we will not meet GDPR requirements because of the lack of capacity at Fujitsu to make the changes. The Telecoms Team, FS&T Risk and Post Office's GDPR team are working together on the remediation plan.
   - Customer Hub (4x4): Whilst the Customer Hub establishes itself, there are a series of programme and wider stakeholder engagement risks to be managed, mitigated and controls to be put in place. These include operational functionality and aligning them to business requirements, contractual risks, relationships with third parties and managing compliance, including regulatory requirements and data security standards.
   - Travel Money AML (4x4): The HMRC audit (Jan 17) identified that Post Office is not collecting nor can it evidence the required information in respect of our bureau transactions. A plan of improving controls was agreed with the regulator. There remains a risk we will not meet the timescales or required solution to HMRC audit requirements for Travel Money. The risk has increased as HMRC appears to be changing its position in relation to KYC record requirements. There is a remedial plan in place overseen by the Financial Crime team, which includes regular engagement meetings with HMRC.
   - Business Continuity Planning (5x3): Whilst the outsourced business centres, such as BoI, Fujitsu and FRES, have BCP plans it is unclear to the management of FS&T what the overall arrangements are, how we gain comfort that these are adequate and what the local arrangements are for staff members and how these are tested.
   - Regulation (3x4): There is a risk that the on-going growth in regulation in FS&T increases the risk of non-compliance and/or making various business activities unprofitable. Regulatory initiatives such as price caps on BT for home

POL00401626

phone-only contracts and automatic compensation risk significant impact on our costs and margin.

- Senior Manager and Certification Regime (4x3): Whilst POMS will be subject to this regime (timetabling yet to be determined by the FCA) there could be significant impacts on FS&T (and Post Office) as an Appointed Representative (AR) and supplier. This includes the need to ensure that responsibilities for all activities caught by the regime (vetting, conduct rules for a wide set of employees, systems and controls) can meet the SMCR requirements of POMS. POMS has an SMCR action plan in place.
- Key Person Risk (4x3 same risk as Banking Services): A significant amount of business knowledge and experience is covered by a few key individuals in FS&T, which, if they left the business, could have a significant detrimental impact on the ability of FS&T to complete its objectives. Following the recent changes to the management structure the team will be reviewing succession planning and retention measures.

POMS

7. POMS has provided a consolidated top down view of their respective risk and controls and has built on an existing risk management framework. POMS has identified 82 risks overall with 6 top risks (4 red, 2 amber). The highest scoring in the profile are as follows:
   - Marketing capacity and capability (4x3): POMS is currently recruiting approximately 12 staff to ensure its marketing needs can be met. The lack of sufficient and capable resource within the central marketing team with the required skill sets to deliver the POMS marketing plan may result in an under performance against the stated plan.
   - GDPR Compliance (3x4): Whilst progress is being made within the GDPR project, with both privacy notices and our approach to permissions nearing completion at the time of writing. Benchmarking with other insurers and via our new ABI membership has proven useful in moving the project forward. Uncertainty remains over readiness to comply with or understand the impact and costs associated with GDPR and DPA.
   - AR compliance (4X3): POMS has regulatory responsibility for the regulated activity of it's AR. There is a risk relating to PO's inability to provide assurance to POMS that its activities are is compliant. This includes: training, vetting, oversight, reporting and performance management/incentives. A separate list of PO risks has been created. A number of actions need to be undertaken if POMS is to be able to demonstrate it has a fully effective AR control framework. These include:
     - Conduct MI for use by POMS is being restructured and the revised MI set is on track for delivery by the end of March.

POL00401626

  - The branch review process is being restructured, and consideration is being given as to the overall approach to mystery shopping and how this might be better coordinated with our branch reviews.
  - EUM will create an ability to ensure all staff have been subject to proper fit and proper checks and have undertaken adequate training. Without the completion of adequate training or fit and proper checks, staff will not be able to access the system for these products. The EUM project is on track for material delivery by the end of July 2018. POMS management are obtaining regular updates regarding the EUM project which are also being reviewed by the Non-Executive Directors (NEDs).
- POMS strategy (4x3): The POMS strategy has been produced and is currently awaiting POL approval, which is expected by the end of March 2018. The strategy will highlight the key targets that POMS will be expected to achieve going forward.
- Senior Management Regime (SMR) readiness (3x3): The SMR will need to be introduced by late 2018.
- IDD readiness (3x3): EIOPA introduced the Insurance Distribution Directive to replace the Insurance Mediation Directive and is due to be enacted into local regulation by February 2018.

Retail

8. To date, Retail has identified 132 risks within each team. Debbie Smith will present the top down view at the May RCC. The risks cover the teams led by Mark Siviter (Mails and Retail), Roger Gale (Network and Sales), Tom Moran (Network Development), Tom Wechsler (G&PS) and Martin Kearsley (Banking Services). Debbie Smith will present the "top down" view at the May RCC. The rollout of the placemat to Mails, Network Sales and Network Development has built on the existing risk management framework. The Q4 reassessment in Government and Payment Services (G&PS) has further enhanced risk awareness. The highest scoring risks in the profile are as follows:

   Mails and Retail
   - RM renegotiation (4x2): A significant amount of work has gone into Mails renegotiation readiness, but uncertainties continue to exist over our current agreement with Royal Mail beyond 2020, until an outcome is reached. The existing MDA will require better alignment to today's market challenges.
   - Product Risk: 30% of net risks in Mails relate to Product Risk resulting in a loss of revenue and footfall, with customers likely to migrate from RM to competitors as well as, general market declines in lottery, retail and stamp sales.

POL00401626

Network Development

- Retail Proposition and Network Sustainability (5x3): There have been significant developments in almost all areas relevant to the Retail business area and this is reflected in the risks being managed by Network Development. The most significant relates to the attractiveness of the Post Office proposition to Retailers, which is being addressed through a fundamental reassessment of our Retail Network Strategy.
- HNGT (4x3): There is a risk that HNGT cannot deliver the new simpler operating model for agents and POL due to operational and financial constraints.
- Employment Status (5x2): The employment status of Postmasters remains under ongoing review, a risk which carries a significant impact but low likelihood.

Banking Services

The rollout of the placemat in Banking Services was conducted by FS&T Risk (now part of LRG) in collaboration with the Central Risk team and who continue to support Banking Services going forward. The highest scoring risks in the profile are:

- PCI DSS non Compliance for Post Office (5x4 same risk as FS&T): This risk is scored highly because of the contractual requirements of the Banking Framework. Following a PCI Audit in December, the planned remediation requirements to certification are scheduled to be in place by the end of March 2018, working with the Information Protection and Assurance Team.
- Cheque Clearing (3x5): Provider, Barclays Bank, is to change cheque clearing sub-contractor (from iPSL in Northampton to Parseq in Rotherham) which will negatively impact SLAs and cause disruption for the Banking Framework. The Banking Services team is working on mitigating disruption together with Royal Mail.
- Key Person Risk (4x3 same risk as FS&T): A significant amount of business knowledge and experience is covered by a few key individuals, which, if they left the business, could have a significant detrimental impact on the ability to complete objectives. Following the recent changes to management structure the team will be reviewing succession planning and retention measures.

G&PS

There are 15 existing top risks. Since the Q3 reassessment, 8 new risks have been identified and 5 closed or transferred. The highest scoring Q3 risk relating to the POca procurement has been closed, while the majority of the risk relating to AEI infrastructure has been transferred to the new Identity Services team:

- ATM industry (4x4): Wider changes in the ATM industry and market may lead to BOI invoking a renegotiation of the ATM agreement.
- PCI DSS noncompliance for Post Office (4x4): There is a risk that the business will not complete the remediation activities needed to meet PCI DSS within

POL00401626

the extended timeframe of 31st March, which would jeopardise current and prospective G&PS client business.

- TLS upgrade (5x3): The Transport Layer Security (TLS) upgrade may not meet the deadline of 20th May 2018. If we do not meet the deadline, there is a risk we will not be able to process card payments for G&PS clients (e.g. BT, DVLA)
- POca contract (4x3): The contract becomes loss making towards the end of the main term with a corresponding loss of branch footfall from POca customers. A 'Future of POca' programme has been established to develop future products for this customer group.
- ATM operational availability (3x4): ATM operational availability continues to be a concern. The Post Office Service Team is now in place and improvements taken and underway are starting to be reflected in performance improvements.

Network and Sales

- Failure of IT infrastructure (5x3): The most significant risk for Network and Sales continues to be the reliability and recoverability of IT infrastructure. The size of the overall branch network makes it resilient to most operational issues other than complete system failure, but if whole sub-networks of branches with specialised equipment such AEI kit are affected, customer disruption could be severe.
- Reduction in agent remuneration (5x3): Reduction in agents' remuneration makes branches less sustainable and this could lead to a reduction in staff numbers with a negative impact on customer experience.
- Proposed changes to Directly Managed Branches (4x3): On-going changes to the DMB network continue to carry a reputational risk.
- Managing change (3x4): In common with other business areas, Network and Sales is vulnerable to changes to products, processes or systems which have a negative impact on customer experience in branch. On-going changes to the Directly Managed Branch network continue to carry a reputational risk.
- Retail supply of Postpak (3x4): Current challenges with the supply of Postpak retail items pose a risk to sales and customer experience, but work is underway with the Mails team and WH Smith to resolve the supply issues.

What does the Q4 reassessment of risks tell us?

9. Since the Q3 reassessment in November 2017, risk registers covering 22 teams have been formally reviewed with senior management. The most notable changes to the "top risks" for F&O and LRG are as follows:

F&O

There are 32 existing top risks. Since the Q3 reassessment, 41% of the F&O risk profile has changed, with better processes and controls leading to reductions in 6 risks, most notably to cash management, client settlement and the appointment of agents. 7 risks have increased in the period and 1 new risk has been identified

POL00401626

relating to instability of the NBSC telephony system (3x2). Key elements of the F&O risk profile are as follows:

- Legacy Systems (4x2 from 4x3): Good progress has been made towards reducing the risks posed by aged IT systems with the successful transfer from HRSAP of staff payroll to SuccessFactors and agents' remuneration to CFS. POLSAP and legacy systems at Swindon remain vulnerable and the overall risk is unchanged.
- Health and Safety (5x3 from 5x2): An increase in small accidents in Supply Chain has resulted in an increased score. A proactive approach to health and safety management is being rolled out across Supply Chain, including training Safety Champions in each business unit and setting up a Safety Forum to provide support and guidance.
- Agent Theft and Fraud (3x5 from 2x5): A significant increase in agent debt compared to last year means this is now one of the highest scoring risks in the F&O risk profile. Improvements in detection of fraud and better control of cash are helping to limit the consequences of fraud, but the key driver continues to be the inability to prosecute.
- Management information (3x5 from 2x5): This risk has been scored higher to reflect the importance of management information in driving business improvements. The Data Governance project (Arrow) has been initiated and a Data Strategy will be presented in March 2018.
- Business Continuity (4x3 from 3x3): Business continuity is an increasing risk because of the aged systems and untested plans. Plans are in place to test Chesterfield in March and Bolton in April 2018.

<u>LRG</u>

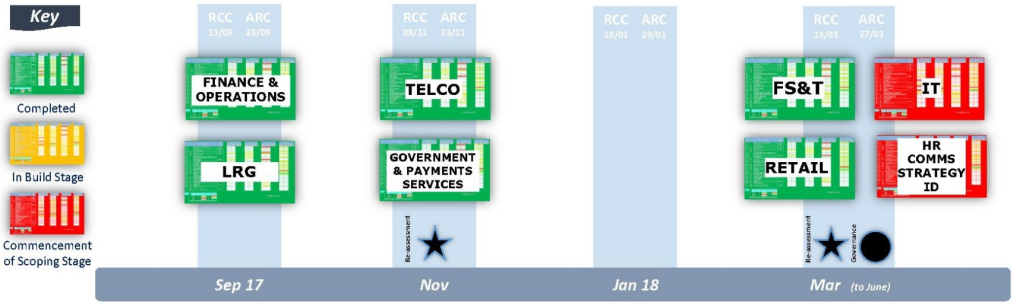
There are 10 existing top risks. Since the Q3 reassessment, 20% of the LRG risk profile has changed, most notably to GDPR (4x4 from 3x3). Key elements of the LRG risk profile are as follows:

- PCI accreditation (5x4 no change): Progress is being made towards reducing the risk with actions plans in place to remediate the shortcomings identified in the audit. Fujitsu and Computacentre are also involved in the remediation and audits continue across the network. There is a dependence on Computacentre to deliver remediation activities, confidence in which is currently low.
- GDPR (4x4 from 3x3): A lack of documentation, scale and complexity and capacity in the BAU DP Team has increased the likelihood. Recruitment is underway for interim Data Protection SMEs which are scarce due to demand in other GDPR programmes.
- Insider threat (4x3 no change): Progress to date include the signing of the Verizon contract to establish a Security Operations Centre, which will provide oversight of all security controls from each provider, centralise and aggregate events and incidents to enable POL to react against security issues efficiently and effectively, thereby reducing our risk exposure.

POL00401626

What are the next steps in enhancing the roll out?

10. The final phase of the Placemat approach will be rolled out to teams in IT, HR, Comms, Strategy and Identity Services; an update will be provided for May RCC.



What is the current status of Risk Exceptions?

11. The current approved Risk Exceptions are as follows:

Title	Risk	Category	GE Owner	Accountable owner	Date Raised	Closure Date	Actions	Due Date	Status/ Update
Robotic Process Automation (RPA) Live Operation - Finance Service Centre	There is a risk of loss of data /service as the RPA software is running on stand-alone desktop machines, which are not backed-up, have no UPS and have no provision for real time resilience.	Policy	Al Cameron	Angela Van-Den-Bogerd	29-Nov-16	31-Dec-17	Migrate to a permanent infrastructure.	31-Dec-17	**On-going.** Risk Exception is being renewed with detailed actions and timelines. Business was pursuing a hosted solution. Accenture have returned with a reduced cost proposal which looks like it will factor in to the existing budget. Detailed time frame will be assessed and included in the revised Exception.
SalesForce – Procurement	Contract has been renewed /extended non-compliantly for a period of 12 months.	Regulatory	Owen Woodley	Chrysanthy Pispinis	21-Apr-17	29-Apr-18	POL should seek to run a full compliant procurement as soon as possible to reduce the risk of a challenge.	29-Apr-18	**On-going.** The business requirements for Salesforce have been included in the scope of the CDP Procurement, which has recently been awarded to Accenture. A Change Request has been submitted into Accenture and is under review by both legal teams. On-track to deliver by end of April 2018
Success Factors	Implementation of Success Factors without addressing certain data protection and information security risks could result in breach of data protection regulation and Post Office policy requirements as line managers can download, copy, export and distribute, personal data of their team members, via non-corporate devices.	Regulatory	Martin Kirke	Martyn Lewis	02-Jan-18	30-Jun-18	Directive from the Group HR Director for a declaration to be signed by the staff in HR Service Centre	08-Jan-18	**Closed -** HRSC team have all signed the declaration.
							Weekly report to monitor access via IP addresses of non-corporate devices	w/c 08-Jan-2018	**Closed–** No longer required due to action 3.
							Installation of a password manager	26-Jan-18	**Closed -** Password Manager App has now been deployed to the HRSC team, meaning a technical restriction is now in place for this population. This will remain until the corporate solution is identified.
							Suitable training and information during the roll out of SuccessFactors to all line managers and new joiners.	08-Jan-18	Measures to be put in place : - **Closed.** Data Protection statement screen when logging on. - **On-going, to be included in the 18/19 compliance test.** Compliance training Info SecDP, updated module content to reflect. - **Closed.** Further training and comms have been issued to the HRSC team to strengthen operational controls.
							A corporate solution (combination of SSO/BYOD)	30-Jun-18	**On-going** - The JML project has run a design on SSO/Provisioning that we believe will solve this issue. design documents are now with The CTO for review. - The business case is being updated to include this work and is expected to be submitted this week (w/e - 3/3/18). - Technical work can begin once design is complete and funding is agreed. - At this stage we believe significant progress will have been made by June, reducing this wider risk for our business.

POL00401626

Appendices

1: Placemat
2: Financial Services and Telecoms results
3: POMS results
4a: Mails and Retail
4b: Network Development
4c: Banking Services
4d: G&PS
4e: Network and Sales
5: Finance and Operations Q4 refresh
6: Legal, Risk and Governance Q4 refresh

POL00401626

Appendix 1

Placemat - RCC 12/3/2018

Ref		Principal Risks	GE Owner	Retail: Mails and Retail Q4 18	Retail: Mails and Retail Influencing Factor	Retail: Network Development Q4 18	Retail: Network Development Influencing Factor	Retail: Banking Services Q4 18	Retail: Banking Services Influencing Factor	Retail: Government and Payment Services Q4 18	Retail: Government and Payment Services Influencing Factor	Retail: Network Sales Q4 18	Retail: Network Sales Influencing Factor	Financial Services and Telecoms Q4 17	Financial Services and Telecoms Influencing Factor	POMS Q4 17	POMS Influencing Factor	Finance & Operations Q3 17	Finance & Operations Q4 17	Finance & Operations Influencing Factor	Legal, Risk and Governance Q3 17	Legal, Risk and Governance Q4 17	Legal, Risk and Governance Influencing Factor	Principal Risks	Ref	Risk Appetite - Mar 2015: Averse	Neutral	Tolerant	Seeking
1	OPERATIONAL	Manage process and deliver services	TBC	2	Transition of retail to WHSmiths	2	Employment status	1	Knowledge risk on key man dependency / Demand for Banking Services	2	Transport Layer Security upgrade / ATM availability	2	Customer experience	1	Knowledge risk on key man dependency			2	2	Supporting agents				Manage process and deliver services	1				
2		Product risk	OW / DS	2	Decline in revenue - stamps, lottery and retail																			Product risk	2				
3		Make payments	AC															2	3	Client settlement				Make payments	3				
4		Records management	TBC																					Records management	4				
5		Procure	AC							2	Replacement of Paystation							2	2	Procure badly				Procure	5				
6		Contract Management	All	2	MDA			2	Barclays IPSL relationship	2	Non-compliance in Branch	2	Gaps in Postfish								2	2	Contract non-compliance	Contract Management	6				
7		Managing change	AC			2	HNGT programme and volume of change	2	HDRC upgrade / Atos capacity			2	Potential industrial action	2	Horizon development			1	2	POLSAP / Legacy Systems				Managing change	7				
8		Keep our people, customers & 3rd parties safe										2	Security guidelines in branches					2	2	Increase in small accidents (ISC)				Keep our people, customers & 3rd parties safe	8				
9		Physically secure																3	3	Cash centre security				Physically secure	9				
10		BCP (excel ITDR)	JMaC							2	No contracts for some clients			1	Infrastructure Failure (Lack of BCR)			2	2	BCP Plans / Swindon	2	2	BCP arrangements	BCP (excel ITDR)	10				
11	TECH	Technology Ops	RH									2	Branch technology refresh											Technology Ops	11				
12		Business Interruption (ITDR)										2	Disruption to Network					2	2	POLSAP/Telephony system				Business Interruption (ITDR)	12				
13		IT Security																			2	2	Cyber Threat	IT Security	13				
14		Dependence on IT 3rd Parties																						Dependence on IT 3rd Parties	14				
15	LEGAL & REGULATORY	Managing losses and Fraud	AC					3	Splitting transactions					2	Vulnerable customers			2	2	Agent fraud				Managing losses and Fraud	15				
16		Financial Crime	JMaC	2	Gift cards for money laundering			2	SYSC 6					2	HMRC Audit						2	2		Financial Crime	16				
17		Information Protection						1	PCI compliance	2	PCI compliance			1	PCI / GDPR compliance	2	GDPR	2	2		2	2	PCIDSS / GDPR	Information Protection	17				
18		Brand	MD																					Brand	18				
19		Record and pay taxes	AC															2	2	Resource changes				Record and pay taxes	19				
20		Litigation	JMaC																		3	3	Incessing : Postmaster Litigation	Litigation	20				
21		Governance						3	Banking Reform							2	AR				2	2	Risk mgt & policies	Governance	21				
22		Compliance with laws and regulations		2	MDA change request					2	ATM exemption	2	Mis-selling of easy life product	2	SMR / Telco Reg Regime	2	SMR and 3DD	2	2	EUM roll-out not yet complete	2	2	Increased visibility to Regulators	Compliance with laws and regulations	22				
23	FINANCIAL	Reporting results and providing data accurately	AC	1	Credence reporting													2	2	MI / Forecasting				Reporting results and providing data accurately	23				
24		Sufficient cash / headroom																2	2	Cash data / Mgt of cash				Sufficient cash / headroom	24				
25		Ensuring sustainable profit				3	NFSP relationship / Model profitability and consentration			2	ATM industry changes / ATM Availability / POCA	2	Reduction in agent remuneration					2	2	Insurance Coverage				Ensuring sustainable profit	25				
26		Control activities																2	2	Informal controls in FSC				Control activities	26				
27	STRATEGY	Competitiveness	OW/DS	2	RM customer acquisition strategy	2	Retail proposition and Network Sustainability			2	Bill payments market / contract exchange / CMA conditions	2	Customer feedback methodology	2	Wholesale fibre customer retention									Competitiveness	27				
28		Strategic Risk		2	RM renegotiation									2	Failure of Customer Hub	2	POMS strategy sign off							Strategic Risk	28				
29		Market																						Market	29				
30		Customer Relevance																						Customer Relevance	30				
31	PEOPLE	Communicate, inspire and align	TBC	2	Employee engagement	3	Capacity, capability and engagement					2	Uncertain future and lack of development opportunities			2	Marketing resource	2	2	Supply Chain / SecOp comms on front line				Communicate, inspire and align	31				

Key	Risk & Control Status	Harm Tarsie (L/L) Minimum Score	RAG	Control Effectiveness Score	RAG
	Low	1	G	1	R
	Medium	6	A	2	A
	High	11	R	3	G
	Risk n/a				

Colour indicates net risk score / Number equals control effectiveness

POL00401626

Appendix 2

FS&T Dashboard

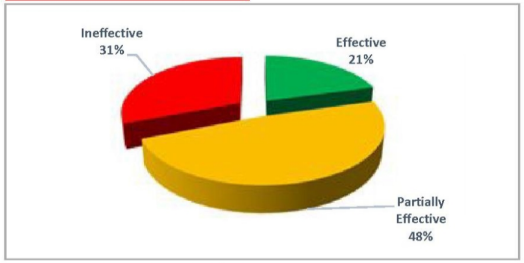
Top Risks by Risk Score

#	Sub-Risk Title	Risk description	CSA	Residual Risk Score	Commentary
1	Information Protection	PCI auditors identified remediation activities that will go beyond the date (28th December 2017) that our Report of Compliance (RoC) should be completed .The outcome of the audit , PO has failed to obtain the required PCI -DSS certification. This is a breach of our agreed banking framework and may lead to a legal/regulatory breach, financial loss and reputational damage. If Post Office fails to ensure operational activities, IT infrastructure/security and related services are PCI-DSS compliant it cause challenges during external audit, and require significant remediation actions, attracting unbudgeted costs.	1	20	PCI certification is critical to the Post Office. PCI audit remediation activities will go beyond the date (28th December 2017) that our Report of Compliance (RoC) should be completed .The outcome of the audit , PO has failed to obtain the required PCI -DSS certification. This is a breach of our agreed banking framework and may lead to a legal/regulatory breach, financial loss and reputational damage. If Post Office fails to ensure operational activities, IT infrastructure/security and related services are PCI-DSS compliant it cause challenges during external audit, and require significant remediation actions, attracting unbudgeted costs. We have formed a steering committee to oversee remediation activities. RCC is receiving regular updates and we are aiming to achieve PCI certification by or before 31 March 2018.
2	Information Protection	Failure of Fujitsu to have the correct controls and processes in place to meet the new requirements of General Data Protection Regulation in 2018 (GDPR) . Failure to do so will result in loss of global turnover of between 2%-4%.	2	16	Post Office needs to be compliant with GDPR by May 2018. Post Office is the data controller for customer data but we are largely reliant on Fujitsu to ensure compliance with GDPR. There is a risk that we will not meet GDPR requirements because of the lack of capacity at Fujitsu to make the changes. The Telecoms Team, FS&T Risk and Post Office's GDPR team are working together on the remediation plan.
3	Strategic Risk	Failure to operationalise the hub to meet business requirements due to inadequate alignment to business, lack of governance and controls or third party and contractual risks	2	16	The hub is an innovative digital programme (Post Office in your pocket) to support customers and help move Post Office further up the value chain. Whilst it establishes itself there are a series of programme and wider risks to be managed. These include operational functionality and aligning them to business requirements, contractual risks, relationships with third parties and managing compliance, including regulatory requirements and data security standards. The FS&T Risk team is working with the Hub business and programme teams to ensure controls are put in place to mitigate this risks, whilst supporting an agile approach. This includes ensuring that the programme engages with stakeholders across the Post Office.
4	Financial Crime	(A) The HMRC audit (Jan 17) identified we are not collecting or can evidence the required information in respect of our bureau transactions. FRES13(B) Risk we may not delivery the required changes within the deadlines outlined in the plan . HMRC have made is clear that there is zero tolerance in respect of missing these deadlines.	2	16	The HMRC audit (Jan 17) identified that Post Office is not collecting nor can evidence the required information in respect of our bureau transactions. A plan of improving controls was agreed with the regulator. There remains a risk we will not meet the timescales or required solution to HMRC audit requirements for Travel Money. This risk has increased as HMRC appears to be changing its position in relation to KYC record requirements. There is a remedial plan in place overseen by the Financial Crime team, which includes regular engagement meetings with HMRC.
5	BCP (excl ITDR)	Significant infrastructure failure-no effective Business Continuity programme for FS & T.	1	15	Business continuity planning is not only important for Post Office to continue its operations, it is also a contractual requirement across a number of contracts. Whilst the outsourced business centres, such as BoI, Fujitsu and FRES, have BCP plans it is unclear to the management of FS&T what the overall arrangements are, how we gain comfort that these are adequate and what the local arrangements are for staff members and how these are tested.
6	Compliance with laws and regulations	There is a risk that the on-going increase in regulation in FS (and Telecoms businesses) increases the risk of non-compliance and/or making various business activities unprofitable (e.g., Insurance Distribution Directive requirements). Regulatory risk from Ofcom activity e.g. review of general conditions, complaints, automatic compensation could lead to a drain on resources, increased costs to the business and impact on the change schedule.	2	12	There is a risk that the on-going growth in regulation in FS&T increases the risk of non-compliance and/or making various business activities unprofitable. Regulatory initiatives such as price caps on BT for home phone-only contracts and automatic compensation risk significant impact on our costs and margin. We undertake regulatory horizon scanning to anticipate future requirements and work with each business area to undertake appropriate solutions. We also have a planned budget for regulatory change, relationship with OFCOM. We have also recently recruited a Senior Risk & Compliance Manager for Telecoms.
7	Compliance with laws and regulations	Senior Managers and Certification Regime, PO are unprepared or can not deliver the extension of these requirements due in 2017 and 2018.	2	12	POMS will be subject to the Senior Manager and Certification Regime, there could be significant impacts on FS&T (and Post Office) as an Appointed Representative and supplier. This includes the need to ensure that responsibilities for all activities caught by the regime (vetting, conduct rules for a wide set of employees, systems and controls) can meet the SMCR requirements of POMS. Post Office and POMS are working together to ensure that Post Office is in a position to support POMS.
8	Manage process and deliver services	A significant amount of business knowledge and experience is covered by a few key individuals who if they left the business suddenly could impact significantly on the ability to complete our objectives.	1	12	A significant amount of business knowledge and experience is covered by a few key individuals in FS&T, which, if they left the business, could have a significant detrimental impact on the ability of FS&T to complete its objectives. Following the recent changes to management structure the team will be reviewing succession planning and retention measures.

Heatmap



Control Self Assessment



Risk Headline

No of Risks (Open or New)	155
No of Red Risks	21
No of Amber Risks	69
No of Green Risks	65
No of Red risks with ineffective controls	14
No of New Risks	49
No of Closed Risks	38

POL00401626

Appendix 3

POMS Dashboard

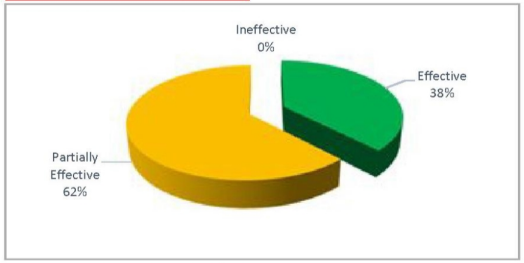
Top Risks by Risk Score

#	Sub-Risk Title	Risk description	CSA	Residual Risk Score	Commentary
1	Communicate, inspire and align	Lack of sufficient and capable resource within central marketing with the required skill sets to deliver the POMS marketing plan results in an under performance against our stated plan.	2	12	In 2017, there was a restructuring in the Post Office Marketing team and POMS is currently recruiting approximately 12 staff to ensure its marketing needs can be met.
2	Information Protection	Failure for readiness to comply with or understanding the impact and costs associated with GDPR and DPA - this could lead to financial penalties by our regulators and loss of reputation/confidence by customers affecting market share.	2	12	Progress is being made within the GDPR project, with both privacy notices and our approach to permissions nearing completion at the time of writing. Benchmarking with other insurers and via our new ABI membership has provided useful in moving the project forward.
3	Governance	POMS has regulatory responsibility for the regulated activity of it's AR. Given that there are over 11,000 agency branches, there is a risk that POL is unable to provide assurance to POMS that activity is compliant. This includes: training, vetting, oversight, reporting and performance management/incentives. N.B. A separate list of POL risks has been created.	2	12	It has been identified that a number of actions need to take place if POMS is to be able to demonstrate it has a fully effective AR control framework. These include: • Conduct MI for use by POMS is being restructured and the revised MI set is on track for delivery by the end of March. • The branch review process is in the process of being restructured, and consideration is being given as to the overall approach to mystery shopping and how this might be better coordinated with our branch reviews. • EUM will create an ability to ensure all staff have been subject to proper fit and proper checks and have undertaken adequate training. Without the completion of adequate training or fit and proper checks, staff will not be able to access the system for these products. The EUM project is on track for material delivery by the end of July 2018. POMS management are obtaining regular updates regarding the EUM project which are also being reviewed by the Non-Executive Directors (NEDs).
4	Strategic Risk	Risk that POMS Strategy/Business Plans (including Annual Operating Plan target) are not implemented completely and/or as per agreed deadlines.	2	12	The POMS strategy has been produced and is currently awaiting POL approval, which is expected by the end of March 2018. The strategy will highlight the key targets that POMS will be expected to achieve going forward.
5	Compliance with laws and regulations	The SMR will need to be introduced by late 2018 - there is a risk that POMS are not able to meet the requirements of SMR, leading to financial penalties.	3	9	HM Treasury announced that the SM&CR will apply to insurers from 10 December 2018. It is likely that insurance intermediaries (including POMS), will follow shortly after. There is therefore a need to ensure that we have a clear plan and timeline for SMCR deliverables, and that appropriate resources are applied to this work.
6	Compliance with laws and regulations	EIOPA introduced the Insurance Distribution Directive to replace the Insurance Mediation Directive and is due to be enacted into local regulation by February 2018. There is a risk that POM's are not able to meet the requirements of the IDD, leading to financial penalties.	2	9	Following the revision of the IDD delivery date to 1 October 2018 POMS has spent time re-planning the deliverables required to ensure Compliance. At this stage the project is green and on track. Work is also ongoing to ensure that the web based process is optimised within the requirements of IDD.

Heatmap



Control Self Assessment



Risk Headline

No of Risks (Open or New)	82
No of Red Risks	6
No of Amber Risks	61
No of Green Risks	15
No of Red risks with ineffective controls	0
No of New Risks	0
No of Closed Risks	0

POL00401626

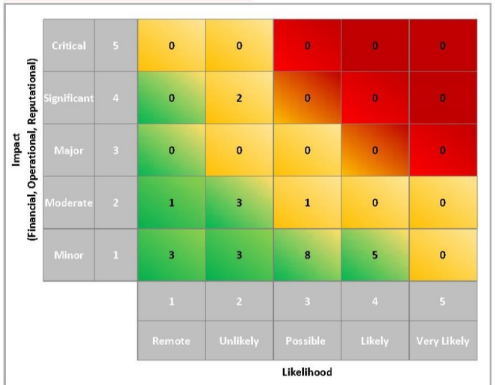
Appendix 4a

Retail – Mails and Retail Dashboard (1/5)

Top Risks by Risk Score

#	Principal Risk Title	Risk description	CSA	Residual Risk Score
1	Strategic Risk	New - Misalignment of objectives and unsuccessful renegotiation of MDA or negotiation of disadvantageous terms.	2	8
2	Strategic Risk	New - RMG give notice of termination of contract in 2020 which would involve us ceasing all existing mail services and seek a replacement possibly at a lower income rate.	2	8
3	Product risk	In branch fraud e.g. false accounting of stock resulting in financial loss to agent or PO.	2	6
4	Ensuring sustainable profit	Mail work negotiations leave Post Office less value in the proposition - c. £1-2m p.a. income below forecast.	2	4
5	Competitiveness	A competitor launches a Letter/Large Letter format product to compete with RMG resulting in a loss of revenue and income from the transaction as customers migrate.	3	4
6	Manage process and deliver services	Transitional arrangements for the handover to a new retail supplier lead to either no stock available for sale, or too much stock left over in branch.	2	4
7	Financial Crime	New - Customers purchase gift cards for the purpose of money laundering or financing terrorism.	2	4
8	Product risk	On-line Postage takes off faster as a result of increased differential channel pricing - projected impact of £1.8m	3	4
9	Contract Management	Product Team breach compliance requirements within the MDA (Change Request timelines not met) resulting in RMG reputational damage.	2	4
10	Product risk	Drop & Go - Errors in systems allow customers to go into a negative balance and can then be blocked.	2	4
11	Communicate, inspire and align	New - Poor employee engagement leads to low productivity and/or higher propensity to churn.	2	4
12	Manage process and deliver services	Customers defraud POL through misuse of the Cheque Authority Card processes resulting in losses due to funds being unrecoverable.	3	3
13	Product risk	RM's new 'confirmation of delivery' option will cannibalise SF and SD further than budgeted. Expected to be £1.3m (on top of £1.3m in budget).	3	3
14	Communicate, inspire and align	Projects may not deliver to time or quality as a result of reduced resourcing and potential conflicting time scales.	2	3
15	Competitiveness	RMG 'poach' customers through offering doing significant volume - POL earn £1.5m p.a. from customers who post 50+ items per week.	2	3

Heatmap



Risk Headline

No of Risks (Open or New)	26
No of Red Risks	0
No of Amber Risks	3
No of Green Risks	23
No of Red risks with ineffective controls	0
No of New Risks	4
No of Closed Risks	2

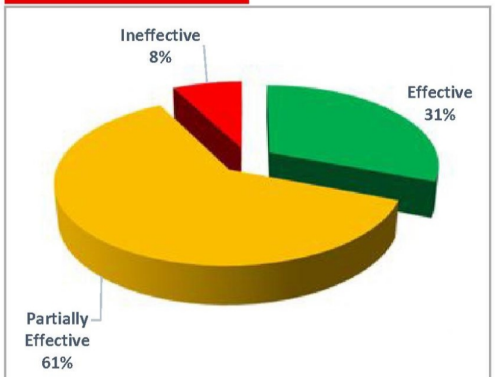
Control Headline

No of Risks assessed as effectively controlled	8
No of Risks Self assessed as partially controlled	16
No of Risks assessed as ineffectively controlled	2

Top Risks by Principal Title



Control Self Assessment



POL00401626

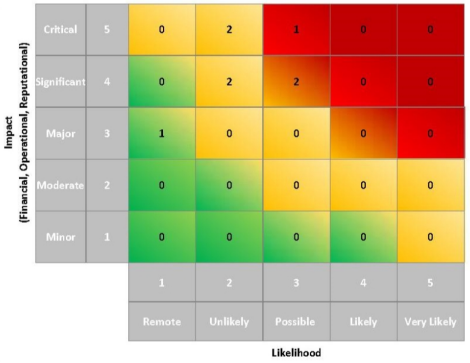
Appendix 4b

Retail – Network Development Dashboard (2/5)

Top Risks by Risk Score

#	Principal Risk Title	Risk description	CSA	Residual Risk Score
1	Competitiveness	New - Post Office's retail value proposition becomes insufficiently attractive to retailers result in shrinkage to our branch network and breach government commitments.	2	15
2	Managing change	New. HNGT does not deliver the new simpler operating model for agents and POL due to operational and financial constraints.	2	12
3	Managing change	New – The extensive change currently underway and planned within Post Office negatively impacts Postmasters and their business.	3	12
4	Manage process and deliver services	A successful challenge is made with regard to the employment status of postmasters such that they are categorised as employees or workers and Post Office becomes liable for additional cost.	2	10
5	Ensuring sustainable profit	New - One of our large multiple partners McColl's, Spar, One Stop, Co-Op resigns their Post Offices, damaging our reputation, proposition and may breach government commitment on network numbers.	3	10
6	Ensuring sustainable profit	The relationship with the NFSP becomes unworkable, resulting in an inadequate return on investment and need to cease funding.	3	8
7	Communicate, inspire and align	New - Poor employee engagement, lack of capacity or capacity leads to ineffectiveness low productivity and/or higher propensity to churn.	3	8
8	Ensuring sustainable profit	New - CWU Postmaster branches increases to 50% (plus) in membership, giving them a strong case for recognition, meaning PO would have to negotiate with another party.	3	3

Heatmap



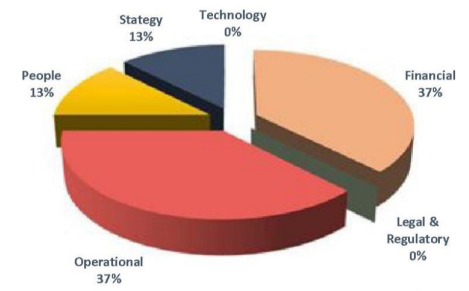
Risk Headline

No of Risks (Open or New)	8
No of Red Risks	3
No of Amber Risks	4
No of Green Risks	1
No of Red risks with ineffective controls	0
No of New Risks	6
No of Closed Risks	0

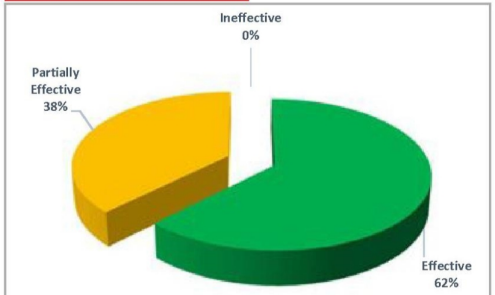
Control Headline

No of Risks assessed as effectively controlled	5
No of Risks Self assessed as partially controlled	3
No of Risks assessed as ineffectively controlled	0

Top Risks by Principal Title



Control Self Assessment



CONFIDENTIAL

POL00401626

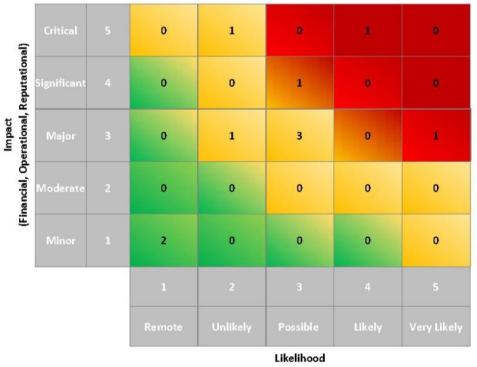
Appendix 4c

Retail - Banking Services Dashboard (3/5)

Top Risks by Risk Score

#	Sub-Risk Title	Risk description	CSA	Residual Risk Score
1	Information Protection	This is a breach of our agreed banking framework and may lead to a legal/regulatory breach, financial loss and reputational damage. If Post Office fails to ensure operational activities, IT infrastructure/security and related services are PCI-DSS compliant it cause challenges during external audit, and require significant remediation actions, attracting unbudgeted costs.	1	20
2	Contract Management	There is a risk that Barclays change of cheque clearing sub-contractor (from iPSL in Northampton to Parseq in Rotherham), due to the industry transition from paper to image clearing, will negatively impact our partner banks.	2	15
3	Manage process and deliver services	New - A significant amount of business knowledge and experience is covered by a few key individuals who if they left the business suddenly could impact significantly on the ability to complete our objectives.	1	12
4	Managing change	HDCR Programme Upgrade to PODG in March 2018. There is a risk that the testing to be undertaken fails to identify defects that could result in a loss of connectivity between POL and the client banks. A loss of connectivity would result in no client files being sent to circa 15 Banks, resulting in them being unable to reconcile customer accounts with deposits or charge them for using services such as Change Giving.	1	10
5	Financial Crime	SYSC 8 - Banking Framework has made a POL Board approved commitment to SYSC 8 (material outsource partners to banks). SYSC 8 requires auditable evidence of HR vetting for all counter based staff. This could be audited anytime from Jan 17 onwards, Current systems and processes offer limited scope for successfully achieving the required standard.	2	9
6	Managing change	ATOS Capacity and Capability to Deliver the Volume of Banking Services Projects with a high number of projects forecast to be delivered, there is a risk that anticipated timescales will not be achieved by ATOS and a further risk that where the team are stretched errors could occur which impact live services.	3	9
7	Contract Management	Link Members Council has discussed and agreed two candidate changes to the Link regulations. They are 1) Contactless ATM and 2) Settlement Disaggregation. The second of these could be significant for POL regarding how we clear and settle daily sums via Vocalink into the BOE RTGS system to banks. The main reason would seem to be a desire to ensure all scheme companies (LINK, FPS, BPSL etc.) remain totally arms-length from the Infrastructure companies . If this threat materialises for PO, it will have a major impact on our Banking and POCa transactions.	2	9
8	Manage process and deliver services	Increase in Banking Services demand through POL Network. Whilst this is great news for the business, there are risks that the increase in demand could adversely impact areas of the business, inclusive of: - An increased queuing time for services within POL Branches - Insufficient cash storage space within POL Branches - An increase in transactions being processed by the FSC that require intervention	3	6

Heatmap



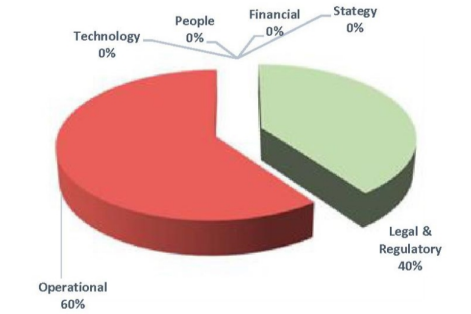
Risk Headline

No of Risks (Open or New)	10
No of Red Risks	3
No of Amber Risks	5
No of Green Risks	2
No of Red risks with ineffective controls	2
No of New Risks	1
No of Closed Risks	20

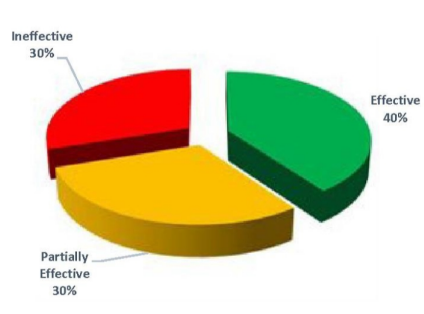
Control Headline

No of Risks assessed as effectively controlled	4
No of Risks assessed as partially controlled	3
No of Risks assessed as ineffectively controlled	3

Top Risks by Principal Title



Control Self Assessment



POL00401626

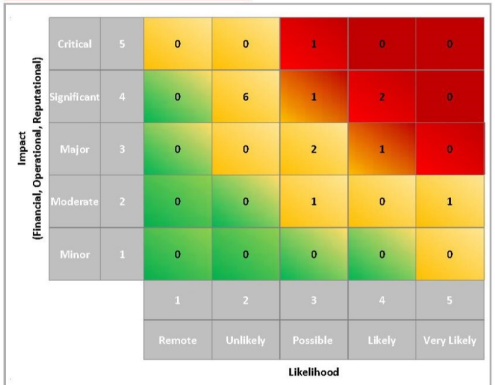
Appendix 4d

Retail - Government & Payment Services Dashboard (4/5)

Top Risks by Risk Score

#	Sub-Risk Title	Risk description	CSA	Residual Risk Score
1	Ensuring sustainable profit	New - Wider changes in the ATM industry and market will cause BOI to renegotiate the ATM Agreement to review the ATM model beyond 2022. They may also try to include as part of the wider changes/ business discussions with POL.	2	16
2	Information Protection	New - There is a risk that the business will not complete the remediation activities to meet PCI DSS (Payment Card Industry Data Security Standard) compliance within the extended timeframe (31st March 2018) which will jeopardise current and prospective G&PS client business.	2	16
3	Manage process and deliver services	New – There is a risk the Transport Layer Security (TLS) upgrade will not meet the deadline (20th May 2018). If we do not meet the deadline, there is a risk we will not be able to process card payments for G&PS clients (e.g. BT, DVLA).	2	15
4	Ensuring sustainable profit	New - There is a risk of the POca contract becoming a loss making contract towards the end of the main term (to November 2021) with a corresponding loss of branch footfall from POca customers.	2	12
5	Manage process and deliver services	ATM operational availability is less than 96% resulting in lost revenue.	2	12
6	Contract Management	Non-compliance in branch leads to breach of contract and financial penalties.	2	10
7	Compliance with laws and regulations	VOA reconsiders their operational decision to exclude Bank of Ireland ATMs in Post Office branches from separate assessment and agents become unwilling to host BoI ATMs.	2	9
8	Ensuring sustainable profit	There is a risk that non-cash payments costs are increasing due to unpredictable scheme fee changes and regulatory changes.	2	9
9	Manage process and deliver services	New - There is a risk that DVLA cease credit card as a payment method at Post Office branches due to an inability of POL to add the legislative charge for commercial cards.	2	8
10	Procure	Procurement exercise to replace PayStation by end May 2018 is unsuccessful and Ingenico ceases to service or support the current model, adversely impacting our ability to deliver bill payment services.	2	8
11	BCP (excl ITDR)	No known contracts in force for 45 client and supplier business relationships.	2	8
12	Competitiveness	We are unable to compete effectively in the bill payments marketplace and are unable to gain market share.	2	8
13	Competitiveness	New - Prior to contract exchange, market is informed of the deal before going public.	2	8

Heatmap



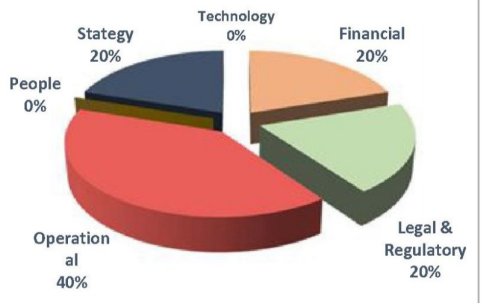
Risk Headline

No of Risks (Open or New)	15
No of Red Risks	5
No of Amber Risks	10
No of Green Risks	0
No of Red risks with ineffective controls	0
No of New Risks	8
No of Closed Risks	5

Control Headline

No of Risks assessed as effectively controlled	0
No of Risks Self assessed as partially controlled	15
No of Risks assessed as ineffectively controlled	0

Top Risks by Principal Title



Control Self Assessment



POL00401626

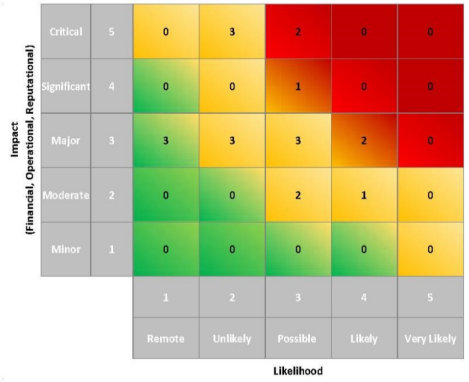
Appendix 4e

Retail – Network & Sales Dashboard (5/5)

Top Risks by Risk Score

#	Principal Risk Title	Risk description	CSA	Residual Risk Score
1	Business Interruption (ITDR)	Failure of IT infrastructure disrupts branch network leading to operational disruption and poor customer experience.	2	15
2	Ensuring sustainable profit	Reduction in agents' remuneration makes branches less sustainable and leads to reduction in staff numbers with negative impact on customer experience.	2	15
3	Managing change	Proposed changes to the Directly Managed Branch network and other business issues create stakeholder noise, which leads to reputational damage.	3	12
4	Contract Management	New - The transition of our retail offer now being provided by WHS has led to some initial gaps in our Postpak range with the risk to sales levels, commission and customer experience.	2	12
5	Managing change	New- Changes to products, processes or systems agreed in other parts of the business have a negative impact on customer experience in branch.	2	12
6	Compliance with laws and regulations	Failure to comply with legal or regulatory requirements, including mis-selling, non-compliant marketing and misuse of customer data, leading to poor customer experience and reputational damage.	3	10
7	Keep our people, customers and third parties safe	Risk of harm or breach of regulatory requirements caused by failure to follow Health and Safety procedures.	2	10
8	Compliance with laws and regulations	New-Serious regulatory breach involving customer detriment due to mis-selling of EasyLife product (term life assurance).	2	10
9	Technology Ops	New - Branch technology refresh causes unplanned operational disruption in DMBs.	2	9
10	Competitiveness	New - Changes in the methodology of gathering customer feedback result, could show a decline in feedback received and feedback becomes unrepresentative.	2	9
11	Communicate, inspire and align	New - Unable to influence whole network effectively to ensure consistent customer experience.	2	9
12	Managing change	Proposed changes to the Directly Managed Branch network lead to industrial action which causes operational disruption and reputational damage.	2	8
13	Communicate, inspire and align	Uncertainty around branch futures and a lack of suitable development opportunities lead to loss of key staff to other areas of the business or externally.	3	6
14	Keep our people, customers and third parties safe	New - Security risk due to inability to follow security guidelines at hosted branches because of difference in opening hours between PO and WHS host.	3	6

Heatmap



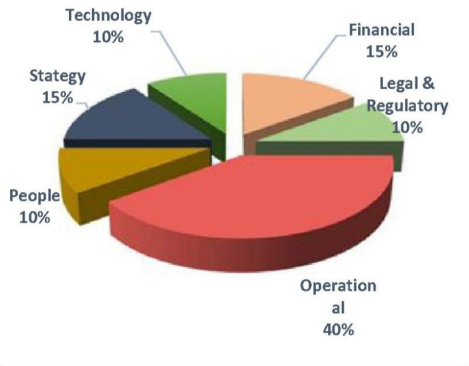
Risk Headline

No of Risks (Open or New)	20
No of Red Risks	5
No of Amber Risks	12
No of Green Risks	3
No of Red risks with ineffective controls	0
No of New Risks (8 top risks)	12
No of Closed Risks	0

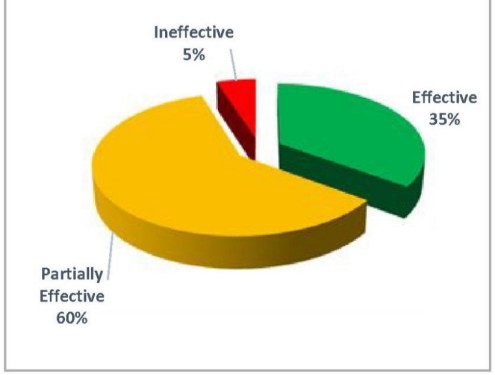
Control Headline

No of Risks assessed as effectively controlled	7
No of Risks Self assessed as partially controlled	12
No of Risks assessed as ineffectively controlled	1

Top Risks by Principal Title



Control Self Assessment



POL00401626

Appendix 5

F&O Dashboard

Top Risks by Risk Score

F&O Top Risks by Score						Q3			Q4				
#	Risk Description	Business Area	Principal Risk	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Impact	Likelihood	Risk Score	Q4 Commentary	Movement
1	High levels of change may cause fragile legacy systems to fail during the migration period.	Finance and Operations	Managing change	Ben Cooke	Tim White	4	4	16	4	4	16	HR SAP, which is out of extended support, is on track to be decommissioned following the deployment of SuccessFactors and expected migration of Agent Remuneration in February (see Risks 4 & 5). Our small apps (SQL & CRM) have been migrated into a secure data centre and consolidated. However areas of concern remain – the highest risks being POLSAP and legacy systems at Swindon. POLSAP is closely monitored and reported on with a number of remedial activities taking place and additional spares being procured. Plans to improve Swindon until a strategic solution is in place are progressing.	◁▷
2	Failure of POLSAP legacy system, results in severe operational disruption.	Finance and Operations	Business Interruption (ITDR)	Michael Passmore	Ben Cooke	5	3	15	5	3	15	The Back Office programme will migrate POLSAP to CFS. The programme scope covers a number of processes which drive our financials (e.g. client settlements, branch transaction corrections). Significant testing will take place and each area will be subject to a "go / no-go" decision by the programme team and Exec sponsors, where all risks will be discussed and 'go live' only approved if any remaining risks are extremely low. A controls specialist joined the programme team in November 2017 and has been overseeing the production of Business Process douments and documenting controls for each process impacted by the programme; the BPDs and controls matrices will all be reviewed and signed off by the Financial Accounting & Governance Manager and the Finance Director, POL. User access controls are also being developed with oversight from the controls specialist on the programme and the Financial Accounting & Governance Manager.	◁▷
3	Safety outcomes are not world class and where they are not in line with required legal and regulatory standards, may lead to serious injury.	Finance and Operations	Keep our people, customers and third parties safe	Angela Van-Den-Bogerd	Martin Hopcroft	5	2	10	5	3	15	Likelihood increased due to an increase in minor accidents in Supply Chain since the last refresh. Proactive approach to health and safety management being rolled out across Supply Chain, including training Safety Champions in each business unit and setting up a Safety Forum to provide support and guidance. A Road Risk Forum is already operating and providing guidance on road safety issues.The scope of agent activities and opportunity for Post Office to provide guidance is under review in Q4. To assess the robustness of the Safety Management System and to identify improvement opportunities to meet World Class level, an independent 3rd party audit is being undertaken by HSL / HSE with interviews held across the business, including front line, line managers, senior leaders and GE. A report has been shared with GE and PO Board.	△
4	Unable to deter agent theft or fraud and unable to recover agent debt effectively due to failure to prosecute.	Finance and Operations	Managing losses and Fraud	Stuart Nesbit / Mark Ellis	Sally Smith	2	5	10	3	5	15	Impact increased due to an increase in identified agent fraud and debt. Faster debt path processes approved and implemented in FSC. Increased levels of agent debt identified IRRELEVANT Effective recovery prevented by inability to prosecute. The Fraud Analysis team have completed implementation of EXL Analytics tool. Use of tool in pilot exercise identified branches which had not been flagged by existing detection methods. Increased number of audits performed in the quarter and further increase in capacity to carry out audits in Network Operations from April 2018. Period 9 **YTD 17/18**/ YTD16/17 **IRRELEVANT**	△

POL00401626

Appendix 5 (cont)

F&O Dashboard

Top Risks by Risk Score

F&O Top Risks by Score						Q3			Q4				
#	Risk Description	Business Area	Principal Risk	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Impact	Likelihood	Risk Score	Q4 Commentary	Movement
5	We make poor decisions because our MI is limited.	Finance and Operations	Reporting results and providing data accurately	Somita Yogi	Tim White	2	5	10	3	5	15	Impact increased to reflect the recognition that the lack of dependable and accessible MI can pose a limit to further improvements in business processes and ways of working. Project Arrow has been initiated and was presented to GE in November 2017 & got approval from CAG in Jan 2018. Currently engaging with GE members to get Data strategy completed and will present Data Strategy in March 2018. Started working on Data Governance, Data Quality, Data Operations and other streams of Arrow. We will also have a proof of concept delivered for Visualisation tool under Arrow.	△
6	Limited DR/BCP plans, largely untested increase the impact of systems and site loss.	Finance and Operations	BCP (excl ITDR)	Various	Tim Armit	3	3	9	4	3	12	Impact increased due to increasing risk posed by aged systems and untested plans. Plans are under way to test Chesterfield in March and Bolton in April 2018. Swindon relies on aged legacy IT systems and work will be carried out with IT to gain a better understanding of the IT DR requirements of the site before planning a live test.	△
7	Loss of Swindon operation causes widespread product loss.	Finance and Operations	BCP (excl ITDR)	Russell Hancock	Tim Armit	3	3	9	4	3	12	Impact increased due to increasing risk posed by aged systems and untested plans. Possible options for the Swindon site have been considered and we are now engaging with Royal Mail to establish what both businesses want from the relationship, which will inform our final decision on the site and future IT solutions.	△
8	Financial Reporting is inaccurate creating reputational damage.	Finance and Operations	Reporting results and providing data accurately	Michael Passmore	Johann Appel	5	2	10	5	2	10	The Financial Reporting Controls project scope is currently being extended to cover Masterdata and FSC processes. Further work will be performed to extend this to cover agent debt, POMS processes, and cash management and forecasting. Existing controls are self-assessed by owners on a monthly basis in TrAction and sample testing is performed within the FRC team. Results of external testing of controls by PwC have been reported to RCC/ARC and were generally good; improvements were recommended in relation to spreadsheet controls and these have now been implemented. PwC are performing further testing prior to FY17/18 year end. Risk remains the same in areas not yet covered by the project, we will have a better view of any new risks emerging as we complete these areas and identify gaps.	◁▷
9	Informal controls and compliance over Operations, weakens the internal control environment, leading to oversight failure.	Finance and Operations	Reporting results and providing data accurately	Various	Johann Appel	2	5	10	2	5	10	See risk 8.	◁▷

POL00401626

Appendix 5 (cont)

F&O Dashboard

Top Risks by Risk Score

F&O Top Risks by Score						Q3			Q4			Q4 Commentary	Movement
#	Risk Description	Business Area	Principal Risk	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Impact	Likelihood	Risk Score		
10	Our change is delivered late, risking costs and benefits or has unintended consequences.	Finance and Operations	Managing change	Angela Van-Den-Bogerd	Tim White	2	5	10	2	5	10	A series of proposals on structure, governance, culture and competency elements of Post Office change management were presented at the November 17 GE and approved. Work has commenced with PA to: • Transfer the executive sponsor of change to Rob Houghton and recruit a new Change Portfolio and a new Finance Lead. Both Rob and Tim have vast experience of managing large change portfolio which will benefit POL – Complete • Share with L300 the new vision and cultural shift for change, this will help to get management to understand the importance of change and support the new ways of working – Complete • Implementation of a Strategic Portfolio Office (SPO) and recommend the Target Operating Model which should be in place, this will ensure POL maximise the RoI on strategically aligned initiatives – End of Mar 18 • Create a new Investment Committee – develop TOR, attendees, roles and responsibilities, again this will support POL to maximise the RoI on strategically aligned initiatives – End of Feb 18 • Develop a project prioritisation methodology, which prioritises those initiatives that contribute the most to the PO's strategy and financial objectives – Mid Mar 18. • Build a phased transition plan to implement the new strategic portfolio office and processes which help increase delivery success and reduce the risk of late / poor delivery (including the introduction of an agile delivery and governance process) - End of Mar 18	◁▷
11	Unable to demonstrate compliance on agent vetting and training.	Finance and Operations	Compliance with laws and regulations	Angela Van-Den-Bogerd / Mark Ellis	Various in LRG	2	5	10	2	5	10	Smart ID (part of EUM) rolled out to 1000 branches (including top FS branches) but not fully implemented as old sign on still operational.	◁▷
12	Loss and churn due to a lack of training and support for newer agents.	Finance and Operations	Manage process and deliver services	Mark Ellis	Jackie Newton	2	5	10	2	5	10	Structural review of field teams completed and phase 1 of restructure commenced end January. Phase 2 to take effect in April 2018. 1 month and 3 month post-appointment visits now taking place. Initial training package reviewed and pilot being carried out in Q4. Joint wider review of training strategy to be carried out with Learning & Development team, due to report in Q2.	◁▷
13	Lack of effective communication resulting in lower levels of staff engagement.	Finance and Operations	Communicate, inspire and align	Russell Hancock	Mark Davies	2	5	10	2	5	10	Efforts being made to use Yammer to encourage more open communication throughout Finance and Operations. Unit programme in Supply Chain is starting to bring operational teams together to work through local issues and solutions.	◁▷
14	Cash is not managed efficiently, leading to increased risk of loss, funding costs and restrictions on change funding.	Finance and Operations	Sufficient cash / headroom	Russell Hancock	Mark Dixon	3	4	12	3	3	9	Likelihood decreased due to improved controls over cash management. Cash Management Project due to complete March 2018. IRRELEVANT IRRELEVANT IRRELEVANT. Increased reliability of CViT performance helping to move this in the right direction too. Have now started to map impact of potential increased transactions as a result of banking framework.	▽

POL00401626

Appendix 5 (cont)

F&O Dashboard

Top Risks by Risk Score

F&O Top Risks by Score						Q3			Q4			Q4 Commentary	Movement
#	Risk Description	Business Area	Principal Risk	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Impact	Likelihood	Risk Score		
15	Failure to transition agents pay from HR SAP, which is unsupported to CFS could result in none payment of remuneration and tax payments to HRMC leading to regulatory action and/ or loss of reputation.	Finance and Operations	Managing change	Angela Van-Den-Bogerd	Nick Beal	4	3	12	4	2	8	Likelihood decreased due to successful testing. The process for transferring agents pay from HR SAP to CFS has been thoroughly tested and we are confident this will be as successful as the employee payroll transferred in January. On track to transfer by end Feb.	▽
16	We do not have sufficient funds to create a sustainable business.	Finance and Operations	Ensuring sustainable profit	Michael Passmore	Johann Appel	4	2	8	4	2	8	A number of initiatives are in place to ensure efficient use of our working capital (particularly our cash inventory) to ensure we create as much headroom under our facilities as possible. In addition, we are formulating i IRRELEVANT IRRELEVANT IRRELEVANT Both these initiatives will create additional headroom capacity under existing facilities.	◁▷
17	Limited cash data and forecasting leads to a facility breach.	Finance and Operations	Sufficient cash / headroom	Michael Passmore	Johann Appel	4	2	8	4	2	8	We continue to focus on improving cash flow forecasting. The Cash Management project is due to complete in March 2018. Due to resource constraints in the Wholesale Cash Team it has not yet been possible to implement the new model which has been developed for forecasting Note Circulation Scheme balances but the old model continues to work effectively albeit with room for improvement. KPMG have completed their review and are working to present their results. The same team is also working on a project with Supply Chain.	◁▷
18	We cannot report, forecast or optimise branch cash.	Finance and Operations	Reporting results and providing data accurately	Russell Hancock	Mark Dixon	2	4	8	2	4	8	New system Cash Web Community (CWC) from Transtrack being implemented as part of the Back Office Programme will enable more accurate forecasting and allow branches to order cash online. Pilot of CWC at Belfast cash centre due to go live March 18. The other cash centres are due to move to CWC by June 2018. Once the system is up and running smart technology will be progressively rolled out to frontline CVIT crew which will allow Supply Chain to introduce greater flexibility into cash deliveries and collections allow better optimisation of cash.	◁▷
19	Unable to achieve operational conformance due to limited monitoring of and communication with agents.	Finance and Operations	Compliance with laws and regulations	Mark Ellis	Various in LRG	2	3	6	2	4	8	Likelihood increased to reflect the fact that technology solutions (EUM) have not yet been fully implemented. Measures in place to improve conformance include the planned implementation of EUM (Smart ID now rolled out to 1000 branches), the Cash Management project, technical changes including the automation of cash declarations and changes in incentivisation for the Mail Segregation targets. Communication is being improved through an improved capacity to make calls in the Branch Standards Team, improved training and support from the Network Operations field teams and the roll out of the Agent Portal.	△

POL00401626

Appendix 5 (cont)

F&O Dashboard

Top Risks by Risk Score

F&O Top Risks by Score						Q3			Q4			Q4 Commentary	Movement
#	Risk Description	Business Area	Principal Risk	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Impact	Likelihood	Risk Score		
20	We are not compliant on tax attracting fines and censure.	Finance and Operations	Record and pay taxes	Michael Passmore	Jane MacLeod	3	2	6	3	2	6	Tax manager in post and processes being embedded. Additional support provided by external specialists.	◁▷
21	We procure badly, destroying value.	Finance and Operations	Procure	Barbara Brannon	Jane MacLeod	3	2	6	3	2	6	Work is under way to procure and implement a Contract Management System.	◁▷
22	Telephony system is unstable and we cannot maintain service to customers and agents.	Finance and Operations	Business Interruption (ITDR)	Mark Ellis	Roger Gale				3	2	6	Transfer from BT to Verizon implemented 3 Nov 2017 but system lacks functionality. High levels of calls due to POCA letter in w/c 13 Nov required interim solution in which POCA calls are handled by BT - this is due to be transferred to TalkTalk mid-Feb. Phase 2 will be to move rest of POEX call plan from Puzzel to Talk Talk. Current uncertainty about capacity of system when BT contract ends (March 2018) - Verizon are supposed to be providing a solution. Overall solution will be fragmented and involve Verizon, TalkTalk and Puzzel.	NEW
23	Financial forecasting is limited.	Finance and Operations	Sufficient cash / headroom	Michael Passmore	Johann Appel	1	5	5	3	2	6	Permanent head of FP&A took up post in February 2018.. Current reporting and forecasting processes will be reviewed to identify opportunities for improvement.	△
24	We appoint unsuitable applicants leading to performance issues and re-work due to increased terminations through losses.	Finance and Operations	Manage process and deliver services	Mark Ellis	Roger Gale	2	5	10	2	3	6	Organisational changes to bring all the field teams into Network Operations (from April 2018) and realignment of objectives have reduced the likelihood of accepting unsuitable applicants. Work is underway to implement the recommendations of the review of the applications process but progress is hampered by a lack of capacity in the Agents Contracts Team due to increased workload.	▽
25	We procure illegally, attracting fines and censure.	Finance and Operations	Procure	Barbara Brannon	Jane MacLeod	2	3	6	2	3	6	No change for Q4.	◁▷
26	We do not keep cash physically secure resulting in financial loss to PO.	Finance and Operations	Physically secure	Russell Hancock	John Flood	5	1	5	5	1	5	No change for Q4.	◁▷

POL00401626

Appendix 5 (cont)

F&O Dashboard

Top Risks by Risk Score

F&O Top Risks by Score						Q3			Q4			Q4 Commentary	Movement
#	Risk Description	Business Area	Principal Risk	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Impact	Likelihood	Risk Score		
27	Risk of kidnap in Supply Chain and branch network.	Finance and Operations	Keep our people, customers and third parties safe	Mark Ellis	Martin Hopcroft	5	1	5	5	1	5	Tiger Kidnap policy and procedure in place. Procedure being revised to call police directly, instead of via Grapevine, in the event of an incident. Due to go live April 2018. Training delivered annually to all staff in Supply Chain.	◁▷
28	Risk of political/social violence in Northern Ireland.	Finance and Operations	Keep our people, customers and third parties safe	Mark Ellis	Mark Davies	5	1	5	5	1	5	No change for Q4.	◁▷
29	Unable to perform client settlement.	Finance and Operations	Make payments	Stuart Nesbit	Johann Appel	4	2	8	4	1	4	Likelihood decreased due to successful live testing of contingency plans. Contingency plans in place and live testing carried out resulting in successful and accurate settlement.	▽
30	Fail to pay suppliers within timeframes required by statutory payment guidelines.	Finance and Operations	Compliance with laws and regulations	Stuart Nesbit	Barbara Brannon	1	4	4	4	1	4	Processes in place and working to at over 95% of invoices paid within 30 days, with actions to move to full conformance.	◁▷
31	Failure to migrate staff payroll from HR SAP, which is unsupported, to SuccessFactors could result in delayed and / or inaccurate salary payments to staff and some agents. This could lead to regulatory action and/ or loss of reputation, also potential employee relations issues at a time of heightened tension.	Finance and Operations	Managing change	Angela Van Den Bogerd	Nick Beal	4	3	12	3	1	3	Impact and likelihood decreased due to successful migration at end of January. Staff payroll migrated to SuccessFactors completed January 2018. All employees successfully paid at the end of January, very few issues reported and all problems relating to employee pay fixed almost immediately.	▽
32	Insurance coverage is insufficient to cover risks or liabilities.	Finance and Operations	Ensuring sustainable profit	Michael Passmore	Jane MacLeod	3	1	3	3	1	3	The broker (Lockton) has been engaged for the past 3 years. The broker understands the business and engagement is good. Appropriateness of coverage is considered at renewal.	◁▷

POL00401626

Appendix 6

LRG Dashboard

Top Risks by Risk Score

LRG Top Risks by Score					Q3			Q4			Q4 Commentary	Movement
#	Risk Description	Principal Risk Category	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Impact	Likelihood	Risk Score		
High Risk												
1	Failure by Post Office to ensure operational activities, IT infrastructure/security and related services are PCIDSS compliant may cause challenges during external audit, require significant remediation activities and attract unbudgeted costs. This may result in a failure to obtain the required certification, breach our agreed banking framework and may lead to a legal/regulatory breach, financial loss and reputational damage.	Information Protection	Jules Harris	Ehstham Ali	5	4	20	5	4	20	Our ability to achieve and maintain **PCI accreditation** is a significant challenge and if we are unable to achieve compliance could lead to significant fines or the removal of our ability to process card payments. The standards are predominately set to ensure security of card data. Non-compliance may result in Post Office being considered an easy target to fraudulently obtain card data. The cost of any such breach could be far higher (both financially and reputational). Next steps: • Audit against V3.2 of the PCIDSS Standard was not successful resulting in failure to obtain a positive Report on Compliance (RoC) • Remediation is underway by Fujitsu and Computacenter • Physical Audit is continuing across our Branch Network • Target date for a successful RoC is 31 March. However, this is dependent on Computacenter's remediation activities being delivered on time. PO confidence in the ability of ComputaCenter to deliver by the new deadline is low.	◁▷
2	There has been a material delay to the programme that has been caused, principally, because of: - A lack of documentation - Scale and complexity - Availability of resources Further delay could impact upon POL's ability to achieve effective compliance by the time GDPR comes into force on 25 May 2018.	Information Protection	Jules Harris	Claire D'Netto	3	3	9	4	4	16	The Programme delivering GDPR compliance for Post Office is challenged, and the ability to achieve effective compliance by the implementation of the act is also at risk. Additional resource is being allocated to ensure that key deliverables remain on-track. **Getting the information we need** To baseline the scope of assets, we need to identify PO products, suppliers, systems and contracts and prioritise based on risk. We need confirmation of Product and Contract Managers to validate our view. The documentation / corporate knowledge we would expect is not readily available so we need to work with suppliers and their Contract Managers to create it. We will be completing retrospective PIAs with Product Managers and the business to create records of processing activities. **Scale and Complexity** The sheer scale of Post Office operations in terms of numbers of products (c117), IT suppliers (100+) (and associated systems) and contracts (600+) means that we have prioritised analysis into tranches and are running this on an agile basis. We are now getting traction using this approach. The complexity is due to the dependencies with other projects which will impact on personal data. Specifically we need to align the GDPR Programme with key IT transformational projects to ensure the appropriate controls are built into third party contracts that are being renegotiated or replaced. **Availability of resources** There are capacity constraints in the BAU DP Team, so we are recruiting interim Data Protection SMEs which are scarce due to demand in other GDPR programmes. It has taken us 3 months to fill a key senior role (ETA 2/10) and we are now looking for a more junior DP resource to provide additional capacity.	△

POL00401626

Appendix 6 (cont)

LRG Dashboard

Top Risks by Risk Score

LRG Top Risks by Score					Q3			Q4				
#	Risk Description	Principal Risk Category	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Impact	Likelihood	Risk Score	Q4 Commentary	Movement
3	Failure to identify and control the insider threat and include security controls in contracts with suppliers.	IT Security	Jules Harris	Mick Mitchell	4	3	12	4	3	12	The Security Operations Centre (SOC) will be established in the over the next 6 to 9 months, providing oversight of all security controls from each provider, centralise and aggregate events and incidents to enable POL to react against security issues efficiently and effectively, thereby reducing our risk exposure.	
Medium Risk												
4	Adverse outcome from current Group litigation.	Litigation	Jane MacLeod	Mark Underwood / Rodric Williams	5	2	10	5	2	10	POL has in place a Steering Group with attendees from across the business with appropriate level of seniority to ensure that the resource, decisions, materials and documentation necessary for POL to be able to robustly defend its position are available to it.	
5	Failure to comply with contractual requirements.	Contract Management	Ben Foat	Ben Foat	3	3	9	3	3	9	The Bravo central contract repository system is owned by the Procurement Team but maintained by both Procurement and Legal teams. Contracts are required to formalise our commercial relationships and transactions. The terms and obligations in those contracts need to be managed / adhered to. As of February 2018, a business case has been drafted and is being driven by Ben Cook's team (CIO Back Office Technology & Transformation) for a longer term contract management system solution accommodating legal needs. The Legal Team has been involved throughout the project and been feeding in requirements which will form part of the business case. As of February 2018, the Contract Obligations Spreadsheet has been updated and will be finalised shortly. The Contracts Obligations Spreadsheet will reflect the current position of material contracts (Legal).	
6	Poor contract management.	Contract Management	Ben Foat	Ben Foat	3	3	9	3	3	9	LRG SLT member is to attend the Finance and Operations Lead Team meeting. Members of the Legal team currently attending various Lead Team meetings (including the Financial Services Lead Team meeting the Banking Lead Team meeting and others) to discuss Framework / minimum control standards for Contract Management. As of February 2018, a business case has been drafted and is being driven by Ben Cook's team (CIO Back Office Technology & Transformation) for a longer term contract management system solution accommodating legal needs. The Legal Team has been involved throughout the project and been feeding in requirements which will form part of the business case.	

POL00401626

Appendix 6 (cont)

LRG Dashboard

Top Risks by Risk Score

LRG Top Risks by Score					Q3			Q4				
#	Risk Description	Principal Risk Category	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Impact	Likelihood	Risk Score	Q4 Commentary	Movement
7	Regulatory Compliance and increased visibility of POL and POMS to regulators e.g. ICO re GDPR, HMRC re AML/CTF, FCA re POMS expansion, FCA via Banking Framework, OFCOM re Mails and Telco.	Compliance with laws and regulations	Jane Macleod	Ben Foat	3	3	9	3	3	9	A Regulatory and Legislative Framework has been developed and circulated to the GE for their business areas as well as tabled at RCC last September. Earlier this year, GE accountability for the key piece of legislation and regulation applicable to POL has assigned to GE members. Since then, the Regulatory and Legislative Framework has been shared with the business areas through the Law and Trends Forum. The Regulatory and Legislative Framework will be maintained and periodically reviewed and updated by the Legal team. Follow up meetings have been held with each GE member to agree accountabilities and responsibilities. A gap analysis will be performed. A second paper has been discussed at RCC on the Criminal Finances Act. In addition, POL is putting together a case with relevant stakeholders in Government regarding the increasing compliance requirements and their impact on the POL business. As of February 2018, the Legal team is working on the Directors Induction Pack, a document to be shared with new directors/executives which will provide an overview of any regulatory impact on POL/POMS.	◁▷
8	Risk management isn't fully developed and embedded, e.g., no mature risk culture, monitoring, oversight, appetite, policy and compliance framework.	Governance	Richard Williams, Deana Herley	Richard Williams, Deana Herley	3	3	9	3	3	9	The Placemat approach / methodology is being rolled out across the business to formalise, embed and create a single view of the risk and control environment. The Placemat outputs have been aligned to the Enterprise Risk Management Framework. Further enhancements, such as appetite will be considered in 2018.	◁▷
9	We do not have sufficient or appropriate BCP arrangements in place that are documented, understood and tested.	BCP	Tim Armit	Tim Armit	3	3	9	2	3	6	BC risks, impacts and strategies will be developed across all areas in 2017/18. Development of business continuity plans has started. Business awareness and training sessions have commenced and will continue through the next quarter. Process to invoke Business Protection Team in case of incidents has been put in place and is working effectively. As a result the impact of incidents has reduced, however, the likelihood remains unchanged due to lack of documented plans and testing (that will follow once plans have been documented).	▽
Low Risk												
10	Policies do not exist or have not been properly reviewed.	Governance	Jane MacLeod	Jane Macleod	2	2	4	2	2	4		◁▷

POL00401626

POST OFFICE
RISK AND COMPLIANCE COMMITTEE

INFORMATION PAPER

Financial Crime Pilot

Author: Ashish Singh/Sally Smith Sponsor: Jane MacLeod Meeting date: 13 March 2018

Executive Summary

Context

The purpose of this paper is to provide the Committee with an overview of the 'Horizontal' Placemat governance and reporting context and proposed approach.

Questions this paper addresses

1. What is the purpose of 'Horizontal' Placemat governance and reporting?
2. How are we planning to do it?
3. What are the next steps in the rollout?

Conclusion

1. The Risk Placemat roll-out will provide each business area (verticals) with a 'bottom-up' view of their risks, and an assessment of how effectively those risks are being managed. This in turn will facilitate the reporting of their 'top risks'. The rollout of the Risk Placemat is on track to be completed by June 2018.
2. To further enhance our understanding and management of risk, we are developing an approach to test the integrity, and formalise the governance and reporting, of the key principal risks (horizontals), ready for embedding prior to full Placemat implementation.
3. Pilots are underway, covering Information Protection, IT Security and Financial Crime principal risks. We are also proposing to run pilots for BCP and Health & Safety.
4. The pilots focus on governance, assurance and reporting over principal risks, including risk profile, risk appetite, key risk indicators, risk exceptions, controls effectiveness, policy compliance, incident management and action tracking.
5. The outputs from the pilots will support our understanding of how we should 'end to end' assure the completeness, quality and consistency of the business areas view (verticals), to support the formulation of a consolidated Post Office view. The overall risk picture will help to focus dialogue on the highest risk items.
6. We expect to report on the 4 pilots at the June Committee.

Input Sought

The Committee is asked to note this paper, provide comment as necessary, and approve the Terms of Reference for the Financial Crime Committee.

POL00401626

POST OFFICE

The Report

What is the purpose of 'Horizontal' Placemat governance and reporting?

1. The Risk Placemat roll-out will provide a comprehensive baseline view of the top risks facing each business area, and an assessment by respective management of how effectively those risks are being managed (verticals). The rollout of the Risk Placemat is on track to be completed by June 2018.

2. However the vertical view, by itself, will provide an incomplete view of the overall risk profile for the Post Office on account of the following:
   a. No visible linkage of Placemat to minimum controls in policies;
   b. No visible linkage or consideration of incidents and exceptions in the Placemat roll-out;
   c. No functional assurance on Principal Risks which appear across multiple verticals; and
   d. No reflection of performance against risk appetite

3. To further enhance our understanding and management of risk, we are developing an approach to test the integrity and formalise the governance and reporting of the key principal risks (horizontals), ready for embedding prior to full Placemat implementation.

4. It will enable us to review the reporting in relation to the current 'perimeter' risks to ensure they align to the Placemat, reflect the policy requirements and enable consistent use of data sets.

5. The purpose of horizontal governance and reporting is to provide the GE owners for the Principal risks, and through them, to this Committee:
   a. Assurance over the consistency of Placemat roll-out across Businesses for the same principal risk;
   b. Assessment of root causes and common themes underpinning vertical risk assessment;
   c. Identification and consideration of interdependencies between Business areas in managing their risks;
   d. Review of material incidents and risk exceptions across Post Office for the relevant principal risks;
   e. Assurance over effectiveness of controls and compliance with applicable policies
   f. Progress on agreed actions in relation to improved mitigation of principal risk across the organisations; and
   g. An overall assessment of the principal risk position at the Post Office level and in comparison to its stated risk appetite for that principal risk.

POL00401626

POST OFFICE

How are we planning to do it?

6. We are running a series of pilots to develop and validate our approach to Horizontal governance and reporting. In Wave 1, currently underway, our pilots cover the following principal risks:
   a. Financial Crime – *via the Financial Crime pilot*
   b. Information Protection – *via the Information Security pilot*
   c. IT Security during - *via the Information Security pilot*

7. These principal risks have been selected as they have a cross-business footprint, have a set of Post Office policies defined for them, and are key areas of focus for both the RCC and the ARC. Governance fora are also being developed for each.

8. The scope of these pilots includes developing proposals for:
   a. Establishing Terms of Reference for relevant governance bodies;
   b. Clarifying ownership and accountability between the Business (risk owners) and Functions (assurance providers);
   c. Developing MI for tracking risk performance, including assessment against risk appetite;
   d. Designing dashboards for risk and compliance reporting; and
   e. Defining functional assurance scope and approach

9. Stakeholders from across the relevant business and functional areas are actively involved in these pilots.

10. Appendix 1 includes the Terms of Reference for the Financial Crime Committee, which has been reviewed by the Financial Crime Committee. It is proposed that the Financial Crime Committee will be a sub-committee of the Risk and Compliance Committee, hence we seek approval for these Terms of Reference.

11. Appendix 2 includes the Risk and Compliance reporting dashboard for Financial Crime. *(A3 copies will be provided during the Committee meeting)*

POL00401626

POST OFFICE

What are the next steps in the rollout?

12. Wave 1 pilots will be completed and results compiled and reviewed by the Financial Crime Committee and Information Security Committee, respectively, before the end of June. We will start reporting on these Principal risks on an ongoing basis to the RCC and the ARC from July onwards.

13. We will also be commencing Wave 2 pilots. Subject to the views of the RCC, we propose to cover the following principal risks:
    a. Business Continuity Planning
    b. Health and Safety

POL00401626

POST OFFICE

Appendix 1

Financial Crime Committee Terms of Reference

1. Purpose:

The overall objective of The Financial Crime Committee (FCC) is to provide oversight of Post Office's management of Financial Crime related risks, internal controls and compliance on behalf of the Risk and Compliance Committee (R&CC), including:

i. Assessing Financial Crime risk causes and impacts so that they are properly understood, and proportionately, consistently and effectively managed across Post Office, in line with the Board approved risk appetite;
ii. Monitor compliance by Post Office, its products and services, and its partners, suppliers and employees, with relevant regulatory requirements including Anti Money Laundering (AML), Counter Terrorist Financing (CTF) and Anti Bribery and Corruption (ABC);
iii. Enabling the Senior Officer (the Group Director of Legal, Risk and Governance) to oversee business regulatory obligations in compliance with the 2017 Money Laundering Regulations
iv. Reviewing Financial crime policies that impact AML, CTF and ABC, including minimum control standards;
v. Recommending remediation activities and monitoring their completion in respect of:
    a. Functional assurance and Internal Audit
    b. Regulatory changes
    c. Incidents
    d. The HMRC audit action plan
    e. Product and Service risk assessments; and
vi. Assessing external threats and regulatory developments.

2. Scope:

The scope of the FCC includes Anti-Money Laundering, Counter Terrorist Financing and Anti-Bribery and Corruption.

3. Specific responsibilities of the FCC will include:

- Reviewing the overall Post Office risk profile against risk appetite and the effectiveness of the control framework
- Reviewing draft and updated policies, prior to submission to the R&CC and Audit & Risk Committee (ARC) for approval
- Reviewing risk profile at individual Business Unit or Function level ensuring there is sufficient and effective mitigation activity
- Reviewing functional and independent assurance results to corroborate management's self-assessment, ensure consistency across Business Units and Functions, and discuss common risk themes and root causes
- Reviewing any proposed policy exception requests
- Monitoring the progress of remediation plan activity
- Reviewing residual risk from product and service risk assessments
- Reviewing non-conformance and 'Fit & Proper' status issues across the Network
- Reviewing any material Financial Crime issues or incidents affecting Post Office, including supplier related issues

POL00401626

- Reviewing operational resource to ensure adherence to regulatory requirements relating to Suspicious Activity Reporting submission and transaction monitoring
- Monitoring the status of change programmes that impact the risk
- Maintaining oversight over current and emerging threats and developments that could impact Post Office
- Discuss and agree R&CC and ARC report subjects/content

4. Authority

Decision making will be made within the FCC members usual business delegated authority.

5. Membership

The membership shall comprise:

- Group Director of Legal, Risk and Governance (chair)
- Director of Risk & Compliance/MLRO
- Head of Financial Crime
- Head of Financial Service and Telecoms Risk and Regulation
- POMS Director of Risk & Compliance
- Network Operations Director

Attendees must nominate a deputy of sufficient seniority who can represent them should they be unavailable to attend the meetings.

The Chair may require other colleagues to attend all or part of meetings as appropriate, including (but not limited to):

- Relevant Product Managers
- Head of Fraud Analysis and Branch Standards
- Sales and Trade Marketing Director
- Network Development Director
- Government and Payment Services Director
- HR Director

The quorum shall be a minimum four members one of which must be the Chair (or their designated representative).

6. Meetings

- The FCC shall meet monthly.
- Minutes of each meeting will be issued to all members.

7. Standing Agenda Items

- Approval of previous minutes and review of actions
- Review of Financial Crime risk dashboard and Business Unit or Functional summaries
- Financial Crime MI:
    - Key risk indicators and metrics

POL00401626

  - Incidents
  - Non-conformance/Fit & Proper issues
  - Operational activity
- Review of internal and external audits and actions plans impacting Financial Crime, including HMRC
- Review of product and service risk assessments
- Review of material issues/incidents
- Review of regulatory change and emerging threats

8. Reporting

Bi-monthly noting or escalation papers to R&CC and, as required, the ARC.

POL00401626

POST OFFICE

Financial Crime Risk Dashboard

Appendix 2

FINANCIAL CRIME – RISK REPORT [March 2018 (Q4)] — **Financial Crime Committee**

- The HMRC audit identified we are not collecting or can not evidence the required information required by the AML requirements in respect of our bureau transactions in the network. However there is a risk we may not delivery the required changes within the deadlines outlined in the plan. Risk has increased as HMRC are changing their position in relation to KYC recording requirement. Regular engagement continues with HMRC.
- Progress has been made on risk assessing and remediating product risks. Awaiting updated Product Information Packs to commence 2018 assessment and further reduce product risk.
- c33% of risks (20 out of 62) are currently owned by LRG. Since LRG (and the FC team within it) is predominantly an advisory and assurance function (2nd line), we would expect to see more Financial Crime related risks being identified, owned and managed within the business areas (esp Retail).

RISK PROFILE (Number of Risks = 62)

from Placemat RACMs

POL / Business

Impact / Likelihood

Top 5 Risks (by Residual Risk Score)

Risk	Score
HMRC– not collecting evidence; changes not delivered on time (FS&T Risk and Regulation)	16
HMRC audit – not collecting evidence; changes not delivered on time (PO Money)	16
Unable to confirm all branch staff have taken compliance tests (Branch Standards)	12
Failure to effectively monitor causing non conformance and MLR breach (Financial Crime)	12

Retail

Risk	Score
Non compliance with SYSC8 as limitations to demonstrate HR vetting of counter staff (Banking Framework)	9

Identified as Top Risk

LRG

Risk	Score
Failure to effectively monitor causing non conformance and MLR breach (Financial Crime)	12
No reporting of gifts and hospitality (Financial Crime)	10

FS&T

Risk	Score
HMRC audit – not collecting evidence changes not delivered within deadline (FS&T Risk and Regulation)	16
HMRC audit – not collecting evidence changes not delivered within deadline (PO Money)	16

Identified as Top Risk

POMS

Risk	Score
POL unable to provide effective financial crime and MLRO resources	9

F&O

Risk	Score
Unable to confirm all branches have taken compliance tests (Branch Standards)	12
Bureau de Change non-conformance (FSC)	12

IT

Placemat not rolled-out

HR

Placemat not rolled-out

Strategy and CB&CA

Placemat not rolled-out

RISK APPETITE = AVERSE

POL / Measures and Indicators



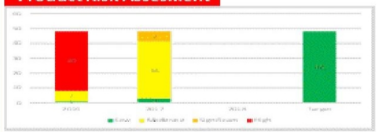
Exceptions

1	Deferred checking *(being drafted)*
2	Xxx
3	Xxx

We are still outside of our averse risk appetite for financial crime due to the following factors:

- 15% of our risks are RED and 54% AMBER
- 87% of our controls are not fully effective
- Functional assurance (partially completed) indicates 45% of policy mandated controls are not effective
- We don't haven't an agreed position with HMRC on evidence retention
- We have experienced increase in SARs and investigations
- Several of our products still need to further lower their risk score

Product Risk Assesment



- 48 products risk assessed with improvement from 2016 to 2017
- 2018 reviews to commence; 31 PIPs received
- Target is to get risk assessments to green

SARs – P10



SAR report highlights an increase in MoneyGram's scams going to Laos and Vietnam. Vulnerable and elderly customers are being targeted by fraudsters posing as TalkTalk. FCT are preparing comms to alert the network.

Whistleblowing - YTD



- Majority Fraud reports in relation to theft – by a Postmaster, Agent Assistant or an employee.
- Theft from vulnerable customers (2 in Jan and Feb)
- 11 of 13 reports (Jan and Feb) named a PO branch.

Gifts and Hospitality – P10

		Volume	Value
Received	Gifts	7	£245.00
	Hospitality	11	£3,930.00
	Breaches	0	
Offered	Gifts	0	-
	Hospitality	9	£750.00
	Breaches	0	-

From March 2018, a new report from the expenses system will be reviewed each quarter to monitor that all external entertainment has been reported accurately via the G&H tool.

***Caveat**: The Dashboard is based on currently reported data. Other actions are being planned to mature the quality, completeness and integrity of data*

Post Office Limited Risk and Compliance Committee-13/03/18

POL00401626

POST OFFICE

Financial Crime Compliance Dashboard

Appendix 2

FINANCIAL CRIME – COMPLIANCE REPORT [March 2018 (Q4)] | **Financial Crime Committee**

- c13% (8 out of 62) controls have been self assessed as fully effective (per Placemat). However remediation actions have not been identified for all risks assessed as partially effective or ineffective. These actions are currently not being formally tracked and/or reported.
- Ineffective controls are in known areas of Bureau, PEPs and Sanctions, and Fit and Proper. Remediation actions are being implemented
- Functional assurance has commenced on effective implementation and operation of minimum controls in relevant policies. Based on partial completion, c55% of controls assured are effective.
- 6 significant incidents reported in the current year, across Retail and LRG. Need to continue to strengthen and monitor vetting process

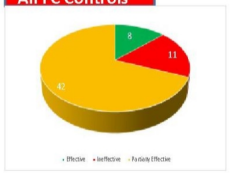
CONTROLS AND POLICY COMPLIANCE

POL

POLICY

Self Assessment *(from Placemat RACMs)*

All FC Controls



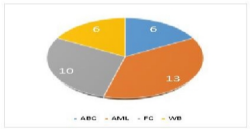
Ineffective Controls



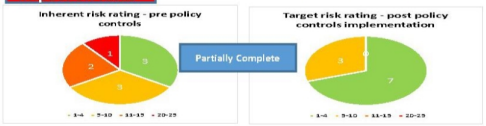
Functional Assurance*

Minimum Controls

AML and CTF	6
ABC	13
Financial Crime	10
Whistleblowing	6



Impact on Risks



Current Status

- For the controls assured to date, c55% are effective
- The ineffective control is around sanctions screening, where IT solution is planned for implementation

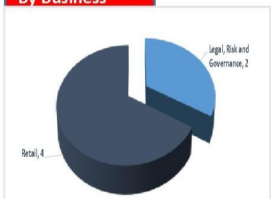
Partially Complete



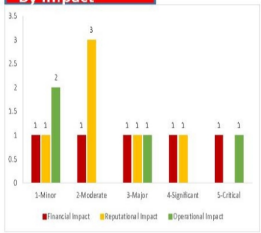
*In subsequent periods we expect to report functional assurance results by Policy and Business Area

SIGNIFICANT INCIDENTS - YTD

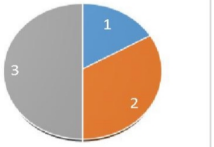
By Business



By Impact



By Root Cause



By Theme

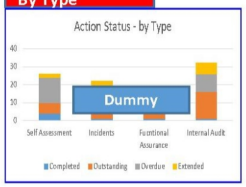


Top Incidents *(and financial impact)*

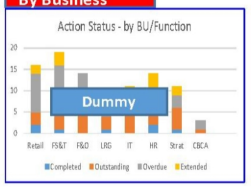
1. Potential Terrorist Financing - Crwys Road Post Office *(Significant)*
2. Potential Money Laundering – Woodland Parade *(Major)*
3. Suspicious SSK Activity - Prepay Tech Ltd *(Moderate)*
4. One4All - Gift Card Top Ups *(Minor)*
5. HMRC Branch Premises Registration - Bureau de Change *(Critical)*
6. HMRC – High value Santander Cash Deposits (£6m in six months)

ACTION STATUS

By Type



By Business



- Xxx
- Xxx
- Xxx
- Xxx
- xxx

(Comments)

OTHER CONSIDERATIONS AND MATTERS

Investigations – P10

Due to the branch contact embargo implemented throughout December, FCT were unable to conduct any Bureau investigations until January, hence the high volume in P10.



NCA Disclosures – P10

Suspicious personal financial activity relating to a Post Master. Post Office unable to comment on personal financial activity, however, the Postmaster submitted their resignation in September and is currently serving their 6 month notice period. No concerns with individual or Post Office branch.

JMLIT s7 requests – P10

- 8 s.7 requests received in P10 listing 62 subjects for screening
- In P10, 3 subject matches were identified and data provided to the NCA
- We have completed searches on 216 known terrorists as per P9, and data on 27 matched subjects has been shared with the NCA

***Caveat**: The Dashboard is based on currently reported data. Other actions are being planned to mature the quality, completeness and integrity of data*

POL00401626

Internal Audit Report

Author: Johann Appel Sponsor: Jane MacLeod Meeting date: 13 March 2018

Executive Summary

Context

The purpose of this paper is to update the Committee on the PO Internal Audit activity and key outcomes. This includes details of the work completed since the last Risk and Compliance Committee (RCC) and Audit, Risk and Compliance Committee (ARC) meetings in January and progress on the 2017-18 Internal Audit Plan.

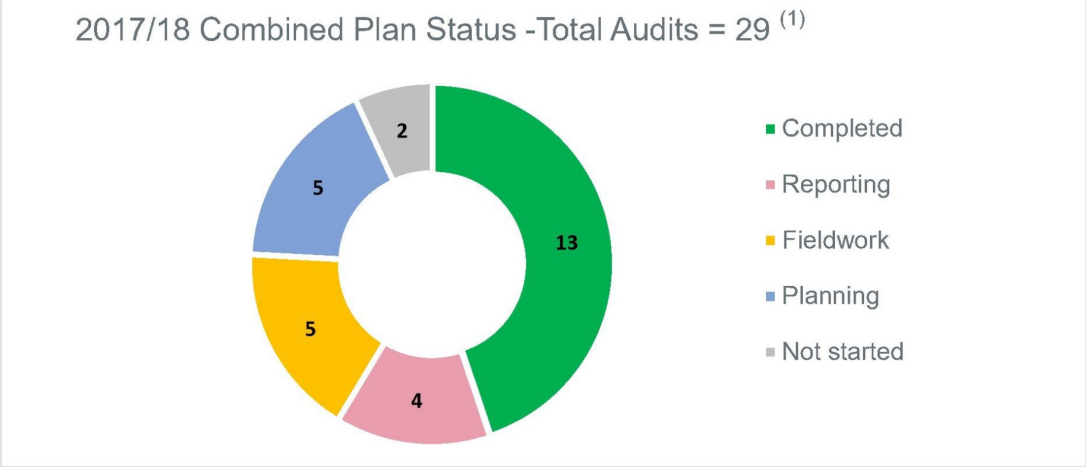
Questions this paper addresses

- Is the Internal Audit Plan on track? What progress has been made since the November RCC meeting?
- What progress is being made with completion of audit actions?
- Have any significant issues arisen that the committee should be aware of?

Conclusion

1. Progress against plan:

Delivery of the 2017-18 audit plan is making good progress and year to date we have now finalised 13 reviews, with a further four reviews currently in reporting. At the time of writing this report five audits were in fieldwork and a further five were being scoped for delivery between March and May. Current progress against plan is as follows:



(1)ARC approved baseline plan for 2017/18 (16 internal control reviews & 13 change assurance reviews)

A full summary of the 2017/18 audit plan status is included in **Appendix 1**.

POL00401626

2. Open and Overdue Audit Actions (as at 28 February 2017):

Audit Action Status:	
Open (not yet due)	38
Overdue (<60 days)	3
Overdue (>60 days)	0
Total	41

More detailed information is provided in paragraphs 10 – 11 of the report.

3. Significant Issues:

There are no significant issues we believe the committee should be made aware of.

Input Sought

The Committee is asked to note and provide comment as necessary.

POL00401626

The Report

Changes to plan since January RCC and ARC meetings

4. No changes to the plan were made during this reporting period.

Internal audit reviews completed

5. Since the January ARC meeting we have finalised the following review:
   - Compliance with Banking Services Framework agreement

   Our findings and observations are summarised below:

Audit	Key Messages
Banking Services Framework (Ref. 2017/18-20) Appendix 2a Needs Significant Improvement ***Sponsor:*** *Debbie Smith* Audit actions: P1: 2 P2: 11 P3: 16 Advisory: 5 Total: **35**	The objective of this audit was to assess adherence to the Framework Agreement by Post Office and its Agencies. With regards to the controls which are specific to the Framework, we observed that Management have implemented effective oversight in relation to the continuing operations of the key Framework processes. However, accountabilities for some services contained in the Framework Agreement have not been clearly assigned to different areas of the business. This contributed to the fact that some of the documentation (i.e. a fraud prevention policy and the Link Information Security Standard) have yet to be developed. With regards to controls which have wider business impact and are critical in supporting the Framework, it was noted that processes need to be strengthened in order to: (i) effectively monitor compliance with the financial crime policy; (ii) implement an effective governance (including planning and testing) of business continuity management (BCM); (iii) improve the IT Disaster Recovery (ITDR) governance arrangements and the oversight of the testing programme; (iv) update information security policies and procedures. Also, for Payment Card Industry Data Security Standards (PCI DSS), back office processes are not included in the PCI scope and neither are users with access to Primary Account Numbers (PAN). There is no ongoing monitoring outside of the annual (external) audit. This report has been rated 'Needs significant improvement' as it highlights weaknesses in internal controls, in particular within the supporting activities across Post Office, which may result in non-compliance with the Framework.

POL00401626

Reviews in Reporting

7. Reports for the following reviews are currently being drafted or cleared through management and is expected to be finalised in time for the March ARC meeting:

	Review	Status / Remarks
1	Customer Complaints	Final draft with exec sponsor for comment
2	Project Solar - HNGT Lite	Draft report being reviewed by project team
3	Back Office Transition	Draft report being reviewed by project team
4	SAP SuccessFactors Payroll - Lessons Learned	Report being drafted

Reviews in Progress

8. The following reviews were in fieldwork at the time of writing this report:

	Review	Status / Remarks
1	Branch Technology - EUC Transition	Fieldwork 5-16 March
2	Network Transformation	Fieldwork 5-16 March
3	Financial Reporting Controls	Nearing completion
4	Pension Schemes	Fieldwork 5-20 March
5	Data Protection (GDPR)	Nearing completion

Reviews in Planning

9. We are currently scoping the following reviews scheduled for delivery in Q4:

	Review	BAU / Change	Timing
1	Telecoms Control Framework	BAU	12-30 March
2	Business Continuity	BAU	12-30 March
3	IT Governance and IT Risk management (Operations)	BAU	March
4	Back Office Transformation - Cash Processing	Change	April
5	Back Office Transformation - POLSAP to CFS	Change	March
6	EUM	Change	April

Updates on Internal Audit Open and Overdue Actions

10. Audit actions are generally being completed on time and year to date 119 audit actions have been completed (103 BAU and 16 Change Assurance actions). At 28 February 41 actions remained open, three of which were overdue.

Audit Action Status:	BAU	Change	Total
Open (not yet due)	36	2	**38**
Overdue (<60 days)	3	0	**3**
Overdue (>60 days)	0	0	**0**
Total	39	2	**41**

POL00401626

11. Following is a summary of the overdue actions, reasons for delay and latest status update:

Description of action and Priority rating	Due date & GE Sponsor	Reason for delay and status update
Data Protection (2016-17)		
Create a Document Retention and Disposal policy.	28/02/18 Jane MacLeod	The new Data Retention and Disposal policy is being created and will be submitted for approval to RCC in March.
NBSC - Handling of Branch Queries and Complaints		
Project to improve the Dynamic System, including system integration, re-design of the knowledge base/ call guides, improved data capture and reporting, and system configurability.	28/02/18 Al Cameron	Project delayed due to technical issues identified during testing which has had a major impact on go live dates. Completion date is now 28/2/18. Project further delayed due to technical issues with drop 1 - dates further extended until end April 2018.
Banking Services Framework		
The Banking Framework services manager will document and submit their product information pack. This will then be used to inform an assessment of the inherent risks, control strengths and residual risks by the Financial Crime Team.	28/02/18 Debbie Smith	Product Information Pack is partially complete and expected to be completed in full by 23 March.

END OF REPORT

POL00401626

Appendix 1

2017/18 Internal Audit Plan - Status as at 5 March 2018					
No.	**Title/Subject**	**Sponsor**	**Original / Addition**	**Timing**	**Status / Rating**
Internal Control Reviews					
1	VAT Process	A. Cameron	**Addition**	May	**Needs Improvement**
2	Lottery Prize Pay-out (Design effectiveness)	K. Gilliland	**Addition**	August	**Satisfactory**
3	Financial Spreadsheet Controls	A. Cameron	**Addition**	August	**Needs Improvement**
4	IT Control Framework (Advisory)	R. Hougton	Original	March - Aug	**Advisory Report**
5	Mails Process	K. Gilliland	Original	July	**Satisfactory**
6	Information Security (2016) Follow-up review	R. Hougton	Original	September	**Needs Significant Improvement**
7	IT Security Transformation (Advisory)	R. Hougton	Original	March - Dec	**Advisory Report**
8	Compliance with Banking Framework	N. Kennett	Original	August	**Needs Significant Improvement**
9	Customer Complaints	A. Cameron	Original	November	**Reporting**
10	MoneyGram: AML Compliance	J. MacLeod	Original	September	**Satisfactory**
11	Telecoms Control Framework	N. Kennett	Original	March	Being Scoped
12	Business Continuity	J. MacLeod	Original	March	Being Scoped
13	Data Protection (follow up) (GDPR)	J. MacLeod	Original	January	**Fieldwork**
14	Pension Scheme(s)	A. Cameron	Original	March	**Fieldwork**
15	Financial Control Framework	A. Cameron	Original	February	**Fieldwork**
16	IT Governance and IT Risk management	R. Hougton	Original	March	Being Scoped
	FRES	N. Kennett	**Postponed**	2018/19	
	Client Settlements Process	A. Cameron	**Postponed**	2018/19	
	Cyber Security (Ph 2)	R. Hougton	**Postponed**	2018/19	
	Branch Cash Forecasting & Management	A. Cameron	**Postponed**	2018/19	
Change Assurance					
1	SAP SuccessFactors - Payroll	M. Kirke	Original	June	**Needs Improvement**
2	Integrated Change Plan (Advisory)	A. vd Bogerd	Original	July	**Advisory Report**
3	IT Networks	R. Houghton	Original	October	**Needs Improvement**
4	SAP SF Payroll Go-Live Readiness Review	M. Kirke	**Addition**	December	**Acceptable (PwC)**
5	SAP SF Payroll Lessons Learned	M. Kirke	**Addition**	January	**Reporting**
6	Back Office Transformation - POLSAP to CFS	A. Cameron	Original	March	Being Scoped
7	Back Office Transformation - Cash Processing	A. Cameron	**Addition**	March	Not started
8	Back Office Transition	A. Cameron	**Addition**	January	**Reporting**
9	Project Solar - HNGT Lite (Prev. Chameleon)	K. Gilliland	Original	January	**Reporting**
10	Network Transformation	K. Gilliland	Original	February	**Fieldwork**
11	Branch Technology - EUC Transition	K. Gilliland	Original	January	**Fieldwork**
12	EUM	K. Gilliland	Original	March	Being Scoped
13	Peer to Peer Encryption Implementation	J. MacLeod	**Cancelled**		Cancelled
	Placeholder (FS Customer Hub?)	N. Kennett	Original	tbc	Not started
	Placeholder (Project Panther?)	K. Gilliland	Original	tbc	Not started
	Agile Methodology and Governance	J. MacLeod	Original	tbc	Not started
	Gating Process - Effectiveness	A. vd Bogerd	**Postponed**	2018/19	Not started
Note: Target audit delivery per original approved plan is for 29 audits (16 internal control reviews and 13 change assurance reviews).					

POL00401626

Appendix 2a

POST OFFICE LIMITED – Internal Audit REPORT
AUDIT TITLE: Banking Counter Services Framework Review
REFERENCE: 2017/18-20 DATE ISSUED: 17 January 2018

Executive Summary

Background

A number of banking institutions (hereafter referred to as "Institutions") appointed Post Office Limited (POL) as their agent to perform services on their behalf at POL outlets as set out in the "Terms and Conditions to Members of Post Office Banking Counter Services Framework version 1.2 January 2017" ("the Framework Agreement"). The services performed by POL include automated services (e.g. cash withdrawal, etc…) and manual services (e.g. cash deposit via magnetic swipe banking card/barcoded deposit slip or pre-encoded personalised deposit slip; cheque deposits, etc...).

Scope & Approach

The objective of this audit was to assess adherence to the Framework Agreement by POL, including its Agencies. This review was not designed to be a deep dive into each area but rather to provide a high level view of the current Framework control environment.

Conclusion

The Framework Agreement includes specific requirements for the processes which directly enable the delivery and monitoring of the service (such as financial processes, management information, counter transaction processes and Link information security processes). For supporting processes (such as Financial Crime, Business Continuity, IT Security and Disaster Recovery processes), the Framework refers to the set of policies and procedures which are expected to be in place for the wider business activities.

With regards to the controls which are specific to the Framework, we observed that Management have implemented effective oversight in relation to the continuing operations of the key Framework processes. However, accountabilities for some services contained in the Framework Agreement have not been clearly assigned to different areas of the business. This contributed to the fact that some of the required documentations (i.e. a fraud prevention policy and the Link Information Security Standard) have yet to be developed.

With regards to controls which have wider business impact and are critical in supporting the Framework, it was noted that processes need to be strengthened in order to: (i) effectively monitore compliance with the financial crime policy; (ii) implement an effective governance (including planning and testing) of business continuity management (BCM); (iii) improve the IT Disaster Recovery (ITDR) governance arrangements and the oversight of the testing programme; (iv) update Information security policies and procedures. Also, for Payment Card Industry Data Security Standards (PCI DSS), back office processes are not included in the PCI scope and neither are users with access to Primary Account Numbers (PAN). There is no ongoing monitoring outside of the annual (external) audit.

This report has been rated 'Needs significant improvement' as it highlights weaknesses in internal controls, in particular within the supporting activities across Post Office, which may result in non-compliance with the Framework.

Management Comment

"Banking Framework management welcomes the findings in the report. Of particular note are the POL-wide findings revealed (PCI, IT security, BC/DR policies that impact all services) – and their potential impact on Banking Framework compliance. Framework specific issues identified are under active management to address." *Martin Kearsley (Director of Banking Services)*

Report rating:



Needs significant Improvement

Confidential

POL00401626

Internal Audit Report: Banking Counter Services Framework Review

Summary of Findings

The table below provides a summary of the P1 and P2 findings and their ratings. The report also included 16 P3 observations and 5 advisory recommendations which have not been listed below.

Finding		Rating*	Action Owner	Date
Scope Area: Financial reconciliation				
1	No financial reconciliation between invoicing and settlement of transactions values.	P2	Dave Jenkins	31 March 2018
Scope Area: Business process integrity				
2	Inconsistent practices across the branch network for accepting Location Exercise based Santander Business deposits	P2	Martin Kearsley	31 March 2018
Scope Area: Financial Crime				
3	No documented fraud prevention policy / operating level process.	P2	Sally Smith	31 March 2018
4	There is no mechanism within POL to monitor compliance with the financial crime policy.	P2	Sally Smith	30 April 2018
Scope Area: Operational stability and resilience				
5	Governance of the business continuity management programme is ineffective.	P2	Tim Armit	31 March 2018
6	Agreed business impact assessments, business continuity strategies, business continuity plans and associated testing is not in place.	P2	Tim Armit	31 March 2018
7	The ITDR programme governance is not formalised.	P2	Mick Mitchell	31 March 2018
8	Recovery Point Objectives have not been defined.	P2	Mick Mitchell	31 March 2018
9	IT have limited oversight of the current ITDR testing programme.	P2	Mick Mitchell	31 March 2018
Scope Area: IT Security				
10	No evidence of the Link Information Security Standard	P1	Jules Harris	30 April 2018
11	Back office processes are not included in PCI scope.	P1	Jules Harris	30 September 2018
12	No ongoing monitoring of PCI DSS controls outside of the annual audit.	P2	Jules Harris	28 February 2018
13	Users with access to PAN are not included in PCI Scope.	P2	Jules Harris	30 September 2018

* P1 = High Priority, P2 = Medium Priority, P3 = Low Priority

POL00401626

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE

Internal Audit Plan 2018-19

Author: Johann Appel Sponsor: Jane Macleod Meeting date: 13th March 2018

Executive Summary

Context

1. The Post Office annual risk-based audit plan for 2018-19 has been prepared in accordance with the applicable requirements of the revised Internal Audit Charter as approved by the ARC in March 2017, as well as the professional standards of the Institute of Internal Auditors (IIA).

Questions addressed in this report

2. What processes, activities and programmes should be assured by Internal Audit in 2018-19? Does the proposed plan focus on the right priorities to support the Post Office strategic objectives?
3. What are the resource requirements to deliver this audit plan and how much will it cost?

Conclusion

4. An integrated audit plan has been prepared to provide assurance over principle business risks and significant change activities. The proposed plan can be summarised as follows:

Category	Number of audits	Estimated effort (days)		Approximate cost of co-source
		Total	Co-source	
Business Risks	16	585	130	£182k
Change Portfolio	10	270	270	£378k
Total	**26**	**855**	**400**	**£560k** [N1]

[N1] 2017-18 Co-source cost budget was £692k. The cost reduction of £132k is after providing for an increase in co-source day rates, but will be partially off-set by hiring a new in-house IT auditor. Overall comparative cost will remain broadly unchanged or marginally favourable compared to the prior year.

Input Sought

5. The Committee is asked to:
   a. Consider the proposed Internal Audit Plan for 2018-19 and confirm that individually and collectively these reviews represent an appropriate programme to support senior management in their activities and to provide assurance to the Audit, Risk & Compliance Committee (ARC) over key risks to the Post Office.
   b. Recommend the proposed Internal Audit Plan to the ARC for approval.

POL00401626

Detail

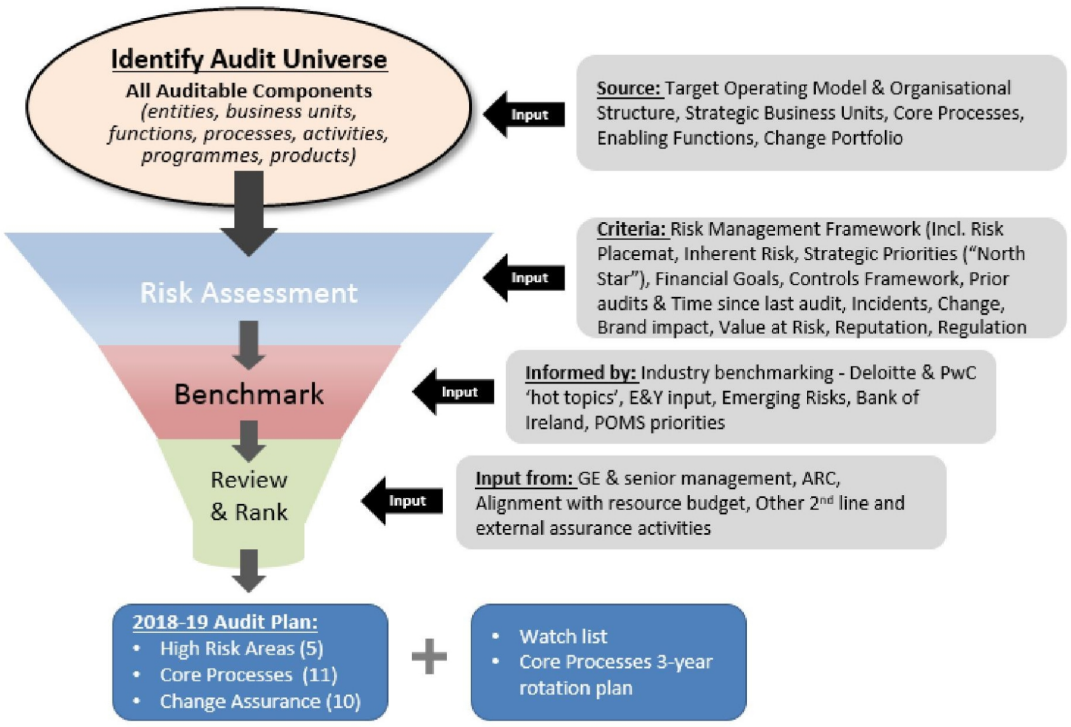
The Planning Context

6. Post Office risk profile is impacted by continued and significant internal change, increased regulatory scrutiny and market pressures. The 2018-19 Internal Audit plan is designed to provide assurance over the organisation's principle risks, core processes and material change activities.

7. As from 2017-18 we have introduced a three year rotation plan for core processes. Core processes are usually mature and generally assumed to be well controlled, but warrant cyclical validation due to their pervasive nature and criticality to the business. The 2018-19 plan includes the second tranche of core processes to be reviewed over a three period.

The Planning Process

8. The following diagram depicts the process we followed to identify, assess and prioritise the processes and activities to be assured in 2018-19:



The Planning Results

9. The proposed list of audits was discussed with GE members and senior management.

10. The tables below outline the proposed audits to take place in 2018-19. However, internal and external events may cause priorities and risk profiles to change, and management may have additional requests during the year for advisory support

POL00401626

or audit assistance. In consequence, we may consider amending the plan as the year progresses. We will seek ARC approval for all material changes to the plan.

11. **Table 1** represents the baseline plan for internal control reviews, of which the target delivery is 80% or 16 reviews.

1. Internal Control Reviews – Target = 16 reviews			
Rank	**Proposed Review**	**Sponsor(s)**	**Timing**
1	Payroll	Al Cameron & Martin Kirke	Q2
2	Accounts Payable	Al Cameron	Q1
3	Branch Cash Forecasting & Management	Al Cameron	Q1
4	Cyber Security	Rob Houghton	Q2
5	Supply Chain	Al Cameron	Flex
6	Contract Management	Al Cameron	Q3
7	IT Control Framework	Rob Houghton	Q2
8	Employee Expenses	Al Cameron & Martin Kirke	Flex
9	Client Settlements Process	Al Cameron	Q3
10	Digital Strategy & Capability	Owen Woodley & Rob Houghton	Flex
11	Whistle-blower Process	Jane MacLeod	Q4
12	Accounts Receivable	Al Cameron	Flex
13	Agents Remuneration	Debbie Smith & Al Cameron	Q3
14	Financial Control Framework	Al Cameron	Q4
15	FS Training & Competence	Owen Woodley & Martin Kirke	Flex
16	Online Sales (Product / Channel to be determined)	Owen Woodley	Flex
17	FRES Governance	Owen Woodley	Flex
18	Procurement (Pre-award)	Al Cameron	Flex
19	Marketing Process / Activities	Owen Woodley	Flex
20	Data Privacy	Jane MacLeod	Q4

12. **Table 2** represents planned reviews of significant change activities. The baseline plan is for 10 Change Assurance reviews. This is an indicative list based on the current change portfolio and will be reviewed and updated continuously as the portfolio of change programmes develops and the risk profile changes. The plan includes at least one thematic review focusing on programme governance (e.g. gating effectiveness, investment committee, agile methodology). In addition we will provide assurance over 9 change programmes – this could be assurance at a point in time or ongoing / real time assurance depending on the project.

POL00401626

2. Change Portfolio / Programme Assurance – Target = 10 reviews			
Rank	**Proposed Review**	**Main Sponsor**	**Timing**
1	Change Programme Governance	Rob Houghton	Q3
2	Panther (Business Integration)	Debbie Smith	Q2/3
3	DMB Strategy	Debbie Smith	tbd
4	Customer Hub – Horizontal & Travel	Owen Woodley	tbd
5	Postmasters Portal	Debbie Smith	tbd
6	Identity Services	Martin Edwards	tbd
7	Tracked Online / Disintermediation Risk	Debbie Smith	tbd
8	Customer Hub (Additional Verticals)	Owen Woodley	tbd
9	Banking Framework – Cash Management	Debbie Smith	tbd
10	Project Everest	Rob Houghton	tbd

13. **Table 3** is our 'watch list' of additional areas for consideration during the year, should either the assurance needs for the priority areas decrease or risk levels for items on our watch list increase. The watch list will also inform the 2019-20 audit plan.

	Topic / Area
1	Payment Services / Bill Payments
2	FS - Branch Sales: New distribution model (Customer Relationship Managers)
3	Asset management - Software licensing management
4	Equal Pay
5	Diversity & Inclusion
6	Sales – Post Office Money Mortgages
7	IR35 Adherence
8	DMB Stationery (WHSmith consignment stock)
9	Money Laundering Directive
10	Revenue Contracts (e.g. POCA)
11	New Agents Process (New Agent On-boarding)

POL00401626

Three Year Rotation Plan

14. In 2017-18 we introduced a rotational audit plan to assess core business processes over a three year cycle. This will provide regular assurance on the effective operation of controls over critical business processes. The rotational plan in the table below has been based on the last review of these processes, known issues and ongoing remedial programmes.

Core Processes – 3 Year Rotation Plan		
Year 1: 2017-18	**Year 2: 2018-19 (in plan)**	**Year 3: 2019-20**
Financial Reporting Controls	Financial Reporting Controls	Financial Reporting Controls
Branch Cash Forecasting & Management (1)	Bill to Cash (Accounts Receivable)	Record to Report (Financial Close)
Sales (Mails Process)	Sales (Rotate Sales Channels)	Sales (Rotate Sales Channels)
Business Continuity	Payroll	Treasury Operations
IT Operations (IT Governance and IT Risk management)	Procure to Pay	Regulatory Compliance
Client Settlements Process (1)	Supply Chain Management	FS Conduct Management Framework
	Contract Management	Fixed Assets
	Agents Remuneration	
	Employee Expenses	

(1) Postponed to 2018-19

Resource Requirements

15. The approved headcount for the internal audit team is 5 FTEs. We are currently recruiting for two vacancies. The co-source requirement to support delivery of the 2018-19 plan was estimated at approximately 400 days with a total cost of £560k. The cost is indicative only and likely to change once the new co-source provider has been selected.
16. The current co-source agreements with PwC and Deloitte runs until September 2018. It is our intention to replace the current arrangements with a single provider by August 2018 and we are in the process of inviting professional firms to tender for provision of these services.

END OF REPORT

POL00401626

GDPR Programme Update

Author: Clare D'Netto Sponsor: Jane MacLeod Meeting date: 13 March 2018

Executive Summary

Context

The General Data Protection Regulations ('GDPR') come into effect in May 2018. Post Office has a project underway to implement the necessary changes to achieve compliance with the GDPR requirements. As a key stakeholder, the Risk and Compliance Committee of Post Office Limited has requested updates on the progress of implementing the necessary changes as they impact Post Office. This update is following the paper submitted to RCC on the 18th January and the training session provided to the ARC on 23rd January.

Questions this paper addresses

1. Where are we relative to where we said we would be?
2. Where are we behind where we said we would be and do we have a path to green?
3. What are the key delivery risks to May?
4. What are the material risks to compliance?

Conclusion

1. Where there has been considerable progress since the programme last presented to the RCC on 18th January, this paper outlines where the certainty of delivery by May has decreased, and the mitigations in place for the following 'at risk' areas:
   (i) 100% of data breaches follow the updated procedures
   (ii) 100% processes updated for new employees, agents and job applicants
   (iii) 100% Privacy Notices and Privacy wording updated to existing employees and agents
   (iv) All contracts will be updated to reflect the GDPR, using a risk-based approach by May 2018.
2. This paper also identifies key material risks to compliance which the RCC is requested to note.

Input Sought

The RCC is requested to:

- note the material risks to effective compliance identified within this paper which will be formally addressd at the programme steering committee.

POL00401626

The Report

1. Where are we relative to where we said we would be?

1. The paper presented to RCC on 18th January described the components of 'effective compliance' that we aim to have in place by May 2018 and described our then level of certainty, in meeting that timeline in light of operational and technical capacity and other key dependencies. It also identified those activities which would therefore extend beyond that date.
2. Annex 1 summarises our current level of certainty in comparison to the position we stated in January, in relation to all new activities which were intended to be compliant with the GDPR by May 2018.
3. Progress has been made in many areas and our overall level of certainty has increased, including privacy notices and marketing permissions for new customers. This is based on our continued work with the business and partners to agree wording and commit to timescales. In addition, we have raised change requests for the POL technical changes. However, delivery of changes for marketing permission for Financial Services (BOI) products is currently at risk as this was dependent on a commercial agreement (see 18 (i)) on whether or not BOI can market to POL customers and then an agreed wording as a result.
4. The Education and Awareness activity in the run up to May is in train, with targeted face-to-face training for priority audiences and themed weekly comms going out to the business.
5. Annex 2 summarises our current level of certainty for all existing activities that will be remediated by May 2018 within the PO's risk appetite.
6. The key area of progress is that the Programme has completed an assessment of the potential impact of GDPR on the number of permissions in the back book to which we can continue to market, using Legitimate Interests.
7. As a result of this analysis, we have a med-high confidence that we can use Legitimate Interests to continue to market to leads who were active within the last 3 years where there is evidence of a relationship based on click through and web browsing. This equates to 4.7m permissions overall and 2m of email permissions, which is a minimal impact to the current situation, whereby the business only actively markets to a proportion of the overall leads in Brands, predominantly those permissions which are less than 3 years old. In Phase 2 of the Marketing sub-project we are investigating the outliers at a more granular level to understand if legitimate interests can be applied.

2. Where are we behind where we said we would be and do we have a path to green?

8. Delays to getting planned resources for key roles, including workstream leads for Governance & Framework, HR and Agents and Contracts, as well additional DP and HR PM resources have impacted on the following deliverables:

   (i) 100% of data breaches follow the updated procedures

POL00401626

(ii) 100% processes updated for new employees, agents and job applicants

(iii) 100% Privacy Notices and Privacy wording updated to existing employees and agents

(iv) All contracts will be updated to reflect the GDPR, using a risk-based approach by May 2018. This includes material (c 80) and non-material contracts (c.400) and SPM contracts.

9. We are working with the HR Business Partner to progress these roles through a mix of interim and consultancy/legal resources and have re-allocated critical tasks within the existing team. In addition, we have recruited a Programme Director to free up additional Programme Management capacity to focus on high-risk areas, including Contract remediation.

10. The remediation of existing contracts has been delayed as a result of a review of the POL DP clauses against the CCS PPN announced in December 2017. This has now been completed and has resulted in changes to the remediation packs. On the advice of Legal, we have also added an additional step to review the liability and insurance risk in existing contracts.

11. Both these factors have has delayed mobilisation of the business for contract remediation, therefore the Programme Team has looked at ways to streamline the process for remediation for non material and low risk contracts in order to minimise the impact. We are also progressing a streamlined process to assess liability and insurance risk in house and using WBD by exception.

3. What are the key delivery risks to May?

12. Delays to planned resources will continue to have an impact on these workstreams.

(i) 100% of data breaches follow the updated procedures

(ii) 100% processes updated for new employees, agents and job applicants

(iii) 100% Privacy Notices and Privacy wording updated to existing employees and agents

(iv) All contracts will be updated to reflect the GDPR, using a risk-based approach by May 2018. This includes material (c 80) and non-material contracts (c.400) and SPM contracts.

13. Quick resolution of resources for (i), (ii) and (iii) will enable us to get back on track for delivery May and this is an urgent focus for the Programme.

14. However, Contract remediation will continue to be at risk due to the delayed mobilisation and the timescales to complete the end-to-end remediation process, particularly high and medium risk contracts. We are prioritising POMS contracts and Tower IT contracts to mobilise first, however there is a dependency on agreement as to the personal data that Tower Vendors process on behalf of the Post Office.

15. A potential blocker for contract remediation will be the capacity of Contract Owners, which particulary applies to high and medium risk contracts, where they will be required to be more involved in the remediation process.

POL00401626

16. We will need confirmed Contract Owners for all contracts, including non-material contracts otherwise we will be unable to remediate. The Programme will be sending out a communication to GE to get confirmation of Contract Owners and to identify any contracts that are not currently on Bravo, and therefore we are not aware of, so we can progress these.

17. Although we have increased confidence regarding delivery of customer-facing changes for new privacy notices and marketing permissions, the timescales for operational and technical changes remain tight. The key risk areas are changes to in branch materials and technical changes on the *partner's* side. The Project Manager is continuing to work with the business and partners to track delivery risk and identify remediations.

4. What are the material risks to compliance?

18. The following material risks have been identified i.e. where there is a risk that the agreed remediation may be considered to not be compliant with the GDPR. The programme is documenting these risks for decision / acceptance by the business via the Programme Governance. All risk-based decisions, including rationale, will be held on OneTrust.

(i) **IRRELEVANT**

(ii) Telecoms currently retain telecoms data at 7 years, which is non-compliant, however they are working towards implementing a 24 month retention period. This will take 12 months to implement, which we consider to be a defensible position.

In the meantime, not being able to delete data that is more than 7 years old before May, could result in fines and compensation if there is a customer complaint.

(iii) Where ever we rely on legitimate interests, including Marketing to the back book and Telecoms, for credit referencing/debt management, there is risk. However we are documenting our rationale for using Legitimate Interests via positioning papers for decision through Programme Governance.

(iv) Due to gaps in Product Manager knowledge and documentation, there is a risk that we have not captured all data types and data flows as part of the information audit and this impacts on the information we provide in the privacy notices. The information captured by the Programme will be held in One Trust and we will establish processes, including the PIA, to ensure that documentation will be updated and maintained to reflect subsequent changes.

(v) Due to gaps in business knowledge and documentation on the personal data processed by IT vendors, there is a risk that we have not captured

POL00401626

all data types and data flows as part of the information audit. This presents a potential risk to the accuracy of processing schedules and therefore the accountabity of our processors in the case of a data breach. Again, improved processes, including PIAs and Change Requests, need to be in place to ensure documentation is maintained in BAU.

(vi) There is risk that the Programme does not have a complete view of all the personal data held by non-IT vendors and in software licenses, due to limited available information in the business. We may not be able to complete personal data analysis which may cause fines from ICO for failure to maintain an up to date inventory and or / if there is a data breach for an unidentified vendor. The Programme is currently working with IT and Procurement on this, however there will be a requirement for tighter controls for new IT vendors and software.

POL00401626

Annex 1 - All <u>new</u> activities are compliant with the GDPR in the following areas by May 2018

Deliverables	Certainty (Jan 18)	Certainty (Mar 18)	Commentary
Privacy Management Governance framework will be implemented to demonstrate Accountability	Medium	Medium	• **No change**: We are engaging specialist resource to lead the Governance & Framework Workstream and increasing the capacity in the DP team, however this activity has a lead time. • However, the team is building the structure for the One Trust Tool which will be the key repository and tool to demonstrate accountability via holding PIAs, LIAs, records of processing activity.
100% privacy notices and privacy wording updated – all channels	Medium	Medium-High	• **Increased**: Considerable progress has been made in drafting of the Privacy Notices, including the overall Privacy wording for Post Office. We are advanced in our discussions with BOI and FRES. The POCA privacy notice has been approved and Telecoms and POMS Travel Insurance are complete. CRs have been raised for POMs TI and POL Digital and Horizon Changes for a go live by end of April. • There are delays at specific partner / product level e.g. Tif/RLG aren't ready with their privacy notices and other journey changes, however we are working with them.
100% Marketing Permissions updated – all channels / partners	Low/ Medium	Medium	• **Increased certainty**: Considerable progress as stated above, including the approval and dissemination of the new Marketing Permissions. Plans are advanced with POL, POMS and partners and CRs has been raised for POL technical changes. • There are Product/Partner-specific dependencies, including the commercial decision for BOI which has impacted on the

POL00401626

Deliverables	Certainty (Jan 18)	Certainty (Mar 18)	Commentary
			time taken to agree the wording for the marketing permissions. Telecoms has flagged capacity constraints to implement across all channels, including product packs. • Timescales to implement operational and technical changes are tight, specifically for technical changes on the partner side and for updating materials in branch.
100% processes updated for new employees, agents and job applicants	Medium	Low/ Medium	• **Decreased certainty:** There is limited time to complete changes by May 2018, however activities are being prioritised using a risk based approach so some activities will continue after May 2018. • The onboarding of a Workstream lead and additional HR PM resource is critical to progress this workstream.
100% of requests follow new and updated procedures for rights	Medium	Medium	• **No change:** Subject to engagement of the Governance & Framework Workstream Lead. Resources identified to update the procedures for individual rights however are potential DP constraints • The known – unknown is the capability of providers to delete data which is already a requirement of current contracts. This is being validated via the Systems Workstream.
100% of data breaches follow the updated procedures	Medium – High	Medium	• **Decreased certainty:** We are engaging specialist resource to lead the Governance & Framework Workstream and increasing the capacity in the DP team, however this activity has a lead time and we planned to complete Testing in March. • Potential issues have been identified with the Atos Incident Management Process which will need to be reviewed as part of this workstream.

POL00401626

Deliverables	Certainty (Jan 18)	Certainty (Mar 18)	Commentary
100% of new contracts contain the new DP clauses and schedules	High	High	• **No change:** P Suite further updated in Feb, to reflect the CCS PPN and security wording.
100% new contracts contain the new security standards	High	High	• **No change:** The existing documentation is being updated to provide a fully updated policy and set of standards for Post Office by June. However we have removed the hard dependency for the Contract Remediation workstream by inserting a short form of words and updating the existing schedule 16 in line with GDPR.
An audit and due diligence process for suppliers will be ready for implementation from May 2018	High	High	• **No change:** Work is currently underway to develop this using the OneTrust tool.
100% of new projects complete a Privacy Impact Assessment (high risk projects)	High	High	• **No change:** However the existing PIA will be launched via OneTrust and there is a requirement to fully embed this process for all products.
100% of relevant employees have received Training and Comms	Medium – High	High	• **Increased certainty**: A new workstream lead is in role, plans are well developed and a training provider has been identified.

POL00401626

Annex 2 - Existing activities that will be remediated by May 2018 within the PO's risk appetite

Deliverables	Certainty (Jan 18)	Certainty (Mar 18)	Commentary
Information audit completed, using a risk-based approach	Medium	Medium	**No change:** • Product Reviews**:** T1 products analysis has been completed but there are some information gaps due to lack of knowledge / documentation in the business. There is a risk that Completion of the remaining T2 & T3 product will continue beyond May. • Systems questionnaire: IT Vendors have provided incomplete information (See systems) • Business Functions: We have agreed an approach using a risk-based approach.
100% Privacy Notices and Privacy wording updated to existing customers	Medium	Medium	**No change:** • Activities agreed with e.g. POMS via renewals and Telecoms. This is included in planning discussions with partners where relevant and is subject to the same dependencies as for privacy notices for new customers.
Continuation of marketing to the back book using legitimate interests	Medium	High	**Increased certainty**: • Positioning Paper agreed at the last Programme Steering Group to support Marketing to the Back Book.
100% Privacy Notices and Privacy wording updated to existing employees and agents	Medium	Low-Medium	**Decreased certainty:** Risk to timescales to implement all changes by May 2018 due to resource constraints.
All contracts will be updated to reflect the GDPR, using a risk-	Medium	Low-Medium	**Decreased certainty:** Delayed mobilisation as we needed to review and update the DP clauses against the CCS PPN

POL00401626

Deliverables	Certainty (Jan 18)	Certainty (Mar 18)	Commentary
based approach by May 2018. This includes material (c 80) and non-material contracts (c.400) and SPM contracts			clauses. The inclusion of the risk assessment for liabilities and insurance had increased end to end timescales. The Programme is planning to on-board a specialist resource to lead this workstream as there will be strong business engagement with Contract Owners. Potential blocker: Contract Owners are still not confirmed and they are critical to this workstream. Constraints: Contract Owners time constraints to engage with this activity.

POL00401626

PCI-DSS Compliance Status Report

Authors: Jules Harris/Nicholas Spicer Sponsor: Jane Macleod/Debbie Smith Meeting date: 13 March 2018

Executive Summary

Context

Post Office (PO) processes c85m transactions worth c£4.5bn of card payments to our card acquirer Global Payments (GP). As part of the payment card industry requirements, and due to our large numbers we are classified as a level 1 merchant, there is a requirement to obtain an external audit verified Report on Compliance (RoC) to the Payment Card Industry – Data Security Standards (PCI-DSS). This is an annual process. The Payment Council regularly update the control requirements, in order to ensure that new threats and vulnerabilities are covered. The standard was substantially updated in 2017, and the new version V3.2 put more control requirements on Post Office compared with the previous version to which we achieved compliance last year.

PO appointed a new external auditor this year, and this new auditor is well known for being very thorough in their approach to completion of the audit testing.

The existing RoC expired on 28th December 2017. We have shared our remediation plans with GP, and to date they are satisfied with our expectation to receive a passing RoC by 31st July 2018. Whilst GP could levy penalties against PO, currently they have not chosen to take this action.

Questions this paper addresses

- What were the issues to getting the RoC in the first place?
- What have we already fixed and what remains?
- GP has given PO dispensation to resolve certain issues over a longer period – what are the implications of this?
- What other actions are PO taking in regard to our PCI-DSS compliance?

Conclusion

1. PO are required to be certified to PCI-DSS standards by a number of contracts, most notably the Banking Framework. It is the opinion of the authors that with the relationship we have with our acquirer we will be able to satisfy the banks that their customer data is not at risk.
2. RCC are asked to note that there is a risk in this regard.

Input Sought

RCC is requested to note this paper.

POL00401626

Report

What were the issues to getting the RoC in the first place?

3. There are extra requirements that have been added to the standard during 2017, which owing to the age of our estate are extremely challenging to implement. Additionally, the new auditor has taken a much more forensic approach than previous auditors, and through this has identified further areas of non-conformity.

4. This is the first year that ComputaCenter (CC) have been included in the scope of our PCI certification. Despite engagement since April 2017, they have not been able to complete their required actions in a reasonable timeframe. This has been escalated to senior CC account management in order to try to resolve the issue.

5. CC have struggled to understand the principles of PCI despite escalation to get a qualified PCI expert on board, they have only done this in the last month.

What have we already fixed and what remains?

6. There were 35 items for Fujitsu (FJ) to fix. Of these 3 have been closed, 25 have been completed, and the remaining 7 are on schedule to be fixed by mid-April.

7. There were 32 items for CC to fix. Of these 5 have been closed, 17 have been completed. A further 6 are due be fixed by mid-April. The remaining 4 items are now being worked on by CC, PO are waiting for a confirmed completion date. Initial feedback is that one will take 3 to 6 months to resolve. PO has fed back that this is unacceptable, and are looking at different ways to achieve the desired outcomes without CC effort. There is a possible option to use Verizon and FJ to achieve a suitable set of controls, so as a precaution Change Requests (CRs) have been submitted and we are awaiting formal proposals.

8. The dates have been booked for the external auditor to visit both CC and FJ to see the evidence that the closed controls are all now in place.

Where have PO been given dispensation by GP to allow us longer to resolve some complex issues?

9. There is a back office system called TESQA which is used by the fraud and operations teams to monitor activity and support fraud and police queries related to banking transactions. This system has to retain the full 16 digit card number in order to be able to function. As this system has very limited access (4 terminals in all) and was not previously within scope GP have issued a dispensation for 2018 to allow the external auditor to exclude it from our RoC. PO are looking at options to bring the system within compliance by as part of a wider payment technology upgrade programme.

What other actions are PO taking in regard to our PCI-DSS compliance?

10. The PCI steering committee "PCI SteerCo" has been stood up to ensure focus on resolution by bringing all relevant parties to the table on a weekly basis. The PCI SteerCo programme team has worked with internal and external stakeholders to

POL00401626

track each remedial activity for each of the Vendors (FJ, CC, Accenture, etc.), and provide a weekly update report to PCI SteerCo members. The most recent report has been included as a supporting document. The Steerco programme team also raised the aforementioned CRs for the outstanding CC remedial items that CC have been commercial disputing as out of scope.

11. The legal team is support the CC vendor manager to resolve the CC claim that their contract did not require them to be PCI compliant. PO have paid CC to perform the remedial actions to stop the delays, this will be reviewed and if found to be in PO favour, the monies will be claimed back.

12. PO has a historic issue with the contract with FJ on the version of PCI they will comply with, so this will also be renegotiated after the RoC has been received.

13. PO will run a discovery exercise later in 2018 to test where else payment card details are stored. This will be commissioned once the RoC has been received.

POL00401626

Project Dashboard – *PCI DSS SteerCo*

Minutes (23/02/18):

- Branch visits (48) now complete. Tamper check procedure note sent to branches
- FJ on track for end of March – although additional risk raised for "unknown unknowns" resulting from Segmentation and penetration testing remediation

- Computacenter QSA assessments are scheduled to start w/c 19/3
- Computacenter POAP provided high level view of remediation actions to descope non-payments infrastructure and address network segmentation. POL requested detailed implementation plan
- Network segmentation at Computacenter is a pre-requisite for segmentation and penetration testing
- Solution options proposal for CRs to be presented on 27/2
- A resource constraint (Security Architect) was identified as a possible risk

- Credence: issues getting access to test env, however now on track for 4/3 delivery
- Analysis and rework to implement APADC scripting required after implementation of the Credence cleanup activity

Actions (23/02/18):

- Angus requested meeting on Monday 26/2

POL00401626

Project Dashboard – *PCI DSS RAG / Summary*

Project Name	*PCI DSS*	**Reporting Date**	*02/03/18*
Project Leads	*PM: Chris Eluwa, BA: Simon Woods, Business Owner in Post Office: Nicholas Spicer,*		
Purpose	IRRELEVANT		

Overall	Delivery	Cost	Benefit	Risk
R →	R →	R ↓	A →	R →

Actions Outstanding	Actions For Review	Actions Resolved
17 ↑	42 ↑	8 →

Arrows indicate movement from previous period (downward worsening, upward improving, horizontal no change)

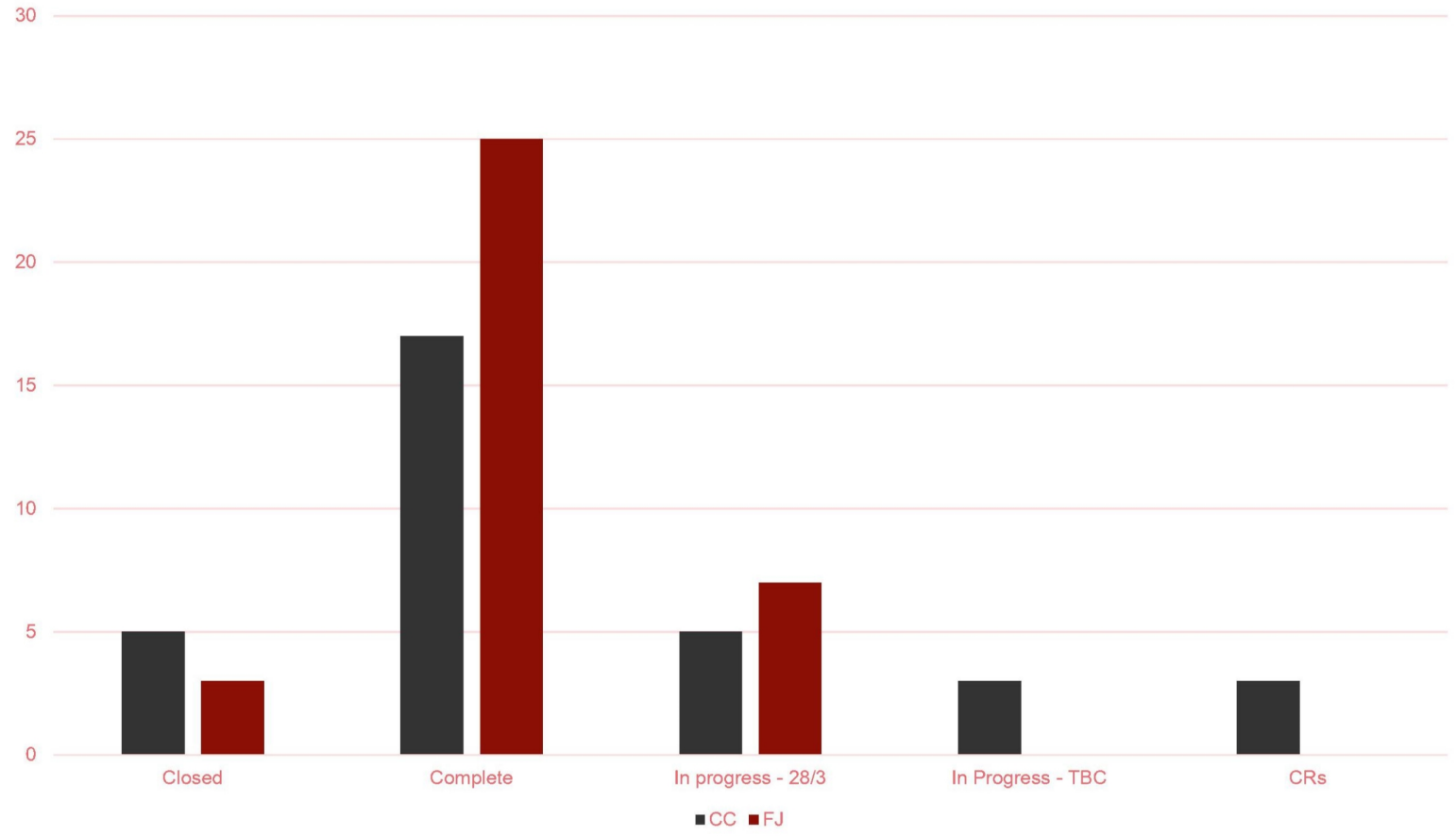
Actions outstanding relate to the remediation plan activities which are grouped by area. Further detail of actions being undertaken is provided on the "Update on suppliers" slide

Executive Summary and Route to Green

IRRELEVANT

POL00401626

Progress Snapshot – *PCI DSS (as at 28/02/18)*



POL00401626

Risks / Issues

Risk / Issue	Top Project Risks/Issues (With Impact)	Likelihood (Current 1-5)	Impact (Current 1-5)	Risk Score (Current)	Mitigation (Route to Green)
~~Risk 1~~	~~There is a risk that the business will not be PCI compliant within the required deadline - 28th December 2017.~~	4	4	~~16~~	~~Engage stakeholders and PM/BA to monitor the remediation plan~~ ~~Note: We did experience the same challenges last year and we were able to manage/ mitigate this successful with our QSA and card acquirer Global Payments. This has been raised to both FST and Retail risk managers.~~ Risk superseded by risk 3.
Risk 2	There is a risk that the business will not be PCI compliant by the IPA-proposed remediation date of 30th March 2018	5	5	25	Formation of a weekly stakeholder steering committee every Friday and updating of RCC. Setting accountabilities with Nettitude. QSA peer review of findings. Commencement of remediation plan including tracking actions. Measurement/Output – achievement of PCI certification by or before revised 31/3/18 deadline. Engage with Acquirer, Partner Banks and Gov Clients to advise of current position and provide high level plan to compliance
~~Risk 3~~	~~There is a risk that POL change freeze (commencing 20/11) will prevent remediation activities from being completed, increasing the likelihood of risk 1.~~	~~1~~	~~5~~	~~5~~	~~Request dispensation with system Owners to conduct change-related activities inside of change freeze window.~~ Risk closed: POL change freeze has ended.
Risk 4	There is a risk that the scope of actions identified falls outside of the contracted services provided by suppliers, requiring contract revision or amendment and increased cost of service provision.	4	4	16	Agree scope of service with suppliers and procurement Estimate additional costs and present business case for future funding approval 3 CRs have been raised to CC to resolve the disputed scope of their obligations.
Risk 5	IRRELEVANT				
Risk 6	There is a risk that the segmentation/penetration test results identify additional remediation activities that will take until after 31/3 to complete.	1	3	3	Agree with FJ to remediate Seg/pen test results as matter of priority Note: as the potential seg/penetration issues are "unknown unknowns" is it not possible to know all mitigation activities at this early stage.
Issue 1	IRRELEVANT				
Issue 2					

POL00401626

Update on Suppliers

Supplier	Target Resolution Date	Update on Remediation	Status ("In Progress"/"Cannot Address"/"Closed")	Mitigation If Status = "Cannot Address"
Fujitsu	31/03/18	Fujitsu 35 Emerging Findings 3 Finding Closed by QSA 25 Findings marked as Complete (QSA to review and close) 7 Emerging findings In Progress 0 Emerging Findings To Initiate CR raised and approved for FJS to provide consultancy assistance for an "at source" solution for the data flowing from Horizon through PODG and Credence.	In progress	
Computa-Center	31/3/18	Computacenter 32 Emerging Findings 5 Finding Closed by QSA 17 Complete to be closed by QSA 10 Emerging findings In Progress 4 Findings above in progress Change Requests have been raised.	In progress	
Verizon	28/12/17	Verizon's scope for remediation is limited but may include wi-fi vulnerability scanning and identifying unauthorised connected devices. Scope to be confirmed	In progress	
IPA	30/3/18	Organising outstanding audit activities with QSA: • 46 branches visits were completed over the past 3 weeks • Completed the planned sample size of 60 branches • Arranged the Fujitsu Belfast site visit which shall take place W/C 5th March • Article on card machine tamper checks was published onto branch focus	In progress	
Accenture	04/03/18 ~~21/02/18~~ ~~12/02/18~~ ~~08/02/18~~	Issues in test identified; awaiting resource from data team to confirm issues resolved. Targeting 28/2 for forward fix, 4/3 for historic cleanse CR approved for Accenture to obfuscate the PAN data from Credence – due for delivery approx. 12th Feb 18 CR raise for Accenture to provide a solution to remove the PAN data from the Credence server (which the data lands on from PODG before being FTP to Credence	In Progress	

POL00401626

Procurement Compliance Reporting

Author: Barbara Brannon Sponsor: Al Cameron Meeting Date: 13 March 2018

Executive Summary

Context

As a business in receipt of public funds POL is bound by the Public Contract Regulations (2015). PCR 2015 oblige POL to behave in a fair, objective & transparent way when contracting with 3rd party suppliers. Additionally, set procedures must be followed for spend above £25k and £181,302 (total contract value, increased from £164,500 in 2018).

Failure to abide by the legislation or "slicing and dicing" contracts exposes POL to risk, both as far the commercial outcomes of the contracts as well as the reputational damage, legal remedies, censure & fines that can follow the discovery of a breach. Our compliance to PCR can be requested under a Freedom of Information request at any time.

The PCR Compliance Register allows for the tracking of breaches to PCR regulations at the Post Office and internal governance processes. One aim of collating this information is to drive improvement in awareness and compliance behaviour across the organisation. The second and primary aim is to work with GE and Business Units to commence commercial reviews in a more timely way ensuring POL obtains value, commercial and contractual flexibility fitting the requirements and business strategy of the organisation.

Questions addressed in this paper

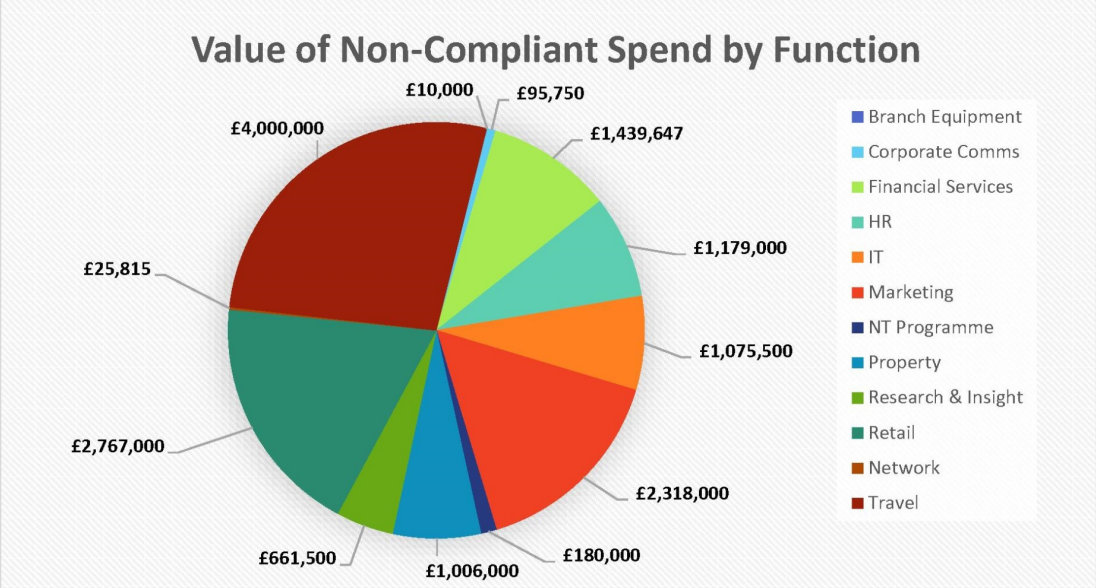
1. *How many and what types of procurement non-compliance have occurred in the past quarter?*
   Since the last RCC in October there have been a total of 0 non-compliant incidents with a total value of £0.

2. *What are we doing about it?*
   In the past quarter, while we have no new non-compliant spend we have reviewed and adjusted forecast spend data against actuals resulting in a small reduction in risk exposure overall. Our overall value has therefore dropped from £15m in January to £14.75m in March.

POL00401626

Open non-compliant awards since January 2017 are outlined below:

Function	January - Sum of Value	March - Sum of Value
Branch Equipment	£ 10,000	£ 10,000
Corporate Comms	£ 95,750	£ 95,750
Financial Services	£ 1,289,647	£ 1,439,647
HR	£ 1,579,000	£ 1,179,000
IT	£ 1,075,500	£ 1,075,500
Marketing	£ 2,318,000	£ 2,318,000
NT Programme	£ 180,000	£ 180,000
Property	£ 1,006,000	£ 1,006,000
Research & Insight	£ 661,500	£ 661,500
Retail	£ 2,767,000	£ 2,767,000
Network	£ 25,815	£ 25,815
Travel	£ 4,000,000	£ 4,000,000
Grand Total	**£ 15,008,212**	**£ 14,758,212**



3. What are the potential consequences?

a. Pre-contractual remedies overview: During a Procurement, an aggrieved party can seek an interim injunction suspending the tender or the implementation until the court decides on an outcome.
b. Post-contractual remedies: The court can order an 'ineffectiveness order' rendering the contract void &/or can award damages.

4. Why are these incidents occurring, and what can be done about it?

Non-compliant awards are made for a variety of reasons at the Post Office.

POL00401626

a) Low value, time constrained or highly sensitive/specialist engagements are common. For example, the Board have requested a number of expedited reviews since the New Year on a short turn-around time.
b) Large commercial arrangements cannot often be easily competed or unravelled without operational impact, and re-procurement may be subject to a pending evolution of a supporting Business Strategy.
c) The contractual arrangements may pre-date PCR 2015 regulations or the contract novated during separation from RMG, automatically becoming non-compliant at the renewal point. Non-compliant awards are frequently made on a tactical basis to extend contractual services while public tender processes are executed.
d) Delays to public sector panels of suppliers becoming available. The Post office makes extensive use of this low cost route to market and new/refreshed panels are subject to frequent delays from Crown Commercial Services. Single interim extensions [of periods under 12 months] while tender processes are run are considered to be low risk legally.
e) Changes in scope or value over the term of a contract may render the extension or renewal of services non-compliant. Material changes to the scope of a contract may render the whole contract non-compliant.
f) Disregard for, or lack of understanding of the regulations.

5. *Why are we receiving this report now?*

A decision to collate this information into a single location was taken in the Autumn of 2016. The aim is to track and improve our overall compliance and commercial results as an organisation, while also ensuring perceptions are accurate. However it should be noted that it will facilitate timely responses to Freedom of Information requests which adds risk to the Post Office commercial landscape.

6. *What is in the current Procurement pipeline which is high value and at risk of being awarded non-compliantly?*

A full list is appended at Appendix B. Since the last RCC in January 2018, three material items have been added. Two short term contract extensions for Internal Communications services and Events Management have been proposed while tender processes are concluded however, the extension provides commercial and contractual cover with no commitment to spend. The aim is to expedite the tenders to ensure any pending large value work goes under a new supply agreement.

POL00401626

The last item is for POL's ATM supply and maintenance services currently provided by Bank of Ireland. The value of this contract is £30m (p.a.) in income/revenue to POL. It was exempt from PCR when awarded in 2005 and the re-stated contract in 2014 but any new contract that POL intends to enter into will now be subject to the Concession Contracts Regulations 2016 and is therefore requires to be published. The current contract expires on 31st March 2022.

BoI and POL have agreed in principle to extension of the individual [ATM] Licences that expire during the period of the current contract, up to 31st March 2022 and that this has been recorded in the POL/BoI ATM Monthly Board April 2017.

As the current contract was not subject to CCR and the PCR, it is unlikely that the above variation (extension) can be successfully challenged under those Regulations.

Conclusion

Non-compliant awards of contracts are already subject to extensive internal governance, legal and risk review, explicit GE and Board approval where value/risks reach a minimum threshold.

*The YTD non-compliance value is high at £**14,758,212** the majority of which are interim extensions while procurement processes are run and to allow for operational migration risk to be mitigated. Individually, all large value non-compliant contracts have been reviewed by appropriate Post Office governance forums with agreement on next steps and actions towards remediation allocated where appropriate.*

Executive support towards moving POL towards a more compliant footing is very strong, but equally as important there is extensive support towards the cultural change required to ensure that Procurement activities and outcomes will support longer term business strategies and we reduce commercial risk making our 3rd party arrangements fit for purpose.

Input Sought

Review and note content only.

POL00401626

The Report

1. *Are any of these breaches arguable on regulatory grounds or are they all breaches?*

A full explanation of the individual compliance breaches for direct awards over £181k [previously £164k] threshold is attached in Appendix A. Each entry details the nature of, and the value of the breach.

The Procurement Compliance Register does not at present give an indicative risk level attached to the award. This information is provided to the accountable executives under internal governance processes in the form of a PCR risk note before a contract above threshold is entered into, and if necessary under Legal Privilege. In addition, all signatories to a contract have sight of the Risk note as part of the Contract Authorisation Form [CAF].

All entries are compliance breaches. A period of challenge applies to each PCR breach once an aggrieved party becomes aware or ought to have become aware. This risk finally expires at 6 years from the date of breach. The defensibility of a legal challenge is outlined within a Risk Note.

2. *How many of the breaches were approved in advance and how many retrospectively?*

All contracts entered into during this period were compliant with internal governance processes on contract and commercial review. All were for awards of between £0 and £4,000,000.

3. *Why were the approvals given?*

The rationale for approval is relevant to the individual service and is detailed within Appendix A.

4. *What were the unapproved, material breaches?*

There were no unapproved, material breaches during this period.

5. Describe the causes of non-compliance to PCR regulations

Non-compliant awards of contract are made for a variety of reasons at the Post Office:

a) Low value, time constrained or highly sensitive/specialist engagements are common. For example, the Board have requested a number of expedited reviews since the New Year on a short turn-around time.
b) Large commercial arrangements cannot often be easily competed or unravelled without operational impact, and re-procurement may be subject to a pending evolution of a supporting Business Strategy.
c) The contractual arrangements may pre-date PCR 2015 regulations or the contract novated during separation from RMG, automatically becoming non-

POL00401626

compliant at the renewal point. Non-compliant awards are frequently made on a tactical basis to extend contractual services while public tender processes are executed.

d) Delays to public sector panels of suppliers becoming available. The Post office makes extensive use of this low cost route to market and new/refreshed panels are subject to frequent delays from Crown Commercial Services.
e) Changes in scope over the term of a contract may render the extension or renewal of services non-compliant. Material changes to the scope of a contract may render the whole contract non-compliant.
f) Disregard for, or lack of understanding of the regulations.

6. *Describe what you are doing about the breaches. Where we are in breach, do we have a plan to come back into compliance and over what time period will that plan take effect?*

a) A forward view of material contracts falling under each Business Unit is currently prepared by the relevant Procurement Manager for discussions with their key stakeholders. The maturity of this look ahead view does vary currently and is a high priority activity within the team.
b) Sourcing options papers are prepared for review by contract managers and key stakeholders [risk, legal, security] with routes to market agreed. In many cases these are dependent on evolving business and operating model strategies and the Procurement team are now actively involved with some units helping to advise as thinking evolves.
c) Where a non-compliant award is proposed due to time pressure, Procurement are actively working on long term mitigation with awards made on an interim basis to meet urgent operational needs.
d) Each RCC member will now receive a regular report on compliance within their business unit[s].
e) A new Risk & Governance process requires a Risk Exception report to be created for non-compliant direct awards with SLT or GE sign off.
f) All Professional Services engagements must be approved in writing in advance by the COO. A compliant panel of preferred consulting partners has been appointed and proposed engagements outside of this panel are subject to additional review and challenge.
g) Procurement will now provide training as part of the revised Induction process for new staff. Training packs are being updated for existing staff and made available on the Intranet and ad hoc training sessions for interested Business Units are being run.
h) A new Intranet site has been launched for Procurement to improve visibility of process, regulation, and the panels of approved compliant suppliers available to POL business units.
i) A revised POL Procurement Policy is being drafted giving more granular guidance.
j) Using Crown Commercial Services frameworks, panels of Preferred Suppliers are being refreshed and updated across a wide range of spend categories to reduce time to market, improve compliance and greatly improve commercial outcomes and legal risk.

POL00401626

k) A planned change to operational systems will, once live, give Procurement earlier visibility of potential compliance issues eg: contractual value thresholds.

Appendices

1. Appendix A PCR Compliance Risk Register [Attached]
2. Appendix B Procurement Pipeline [Attached]

POL00401626

APPENDIX A

Incident Ref No	Date	Category Manager	Procurement Category	Function	GE Member	User / Staff Name	Value/ Income	PCR Compliance Resolved	Supplier Name	Breach Type 1 - PCR Threshold	Event (what happened) ONLY FOR £25K>	Actions Taken ONLY FOR £25K>	Further Planned Actions ONLY FOR £25K>
2017/0009	21 March 2017	Nicola Sams	Comms, R&I & PR	Research & Insight	Paula Vennells	Ruth Moyer	£ 652,000	OPEN	Inmoment	PCR - >£164.5k	Voice of Customer tracking is used as a performance measure for the business. It used to be a measure for the whole business but is now a measure for the individual Post office's performance	Due to the tracker still being an important measure for the individual post offices the supplerls contracgt will be extended.	Once POL understands how it wants to measure performance a review of current CCS framework that may be applicable or an full OJEU for the requirement will be conducted. Pending Long term requirements and budget from Marketing.
2017/0013	23 March 2017	Antony Ray	Professional Services	HR	Martin Kirke	Stacie Drury	£ 300,000	OPEN	Various	PCR - >£164.5k	Requirements and HR personnel changed. OLD PSL fell into disuse.	As a temporary measure, a short term agreement with standardise commercial terms and fees has been implemented with approximately 50 suppliers. The agreement effective from 1st July 2017 is in place until 31st March 2018 with an option to extend if necessary.	Current short term agreements in place with recruitment agencies due to expire on 31st March 2018. As the new CCS isn't available yet, these will be extended for a further 6 months before we move to a permanent solution. HR is now undertaking a review to determine agency use and spend, hence we will be extending only with the agencies we used the most and performed well. CCS now finalizing tender documents for new Permanent Recruitment framework which
2017/0016	12 April 2017	Nicola Sams	Marketing	Marketing	Nick Kennett	Louise Fowler	£ 2,000,000	WIP	Latitude	PCR - >£164.5k	Latest requisition is sub-OJEU threshold but there are several per month that support mainly Credit Cards, Loans and Mortgage products.	Seeking proposal from Carat (Media Agency) for consolidation within their compliantly let contract.	If proposal is acceptable from Carat then consolidate with them enabling an integrated approach to our full media investment.
2017/0019	01 June 2017	Antony Ray	Professional Services	HR	Martin Kirke	Harpreet Singh	£ 400,000		Towers Watson	PCR - >£164.5k		It was agreed to close the RMPP (DB Pension scheme) in 2016, closure required actuarial advice from a provider that knew the history and complexity of the RMPP. It was necessary to keep Towers Watson for their expertise.	In line with the Board strategy to de-risk the RMPP as far as possible, PO has requested that the Trustee of RMPP look to buy-out the liabilities of the RMPP as soon as possible whilst not requiring further money from PO. The earliest this can happen is 1 April 2018. It is anticipated that the majority of RMPP liabilities will be bought out by 1 April 2019 at the latest. Actuarial advice will be required during this phase. Anticpated spend to 2019 will be £135k. If buy-out occurs in 2018 spend will be £75k.
2017/0028	01 May 2017	Kelly Snares	IT Software	Financial Services	Nick Kennett	John O'Nell	£ 700,000	OPEN	Salesforce	PCR - >£164.5k	Continuation of POL CRM system. 1 year award. Awaiting strategy.	Non-compliant extension in place	CRM Platform to be re-tendered as it has previously been purchased non-compliantly. Awaiting strategy and confirmation of requirements from IT before Procurement approach can be agreed. Renewal due in April 2018.
2017/0036	30 October 2017	Antony Ray	Professional Services	Financial Services	Nick Kennett	Nick Kennett	£ 450,000	OPEN	Mckinsey	PCR - >£164.5k	Direct award with no contract or CAF. Steps are being taken to rectify this but work already completed.	Contract and CAF being raised by business retrospectively	Contract and CAF being raised by business retrospectively
2017/0038	01 January 2018	William Porter	Property	Property	Alisdair Cameron	Steve Norris	£ 1,000,000	OPEN	BNP Paribas	PCR - >£164.5k	Non-compliant but competitive process process for the provision of Estates Management, Rates Management & Treasury Services run in late 2016. Subsequent negotiations have been extended. Contract now finalised.		
2017/0041	10 January 2018	Angela Lamarra	Travel	Travel	Alisdair Cameron	Barbara Brannon	£ 4,000,000	OPEN	CAPITA	PCR - >£164.5k	POL contract with Capita Travel & Events originally commenced on 01 st April 2014 with an initial term up to 30th September 2015 and an option to extend until 15th November 2015.The Contract was subsequently varied to extend for two years until 30th September 2017. The two year extension was non-compliant under the Public Contracts Regulations 2015 as the extension was not provided for under the original terms of the contract.	The Mitigation plan agreed by the Sourcing Council was the following: extending the Capita contracts expiring on the 30th Sept 2017 for 6 months with commitment to utilise the new CCS framework once available. This was supposed to be be awarded on the 31st October 2017 but CCS decided to cancel this and re-issue a new OJEU. The new Framework will be available in March 2018 therefore our Mitigation Plan has been modified. Current contracts will be extended until 31st March 2018. After March 2018 the contracts will continue on a roll-over	CCS have just communicated that the tender process is now complete and suppliers have been selected. Details of the award will be published via the Official Journal of the European Union in the following weeks. Once the agreement is made available and the effective date is communicated, we will be able to run a Tender as part of the Call Off Process in order to refine our requirements
2017/0042	10 January 2018	Angela Lamarra	Professional Services	HR	Martin Kirke	Sean Leahy	£ 400,000	OPEN	Experian	PCR - >£164.5k	A non-compliant interim solution (6 month contract) was put in place with the supplier Experian following a Mini Tender. The agreement effective date is the 8th Feb 2017. At the end of the initial term (6 months), the agreement continues unless terminated by giving 2 month notice	The 6 month Initial Term with Experian terminated on the 8th Aug 2017, a 2 month roll-over solution is now in place. In the past few months the Business Unit wasn't able to finalize the scope of service because the Government was still in the process of issuing/publishing the new Vetting Regulation for all public companies; - HMRC have now published the new regulation and POL is in consultation with them in order to define what is applicable for our business and	The Internal solution (Identity Assurance platform to be extended) is now being discussed as a possible option rather than tendering the requirement
2017/0043	10 January 2018	Anne Cundy	Goods for Resale	Identity	Martin Edwards	Jonathan P Evans	£ 2,500,000	OPEN	Digidentity B.V	PCR - >£164.5k	Initial contract awarded following a non-compliant tender process (RFI with selected Bidders v full OJEU) to support award to POL under the Government FWA (Cabinet Office) for Identity Assurance for a 21 month period to 30/11/17.) 12 month extension required whilst POL strategy is determined.	Current strategy meetings being undertaken.	Legal risk note from Womble Bond Dickinson November 2017 "a medium risk of breach of procurement law though, absent any notice having been received from other providers in the intervening period, the likelihood of a challenge being brought against the extension and variation is probably low." Current strategy meetings being undertaken. **05/03/18 Confidential: Options may include the forming of a subsidiary company.**
2017/0044	10 January 2018	Shahab Hasan	IT Software	IT	Rob Houghton	Andy Garner	£ 788,000	OPEN	NCR	PCR - >£164.5k	Contract about to expire, contract value to be reached imminently. Need to continue to procure additional SSK units and ongoing support and maintenance services (including for existing units) for up to 6 months whilst we compliantly reprocure via OJEU and successful bidder completes set up	Working with business to understand other compliant routes to source ongoing provision whilst OJEU is carried out and successful supplier can complete set up	
							£ 12,538,000						

POL00401626

APPENDIX B : Procurement Pipeline - High Value Forecast or At Risk of Non Compliance

Date Logged	Procurement Category Manager	Procurement Category	Function	GE Member	SLT Owner	Description of Service	Supplier Name	Contract Expiry Date	*Estimate Value / Income per annum	Description of Issue >£164k	PCR Risk Rating H/M/L	Current Status / Mitigation Actions Taken	Key Decisions Outstanding
10/01/2018	Rhona Mclaren	Marketing	Marketing	Owen Woodley	Louise Fowler	Print Services	HH Global	31st March 2018	£ 4,000,000	Contract due to expire March 2018. A short term non compliant contract extension will be needed to give sufficient time to complete the procurement activity and potential transition time. Plan in place to complete 4 month extension proposed to cover this period of risk.	L	Tender is now live with responses and supplier pitches taking place in March.	Formal agreement for a non compliant contract extension and support for agreed timetable across POL.
10/01/2018	Rhona Mclaren	Marketing	Marketing	Owen Woodley	Louise Fowler	Media Buying	Carat	30th April 2018	£ 25,000,000	Contract due to expire Nov 2018. CCS have not completed the retender of the framework, this is now due to be awarded May 2018 with go live Nov 2018. Marketing have agreed to await the outcome of the CCS framework in May and review their supplier options at that point.	L	Extension of current contract to Nov 2018 to maintain contract compliance is now underway.	Formal agreement for a compliant contract extension. **Risk of SME resource shortage due to senior leadership changes**
10/01/2018	Rhona Mclaren	Marketing	Marketing	Owen Woodley	Louise Fowler	Data Services	RAPP	31st March 2018	£ 1,300,000	Contract has been extended non-compliantly for several years and has been under review between IT and Marketing for almost 12 months as part of a possible CRM / Data strategy. Decision made to proceed on basis of current scope for IT requirements but marketing seeking to change their aspect of the commercial model. GDPR concerns which are under investigation.	M	The current plan is to extend non compliantly to 31st March 2019 (12 months) while the business – marketing teams stated preference is OJEU for full service, IT have yet to confirm that this approach is acceptable. An OJEU process is likely to take up to 12 months with a transition of live service thereafter.	Formal agreement for a non compliant contract extension and support for agreed timetable across POL. **Confirmation that the OJEU route to market is acceptable to both IT and marketing**
10/01/2018	Rhona Mclaren	Marketing	Marketing	Owen Woodley	Louise Fowler	Creative	Mullen Lowe	31st March 2018	£ 1,800,000	Contract due to expire March 2018. Reprocurement exercise is now underway using the CCS framework. A non compliant extension is required until Oct 2018 to cover period of delay.	M	Extension of current contract until Oct 2018 to allow time for reprocurement	Formal agreement for a non compliant contract extension and support for agreed timetable across POL.
01/03/2018	Rhona Mclaren	Marketing	Marketing	Owen Woodley	Louise Fowler	Market data	Media Lab	14th April 2018	£ 175,000	Contract was awarded under an OJEU but the ability to extend compliantly has now ended. A 1 year non compliant extension is now required while marketing review their strategy and GDPR implications of utilising cold data	M	Non compliant 1 year contract extension with 3 months termination for convenience rights in the contract	Formal agreement to a non compliant contract extension
01/03/2018	Rhona Mclaren	Marketing	Marketing	Owen Woodley	Louise Fowler	Market data	CACI	14th April 2018	£ 110,000	Contract was awarded under an OJEU but the ability to extend compliantly has now ended. A 1 year non compliant extension is now required while marketing review their strategy and GDPR implications of data analysis services.	L	Non compliant 1 year contract extension with 3 months termination for convenience rights in the contract	Formal agreement to a non compliant contract extension
10/01/2018	Angela Lamarra	Services	Human Resources	Martin Kirke	Sean Leahy	Employee Vetting Services	Experian	8th August 2017*	£ 400,000	Initial 6 month contract is now rolling on a monthly basis while POL agrees sourcing strategy for delivery of service.	M	Stalled: Pending identity strategy and whether POL will insource the service/provide through a subsidiary. Currently at risk of challenge with value increasing monthly.	Timetable.
10/01/2018	Anne Cundy	Retail	Retail	Debbie Smith	Keith Maple	DMB Retail Audit - stationery mailing products	OCS Group UK Ltd (MORECAMBE)	31st May 2018	£ 850,000	Contract will exceed the posted OJEU value during the original procurement to the value of est. £850k (20% over forecast).	L	Service will transfer to WHS - no action required. One final audit due this month Jan then services being undertaken by WHS under the new Retail Arrangement.	None. Termination notice will be issued post audit. Reported January 2018
10/01/2018	Anne Cundy	Retail	Retail	Debbie Smith	Nick Spicer	Visa & Master Card	Global Payments	8th May 2019	£ 10,000,000	The Original Global Pay Agreement was compliantly awarded under a public PCR procedure, covering a period of 5 years to 08/05/17. With TWO x 12 month options to extend. It has become non compliant only because it is now over the forecast value during the OJEU process.	L	A 3rd extension is also being sought for 19/20 pending planned technology roadmap/upgrades.This extension would be legally non-compliant but allow the tender process to be completed at low risk [CMS McKenna]. The intention is to tender under CCS Framework agreement [Merchant Acquiring] effective for award by 09/05/20. The extension period could be reduced in part if the incumbent retains the business. If technology upgrades are completed by FJ, switching provider becomes faster and safer.	Legal advice is that this is low risk. **Detailed paper going to May Board.**
10/01/2018	Kelly Ross	Software	IT/FS	Owen Woodley / Rob Houghton	Jeff Smyth	Salesforce CRM Software	Salesforce	01/05/2018	£ 1,000,000	Contract is currently non-compliant and rolling annually	M	Separate risk paper going to RCC. Compliant route to resolve has been identified and legal advice obtained to that effect. Now subject to supplier negotiations.	None, other than review and approval of commercial outcome. **Risk of increased cost.**
02/03/2018	Angela Lamarra	Comms &PR	Comms	Mark Davies	Paul Swanton	Events Management	Live Union	31/03/2018	£ 500,000	Contract due to expire March 2018.	L	Currently reviewing the possibility to use CCS Frameworks (1. Communication services - Events. Framework has been awarded and it's available; 2. CCS Framework for Venue (Framework hasn't been officially awarded yet)	Agree strategy with Communications team
02/03/2018	Angela Lamarra	Comms &PR	Comms	Mark Davies	Paul Swanton	Internal Comms	AB Publishing; W&J Linney	31/03/2018	£ 300,000	Contract due to expire March 2018. A short term non compliant contract extension will be needed to give sufficient time to complete the procurement activity and potential transition time.	L	A suitable CCS Framework for Communication Services has been identified.	BU and Procurement working on tender Document
05/03/2018	Anne Cundy	Retail	Retail	Debbie Smith	Andrew Goddard	ATM maintenance	BOI	22/03/2022	**£ 30,000,000**	Whilst the BOI POL/ATM Agreement runs to 31/03/22, individual ATMs, start to fall out of contract after October 2018, on a gradual basis up to 31/03/22, however the POL/BOI ATM Board have agreed any such ATM's to continue to be in operation until 31st March 2022. The original contract (2005) and the contract variation (2014) were in place prior to the 2016 Concession Contract Regulations (CCR2016) came into force, therefore the risk of a successful challenge under the CCR 2016 is considered to be low given that the Regulations did not apply to this contract.	L	The ATM team are looking at POLs ATM strategy post 2022 (liaising with the wider supply chain cash strategy) which is being presented to the Board in May. Depending on the outcome of the strategy will impact on the Procurement Risk assessment i.e exit/reduce ATM estate v grow ATM estate. A further update will given at the May R&CC meeting.	ATM strategy - **Detailed paper going to May Board.**
									£ 75,435,000				

Note re *: Where compliant contracts are expiring the financial risk commences from the start of the new non-compliant term.
Where contracts are *already* non-compliant, an additional extension will also include the financial risk of the prior value committed.

POL00401626

Treasury Risk Management Framework, Policies and Authorities

Author: Mark Dixon Sponsor: Alisdair Cameron Meeting date: 13 March 2018

Executive Summary

Context

The Audit, Risk and Compliance Committee approved the most recent Treasury Risk Management Framework, Policies and Authorities (the "Treasury Policy") at its meeting in November 2016.

Our control framework requires an annual review and update of this document.

This paper provides an update as at March 2018 (the "March 2018 Treasury Policy Update").

Question addressed in this report

1. What changes have been made to the Treasury Policy?

Conclusion

We believe that the Treasury Framework, Policies and Authorities set out in the Appendix to this report are appropriate for an organisation of POL's size and complexity.

Input Sought

The RCC is asked to note the Treasury Risk Management Framework, Policies and Authorities set out in this paper for submission to the ARC Committee on 27 March 2018.

POL00401626

The Report

What changes have been made to the Treasury Policy?

1. The full Treasury Risk Management Framework, Policies and Authorities are set out in a Schedule to this paper.

2. The main changes proposed in March 2018 from November 2016 are listed below.

3. In order to conservatively manage its short-term liquidity the Group targets an investment reserve balance of £5m. At critical periods this may be varied. We have formalised delegated authorities around changes to this reserve such that the Head of Treasury, Tax and Insurance ("HoTTI") can approve a temporary change to the reserve so that the target is in the range nil to £20m and for a maximum of two weeks. Any changes outside this range or for a longer period will require approval by the CFOO. All changes will be reported to the Treasury Committee in the monthly Treasury Report. (See **3 Short-term Cash and Liquidity Management**.)

4. Drawdowns under existing facilities require approvals each time a drawdown is made. The delegated authorities vary according to the drawdown period. The delegated authorities for drawing under Other External Borrowings (up to £50m) now include an authority for the HoTTI to approve drawdowns up to 1 week. This has been added in order to ensure that drawings under the proposed £50m RCF (if implemented) can be made quickly and efficiently within deadlines. (See **3 Short-term Cash and Liquidity Management**.)

5. From time to time POMS may have surplus cash balances that it wishes to deposit with POL or may have short-term funding needs which can be satisfied by POL. The policy update delegates authority to the CFOO to agree and execute such loans on behalf of POL. (See **3 Short-term Cash and Liquidity Management**.)

6. Counterparty credit exposures primarily arise as a result of the investment of surplus cash. The March 2018 Treasury Policy Update recognises that other potential credit exposures may arise from the mark-to-market of our derivative activity and undrawn committed facilities provided by banks. The exposure on derivatives is currently minimal, as activity is limited to short-dated FX swaps and outrights, but potentially increases if we execute the POca interest rate swap. The exposure under undrawn committed facilities is currently limited to the undrawn portion of the £400 million of facilities provided by RBS in support of our participation in the Note Circulation Scheme. The exposure will increase if we enter into the £50 million Revolving Credit Facility which is likely to remain

POL00401626

undrawn. The Treasury Policy sets out limits for these exposures. (See **5 Counterparty Credit Risk Management**.)

7. In connection with the investment of surplus cash balances the January 2018 Treasury Policy Update now sets out credit rating bands within which credit limits will be allocated. This allows limits to automatically adjust with changes in ratings. This provides broadly the same limits for counterparty banks as per November 2016 with the exception of RBS, which, as a BBB+, is now restricted to a limit of £30 million (previously £60 million). In addition we have also formalised the procedures for the reporting of limit breaches. (See **6 Investment Risk Management**.)

8. The section on Guarantees/Group Support has been rewritten to distinguish: POL support for POMS; bank guarantees provided to support financing and commercial activity; and, Government support for the Group. The Treasury Policy ensures that any guarantee arrangement entered into in connection with a financing arrangement would require Board approval but that where guarantees are to support commercial activity delegated authority rests with the CFOO. (See **13 Guarantees / Group Support**.)

9. The Treasury Policy sets out the new reporting obligations from January 2018 arising under the European Markets Infrastructure ("EMIR") as a result of changes to MiFID II. (See **14 Regulatory Obligations**.)

10. In order to execute the POca interest rate swaps and to improve the control environment around its other derivative activity (FX swaps and outrights) the Group entered into ISDA Master Agreements in December 2017 with three relationship banks (RBS, Lloyds and Barclays) having received approval from the ARC. The ISDAs also facilitate compliance with new reporting obligations arising under EMIR. The Treasury Policy states that POL will only enter into derivative transactions with a counterparty with which it has executed an ISDA and will ensure that ISDAs are broadly standard across all counterparties. The March 2018 Treasury Policy Update provides a new delegated authority to the CFOO to approve and execute new ISDA agreements on behalf of POL. (See **15 ISDA Master Agreements**.)

11. Minor changes have been made to the governance and reporting section to reflect that the Treasury Committee is now part of the monthly Operations Board. (See **16 Treasury Governance and Reporting**.)

POL00401626

Schedule – Treasury Risk Management Framework, Policies and Authorities - March 2018

POL00401626

POST OFFICE LIMITED AND SUBSIDIARIES (THE "GROUP")

TREASURY RISK MANAGEMENT FRAMEWORK, POLICIES AND AUTHORITIES - MARCH 2018

		Page
I - Introduction		
1	**Background**	**2**
2	**Policy Overview**	**3**
II - Detailed Policies for the Management of Financial and Other Risks Relating to Treasury Activity		
Key Policies		
3	**Short-Term Cash and Liquidity Management**	**5**
4	**Medium and Long-term Funding Management**	**8**
5	**Counterparty Credit Risk Management**	**10**
6	**Investment Risk Management**	**12**
7	**Foreign Exchange Exposure Management**	**16**
8	**Interest Rate Exposure Management**	**18**
9	**Bank Relationship Management**	**19**
10	**Commodity Price Exposure Management**	**20**
Other Guidelines		
11	**Operational Banking**	**21**
12	**Payments**	**23**
13	**Guarantees and Indemnities / Group Support**	**25**
14	**Regulatory Obligations**	**26**
15	**ISDA Agreements**	**27**
III - Governance and Reporting		
16	**Treasury Governance and Reporting**	**28**
APPENDICES		
A	Summary of Counterparty Relationships, Services and Exposures	**30**
B	CHAPS Banks	**31**
C	Delegated Authorities for Authorisation Panels	**32**
D	Delegated Authorities for Drawdowns under Credit Facilities	**33**
E	Individual Write-off Authority Levels	**34**
F	Summary of Delegated Authorities	**35**

POL00401626

I - Introduction

1. Background

1.1. This document sets out the risk management framework, policies and authorities adopted by Post Office Limited ("POL") and its subsidiaries (together the "Group") in relation to its treasury activities and is an update of the paper approved by the ARC Committee in November 2016. It is recognised that Post Office Management Services Limited ("POMS") is subject to regulatory and fiduciary obligations which require derogation from some of the following policies. POMS will determine where there is a conflict between its obligations and these policies and amendments will be agreed and documented. A service agreement will set out the treasury activities which will be carried out on behalf of POMS.

1.2 The treasury risk management framework has been designed to:

- protect financial asset values;
- minimise income statement volatility;
- ensure financial obligations are met as they fall due;
- secure long-term funding to meet overall business objectives and shareholder return requirements;
- ensure regulatory obligations are met.

1.3 The key treasury risks are:

- *Short-term cash and liquidity risk* – the Group does not have sufficient short-term liquidity to meet payment obligations;
- *Medium and long-term funding risk* – the Group does not have sufficient committed long-term funding in place to meet business objectives and going concern obligations;
- *Counterparty credit risk* – a financial institution counterparty cannot meet its obligations to the Group. Such obligations may arise from: investing the Group's surplus cash balances (see investment risk, below); entering into derivatives transactions; entering into committed facility arrangements; and certain other commercial arrangements with clients.
- *Investment risk* – arising from investing the Group's surplus cash balances;
- *Foreign exchange risk* - arising from holding currency note inventory in branches and cash centres to meet on-demand requirements from customers;
- *Interest rate risk* – arising from the impact of changes in interest rates on the cost of funding, the returns earned on the investment of surplus cash, and the returns earned on the POca cash balances;
- *Bank relationship risk* – the Group does not manage its bank relationships in an appropriate manner;
- *Commodity price risk* – arising from the impact of changes in commodity prices on operational costs;
- *Settlement risk* – the risk that operational and business payments are not executed in accordance with agreed policies and procedures, are not settled in a timely manner or are exposed to the possibility of fraud;
- *Regulatory risk* – arising from POL failing to meet its regulatory obligations around its treasury activities;
- Proper recording of treasury transactions, including the reconciliation of bank statement balances to ledger balances in a timely manner;
- Loss or theft of cash.

POL00401626

2. Policy Overview

2.1 The Board is averse to treasury risk. The risk management framework and policies have been designed to reduce risk and concentrate on five principal areas to achieve this:

- **Market Risk**: to minimise any potential loss due to a change in market factors (e.g. interest rates, exchange rates or commodity prices);
- **Credit Risk**: to minimise any potential loss due to a change in the credit-worthiness of a counterparty;
- **Business Risk**: to minimise any potential loss due to economic factors;
- **Operational Risk**: to minimise any potential loss due to system, people, legal and other external events;
- **Regulatory Risk**: to minimise the risk that POL fails to meet its regulatory obligations around treasury activities.

2.2 Day-to-day operation of treasury policy and the activities of the Treasury function are the responsibility of the Head of Treasury, Tax and Insurance (the "HoTTI"), who reports to the POL Finance Director (the "POL FD"). Treasury activities are reported on a monthly basis to the Treasury Committee, which is part of the Operations Board, for review and oversight. The composition and responsibilities of the Treasury Committee are set out in section 16.1.

2.3 Any proposed amendments to, or derogations from, policy will be considered in the Treasury Committee and approved by the Audit, Risk and Compliance ("ARC") Committee or, if appropriate, by the Board.

2.4 Treasury is responsible for the following activities. These activities will only be undertaken by Treasury unless an alternative arrangement has been formally approved by the ARC Committee or the Board:

- management of bank account structures to provide automated concentration of cash and/or offset of balances;
- management of the Group's short-term cash flow forecasting process;
- arrangement and management of short-term committed funding;
- monitoring the debt capital structure to ensure that the Group has sufficient funding to support medium and long-term forecast requirements and to minimise refinancing risks;
- management of short, medium and long-term borrowing requirements;
- providing input to and critical review of the Group's medium and long-term cash flow forecasting process;
- fulfilment of obligations under the rules of the Bank of England's Note Circulation Scheme;
- setting counterparty limits for the financial institutions with which Group does business;
- short-term liquidity management and the investment of surplus cash balances;
- executing FX hedges in accordance with the instructions of the FX Committee, using approved instruments to hedge out to a maximum of 3 months;
- monitoring net interest rate exposure;
- managing bank relationships, in relation to corporate treasury activity;
- monitoring exposure to commodity price volatility;
- executing payments and administrating payments systems;
- acting as a centre of excellence in providing guidance and advice on all operational banking, payments and other treasury-related matters;
- regularly reviewing mandates;
- ensuring adherence to internal controls around internet banking systems and security;
- ensuring adherence to treasury-related regulatory obligations.

2.5 Cash forecasting must be completed in accordance with Treasury's instructions and deadlines and will support short-term, medium-term and long-term forecasting with the current Strategic Plan of the Board (currently the 5-year plan to 2020/21). Any material variances are to be escalated to the POL FD.

2.6 Compliance with the treasury policies set out in this document is mandatory, subject to the derogations provided to POMS noted in 1.1 above.

POL00401626

2.7 **Delegated Authorities**

- *Approve treasury risk management framework, policies and authorities* - **ARC**
- *Approve amendments to or derogations from Treasury Risk Management Framework, Policies and Authorities* - **ARC**

POL00401626

II Detailed Policies for the Management of Financial and Other Risks Relating to Treasury Activity

Key Policies

3. Short-Term Cash and Liquidity Management

Business Context

3.1 On a daily basis the Group has significant operating, investing and financing cash flows across its bank accounts, arising in relation to client-related activity across our counters, and as well as its own business-related activity. Client-related inflows and outflows are material and volatile with approx. £65 billion of flows each year. Flows can vary significantly depending on the day of the week and time of year and can also be materially impacted by other factors, out of the Group's control, such as the weather. Even with appropriate long-term committed funding in place there is therefore a short-term liquidity risk that the Group does not have resources available to meet its day-to-day payment obligations as they fall due.

Risk Management Objectives

3.2 The objective of the short-term cash and liquidity management policy is to ensure that the Group has appropriate liquidity in the right place at the right time to meet its payment obligations as they fall due.

Main Policy Statement

3.3 Through a combination of efficient bank account structures and accurate short-term cash flow forecasting, together with access to appropriate levels of committed short-term liquidity, Treasury will ensure that the Group can meet its obligations as they fall due.

Supporting Policy Guidelines

3.4 Bank Account Structures

3.4.1 Where possible, Treasury will manage cash balances within pooling arrangements which enable cash to be efficiently and effectively concentrated and debit and credit balances to be offset. Business units are not permitted to operate bank accounts that are outside these pooling arrangements unless authorised in writing by Treasury.

3.4.2 **Delegated Authorities**

- *Approve addition of bank account to existing pooling arrangement* - IRRELEVANT
- *Approve removal of bank account from existing pooling arrangement*
- *Approve creation of new pooling arrangement* - IRRELEVANT

3.5 Short-term Cash Flow Forecasting

3.5.1 Short-term cash flow forecasting is an essential tool for the Group and enables it to have confidence that its committed facilities are sufficient to provide the liquidity needed to meet its day-to-day payment obligations.

3.5.2 Treasury will prepare a short-term, daily rolling forecast of the utilisation of the BEIS Facility and the NRF. The forecast, by day, covers a period of up to two accounting periods. Treasury will issue:

- daily reporting to the HoTTI analysing variances of same-day and two-day forecasts to actuals;
- a weekly Liquidity Report to the CFOO and POL FD updating the forecast for the following week and providing a variance analysis for last week;
- a monthly Forecast Update to the CFOO and POL FD updating the forecast for the following two periods and providing a variance analysis for the last period.

3.5.3 The forecasts and variances will be reviewed on a daily basis by the IRRELEVANT Monthly

POL00401626

Forecast Updates will be included in the Treasury Report and reviewed by the Treasury Committee. The ARC will be updated by exception.

3.6 Committed Short-term Funding

3.6.1 Treasury's first responsibility is to ensure that sufficient liquidity and facilities are available to the Group to fund its operations. Funding is therefore negotiated and managed centrally and the management of individual cash pools will be dealt with by Treasury.

3.6.2 Short-term liquidity is managed as follows: POL has access to a £950m working capital facility provided by the Department of Business, Energy and Industrial Strategy ("BEIS") (the "BEIS Facility"). The BEIS Facility is available until March 2021. A utilisation request must be provided to BEIS two days before drawdown. Forecasting variances may lead to a shortfall between the amount drawn down and the actual amount required. The strategy to mitigate the risk of a shortfall between forecast and actual funding requirements is to hold a IRRELEVANT Any changes to the IRRELEVANT will be reported to the Treasury Committee in the monthly Treasury Report. Treasury can also use a IRRELEVANT IRRELEVANT and/or use the NRF (see 3.6.3 below).

3.6.3 In addition, POL is a member of the Bank of England's Note Circulation Scheme (the "NCS"). The scheme allows POL to declare and sell eligible notes to the Bank of England (the "Bank") overnight with a commitment to buy those notes back from the Bank first thing the next morning. This reduces the Group's overnight funding requirement. The NCS rules require the provision of collateral to the Bank. Collateral is currently provided on behalf of POL under a Facilities Agreement entered into by POL with IRRELEVANT IRRELEVANT under which the bank makes available: a £400m intra-day facility; a £350m overnight NRF facility (for the purposes of providing overnight collateral to the Bank); and, a IRRELEVANT collateral facility, used in connection with our crime insurance.

3.6.4 The NCS rules also require that POL has a crime insurance in place that is compliant with BoE requirements.

3.6.5 The amount available to be used under the NRF over the course of the Bank's financial year (to October) is constrained by a cap (the "Cap") that POL generates, mainly as a function of outward rems processed from its NCS cash centres. Treasury will monitor utilisation of the NRF against the Cap to ensure that no more than the Cap generated is used over the course of the year and that financial penalties are therefore avoided. Cap generation and NRF utilisation will be reported to the Treasury Committee on a monthly basis via the Treasury Report.

3.6.6 Any new borrowings require Board approval. See 4 Medium and Long-term Funding Requirement.

3.6.7 The delegated authorities for drawdowns are set out in Appendix D and in 3.6.8 below.

3.6.8 **Delegated Authorities**

- *Approve change to Investment Reserve (in the range nil to £20m / for up to 2 weeks)* - IRRELEVANT
- *Approve change to Investment Reserve (up to £50m / for more 2 weeks)* - IRRELEVANT
- *Propose drawdown - under existing credit facilities* - **Dealing Panel**
- *Approve drawdown - under BEIS Facility* - **Various (see Appendix D)**
- *Approve drawdown - under other external borrowings (up to £50m)* - **Various (see Appendix D)**

[1] *These facilities are currently provided by* IRRELEVANT

POL00401626

3.7 Short-term Cash & Liquidity Arrangements with POMS

3.7.1 From time to time POMS may have surplus cash balances which it wishes to deposit with POL or it may have short-term funding needs which can be satisfied by POL.

3.7.2 POL is permitted to take loans from or make loans to POL.

3.7.3 All loans will be documented.

3.7.4 Margins on loans will be agreed between POL and POMS and will be on an arm's length basis.

3.7.5 For short-term loans and deposits up to 3 months, for amounts up to £50m, authority to agree margins and execute documentation, on behalf of POL only, is delegated to the CFOO.

3.7.6 For the avoidance of doubt, any loans to or from POMS will require the approval of the POMS Board.

3.7.7 At 2018 POMS is the only wholly-owned subsidiary of POL. In the event that new subsidiaries are introduced into the Group structure then, provided such subsidiaries are wholly-owned, then 3.7 will also be applicable for loans to/from those subsidiaries.

3.7.8 **Delegated Authorities**

- *Approve margin on intra-group loans to/from POMS on behalf of POL (up to £50m / up to 3 months)* - IRRELEVANT
- *Execute documentation for intra-group loans to/from POMS on behalf of POL (up to £50m and up to 3 months)* - IRRELEVANT
- *Execute documentation for intra-group loans to/from POMS on behalf of POL (over £50m or over 3 months)* IRRELEVANT

POL00401626

4. Medium and Long-term Funding Management

Business Context

4.1 The Group develops its strategic objectives and prepares long-term business plans to meet those objectives. Such objectives will include the continued participation in the Bank of England's Note Circulation Scheme (the NCS") in order to ensure an adequate supply of notes for the branch network. The Group must ensure that it has sufficient committed long-term funding in place to meet these plans. There is a risk that the funding in place is not sufficient to achieve business objectives or to adequately withstand unforeseen changes to plans.

4.2 In order to present its financial statements on a going concern basis the Group must demonstrate, on an annual basis at each balance sheet date, that it has sufficient committed funding in place.

4.3 The Group's existing funding arrangements, including the facilities made available to enable participation in the NCS, are set out in 3 Short-term Cash and Liquidity Management.

Risk Management Objective

4.4 The objective of the medium and long-term funding management policy is to ensure that the Group has sufficient committed long-term funding in place to meet business objectives and going concern obligations.

Main Policy Statement

4.5 Through a combination of accurate medium and long-term cash flow forecasts and the monitoring of headroom, together with access to appropriate levels of long-term committed funding, the Group will ensure it has sufficient funding in place to meet business objectives and going concern obligations.

Supporting Policy Guidelines

4.6 Medium and Long-term Cash Flow Forecasting

4.6.1 Medium and long-term cash flow forecasting is an essential tool for the Group and enables it to have confidence that its committed facilities are sufficient to provide the liquidity needed to meet its business objectives and loan repayments.

4.6.2 Treasury will provide input to Group's medium and long-term forecasts, in particular the one-year and five-year strategic forecasts and in accordance with the current Board Strategy.

4.7 Funding Strategy

4.7.1 The CFOO and the POL FD will recommend to the Board the appropriate debt capital structure for the Group. The Group will have a debt maturity profile and funding structure adequate to meet its:

- business objectives, including growth strategy;
- going concern obligations.

4.7.2 The debt capital structure and maturity profile will be monitored by the CFOO and POL FD, and reviewed by the Treasury Committee to ensure that the Group has appropriate funding available to support its long-term plans. Where possible, the Group seeks to minimise its refinancing risk by adopting a range of maturities for its debt facilities. Maturity of existing facilities will be monitored to ensure that negotiations commence in a timely manner to extend or replace them.

4.8 Headroom

4.8.1 *Facility Headroom* - Facility Headroom is defined as the headroom available under the BEIS Facility. The Group will aim to maintain Facility Headroom of at least IRRELEVANT (the "Facility Headroom Buffer"). Any reduction in Facility Headroom Buffer will require Board

POL00401626

approval. It will be monitored and reported in the monthly Treasury Report and the monthly Performance Report to the Board.

4.8.2 *Security Headroom* - Security Headroom is defined in the BEIS Facility. Treasury will also monitor the asset security headroom of the BEIS Facility. It will be reported in the monthly Treasury Report and the monthly Performance Report to the Board.

4.8.3 Treasury will use a combination of the short-term forecasts outlined in 3.5 above and the medium and long-term forecasts to monitor headroom.

4.8.4 **Delegated Authorities**

- Approve amendment to Facility Headroom Buffer - **Board**

4.9 Borrowing Policy

4.9.1 Borrowing is only permitted in sterling unless approved by the ARC.

4.9.2 Borrowing should only be incurred in accordance with the restrictions under clause 10 of POL's Articles of Association and may require shareholder approval.

4.9.3 Additional borrowing is only permitted in accordance with the constraints imposed under the BEIS Facility which limits borrowings as follows:

- the existing £950m BEIS Facility itself, or any refinancing thereof;
- up to £50m of additional finance or capital leases;
- up to £50m additional other borrowings.

Together with the facilities in place to support POL's participation in the NCS, namely:

- the £400m intra-day facility;
- the £350m overnight NRF facility.

4.9.4 **Delegated Authorities**

- Approve new medium and long-term funding - **Board**

POL00401626

5. Counterparty Credit Risk Management

Business Context

5.1 Counterparty credit risk arises where a financial institution counterparty cannot meet its obligations to the Group. Due to the nature of POL's business activities such exposures arise both as part of POL's normal corporate treasury activities and its other client-related activities. Exposures arise primarily as follows:

Corporate Treasury Activity

5.1.1 *Investment of Surplus Cash Balances* - Total exposure of approximately £5m but may increase up to £50m when the investment reserve is increased during holiday periods. (See 6. Investment Risk Management.)

5.1.2 *Mark-to-Market of Derivatives* - Derivative contracts (including FX swaps, FX forwards and interest rate swaps) where the mark-to-market position has moved in favour of POL such that the counterparty owes money to POL under the contract. Exposure arises due to changes in market rates. Because FX maturities are managed within one month total exposure is currently minimal.

5.1.3 *Committed Facilities* - Commitments made by a bank or other funding provider under facilities that remain undrawn by POL. Such facilities currently comprise: the BEIS Facility; and, the £400m intra-day facility / £350m overnight NRF facility provided by Royal Bank of Scotland plc. The exposure relating to the BEIS Facility is considered to be nil but there is an exposure on IRRELEVANT that fluctuates during the day depending on how much is utilised under the facilities. If the £50m RCF is arranged with IRRELEVANT an exposure of £50m will exist in connection with the facility, while it is undrawn, split evenly between the three banks. Total exposure may be up to **£450m**.

Other Client-Related Activity

5.1.4 *Banking Framework* - Over-the-counter banking transaction services with retail and business customers. Transactions are cleared through the LINK system with daily settlement to POL received from IRRELEVANT this creates a daily net direct exposure to IRRELEVANT of up to **£30m**. In addition, POL would also be exposed to the failure of an individual client bank to meet its obligations under the LINK system.

5.1.5 *Debit and Credit Card Processing* - When a customer makes a payment to POL over-the-counter using either a debit card or a credit card settlement is received by POL via GPUK LLP ("GlobalPay") on the next business day. This creates a one-day credit exposure against GlobalPay. Total exposure fluctuates but is approximately **£75m**.

5.1.6 *Cheque Clearing* - when a customer makes a payment to POL using a cheque it creates a short-term exposure (up to two days) exposure against the bank on which the cheque is drawn. The total exposure on cheques is approximately **£25m** but this is disaggregated between the banks on which the cheques are drawn.

5.1.7 *Other Client-Related Activity* - Exposures arising from other client-related activities.

- ATM Withdrawals – Exposure to Bank of Ireland linked to cash withdrawals from ATMs. The exposure varies significantly, depending on the time of the year and day of the week, between IRRELEVANT
- POca Related Flows – Exposure to IRRELEVANT in respect of POca-related flows across POL counters. Flows between 13:00 on the previous day and 13:00 are aggregated and paid same day. The exposure fluctuates significantly depending on the day of the week and time of the year and is impacted by holiday periods and winter fuel payments. It can vary between IRRELEVANT

5.2 This policy focuses on counterparty credit risk arising from POL's corporate treasury activities.

POL00401626

Risk Management Objectives

5.3 The objective of the counterparty credit risk management policy is to minimise the Group's risk of loss in its corporate treasury activities as a result of the failure of a financial institution counterparty.

Main Policy Statement

5.4 Treasury will minimise the risk of loss due to the failure of a financial institution counterparty to meet its obligations by only entering into corporate treasury transactions with highly-rated counterparties and through credit approvals, limits and monitoring procedures.

Supporting Policy Guidelines

5.5 Treasury will only enter into corporate treasury transactions with appropriately approved financial institution counterparties.

5.6 The Group's corporate treasury-related credit risk arises primarily from the investment of surplus cash balances. For the purpose of the investment of surplus cash balances limits are allocated according to rating band rather than specified counterparty. Approved counterparties and sub-limits applicable to deposits (as at March 2018) are set out in 6 Investment Risk Management. Deposit limits will fluctuate with changes to credit ratings.

5.7 When monitoring the credit quality of counterparties Treasury will use short-term and long-term credit ratings from S&P and Fitch. The weaker of the two ratings will be used for decision-making purposes.

5.8 Approved counterparties and credit limits for other transaction types are set out in Appendix A.

5.9 New counterparties and limits may be approved from time to time. Treasury will make a recommendation to the Treasury Committee based on credit ratings for consideration and recommendation to the ARC.

5.10 Exposures to investment counterparties will be monitored separately and reported to the HoTTI on a daily basis and to the Treasury Committee on a monthly basis in the Treasury Report. See 6. Investment Risk Management. Exposures to corporate treasury counterparty activities will be aggregated (including investment counterparties) and reported to the Treasury Committee on a monthly basis together with changes to credit ratings as part of the Treasury Report.

5.11 **Delegated Authorities**

- *Approve new financial institution counterparty* - **ARC**
- *Approve financial institution counterparty limit* - **ARC**
- *Approve temporary increase to financial institution counterparty limit* - IRRELEVANT

5.12 Note on the Implications of Ring-fencing - *Effective 1 January 2019 the major UK banks are required to implement the Government's ring-fencing requirements. In 2018 the Group's facilities with* IRRELEVANT *will be transferred to* IRRELEVANT *as part of the bank's restructuring to meet these requirements. From 2019 these facilities will sit inside the ring-fence. (It should be noted that any complex derivative activity would need to sit outside the ring-fence.) Provided that the S&P and Fitch long-term and short-term credit ratings of* IRRELEVANT IRRELEVANT *(or any other entity inside or outside the ring-fence) are the same as, or better than,* IRRELEVANT *then all references to* IRRELEVANT *are deemed to apply to* IRRELEVANT *(or those other entities). This approach will also be applied if* IRRELEVANT *adopt a similar strategy to ring-fencing in 2018.*

POL00401626

6. Investment Risk Management

Business Context

6.1 Treasury manages short-term liquidity to target a cash buffer of £5m. The buffer is reduced to nil at period ends and can be increased up to £50m around holiday periods when liquidity risks are highest. This creates surplus cash balances that can be invested by Treasury.

Risk Management Objectives

6.2 The three core objectives of the Group's investment risk management policy are: (i) *security* – to preserve the principal sum; (ii) *liquidity* – to ensure investments are accessible when needed; (iii) *yield* – to optimise return on investments.

Main Policy Statement

6.3 The Group's overall consideration when depositing surplus cash balances is the preservation of the principal sum. Surplus cash balances will be invested by Treasury to optimise return, subject to counterparty credit risk considerations. These investments will not be subject to fluctuation in capital values.

Supporting Policy Guidelines

6.4 Permitted Investment Instruments - Treasury are permitted to use the following investment instruments: bank term deposits and deposits on interest-bearing accounts; money market funds ("MMFs"); and, when appropriate, deposits with the Debt Management Office ("DMO").

6.5 Permitted Currencies – Treasury will only invest in £-denominated instruments.

6.6 Approved Bank Counterparties and Deposit Limits - It is the Group's policy to establish and monitor limits for each of the counterparties that it makes investments with.

6.6.1 Limits for term deposits and interest-bearing accounts ("deposit limits") are based on credit rating bands rather than specific counterparties. Counterparties are allocated to bands based on the lower of the S&P and Fitch long-term credit rating as follows:

Credit Rating (1)	Approved Limit (£m)
AAA	120
AA + to AA -	90
A + to A -	60
BBB +	30
BBB and below	0

(1) Based on lower of S&P and Fitch long-term credit rating

6.6.2 Counterparties must have a long-term S&P or Fitch credit rating of at least BBB+ and a short-term S&P or Fitch credit rating of A2/F2.

6.6.3 Counterparties must also be a member of CHAPS (see Appendix C for a list of CHAPS banks).

POL00401626

6.6.4 Approved counterparties and deposit limits based on credit ratings as at January 2018 are:

Financial Institution Counterparty	Credit Rating S&P Long-term	S&P Short-term	S&P Outlook	Fitch Long-term	Fitch Short-term	Fitch Outlook	Approved Deposit Limit (£m)
IRRELEVANT	A	A-1	Stable	A	F1	Positive	80.0
	BBB+	A-2	Stable	BBB+	F2	Stable	30.0
	A	A-1	Positive	A+	F1	Negative	60.0

6.6.5 The deposit limits against individual institutions are expected to change with changes in credit ratings.

6.6.5 *Exception* - IRRELEVANT as our cash management bank, is allocated an additional limit of £2m to allow for cash held as operational balances on bank accounts from time to time. IRRELEVANT long-term rating of A would imply a deposit limit of £60m. The limit is increased to £80m.

6.7 Other

6.7.1 Unauthorised arbitrage is prohibited i.e. funds should not be specifically drawn down for investment purposes.

6.7.2 Only Treasury is permitted to invest surplus cash balances.

6.7.3 A proposal for the investment of surplus cash balances will be made by the Dealing Panel and approved by either the Treasury Authorisation Panel (see Appendix C – Delegated Authorities for Approval Panels) or in accordance with 6.11 below.

6.7 Deposit Tenor Limits

6.7.1 Deposits will be no longer than one month.

6.8 Money Market Fund Investment Criteria - It is the Group's policy to establish and monitor limits for each of the MMFs that it invests in.

6.8.1 The MMF must be rated by at least one of S&P and Fitch. If rated it must be rated AAAm by S&P and AAAmmf by Fitch.

6.8.2 POL's holding as a proportion of the fund size must not be greater than 10%.

6.8.3 MMFs must have a constant net asset value (CNAV) (also referred to as stable NAV) or a Variable Net Asset value (VNAV) (also referred to as accumulating NAV).

6.8.4 MMFs must have daily liquidity.

6.8.5 Investment is limited to £50m in any one MMF.

6.8.6 Investment in Prime Liquidity Funds is limited to £350m.

6.8.7 Investment in Government Funds is limited to £150m.

6.8.9 Where a single provider has segregated Prime Liquidity Funds and Government Funds, investments can be made in both MMFs subject to the limits above.

POL00401626

6.9 Approved MMFs and limits as at January 2018 are:

Name of Fund	Credit Rating S&P	Credit Rating Fitch	Asset Class	Currency	Name of Return	Fund Size (£m)	Approved Limit (£m)	Approved Limit / Fund Size (%)
IRRELEVANT	AAAm	AAAmmf	Prime	GBP	CNAV	14,400	50.0	0.3%
	AAAm	AAAmmf	Prime	GBP	CNAV		50.0	#DIV/0!
	AAAm	AAAmmf	Prime	GBP	CNAV	14,400	50.0	0.3%
	AAAm	AAAmmf	Prime	GBP	CNAV	36,800	50.0	0.1%
	AAAm	na	Prime	GBP	CNAV	11,800	50.0	0.4%
	AAAm	AAAmmf	Prime	GBP			100.0	
							350.0	
	AAAm	AAAmmf	Government	GBP	CNAV	2,400	50.0	2.1%
	AAAm	AAAmmf	Government	GBP			100.0	
							150.0	

6.10 DMO Investment Criteria – The Group may invest with the DMO on an unlimited basis.

6.11 Operational Approvals - For each individual investment made approval is required as per the table below:

Investment Amount	< £300m	< £100m	< £50m	< £300m	< £50m	< £50m
Term of Investment	< 1 month	< 3 months	< 6 months	< 1 year	< 1 year	< 1 year
Delegated Authority	*1 member from Treasury Authorisation Panel*	*1 member from Treasury Authorisation Panel*	*1 member from Treasury Authorisation Panel*	IRRELEVANT		

The POL FD is also authorised to approve investments with a maturity of up to 5 years for the purpose of providing collateral for the Note Circulation Scheme.

6.12 Monitoring

6.12.1 Exposures to investment counterparties will be monitored separately and reported to the HoTTI on a daily basis and to the Treasury Committee on a monthly basis in the Treasury Report.

6.13 Limit Breaches

6.13.1 When Treasury are aware of a potential breach in advance (for example, when Treasury choose to hold in excess of the authorised limit because no other investments opportunities are available) approval must be obtained from either the CFOO or the POL FD for a temporary increase to the limit. The temporary increase will normally be for no longer than one night.

6.13.2 When Treasury are not aware of the breach in advance (for example, where we receive more cash into our IRRELEVANT accounts than we had forecasted) Treasury will notify the CFOO of the breach immediately on becoming aware of it but in any event no later than close of business on the day after the breach occurred.

POL00401626

6.13.3 All limit breaches will be reported to the Treasury Committee in the monthly Treasury Report.

6.14 **Delegated Authorities**

- *Approve new investment counterparty - within approved credit rating bands* - IRRELEVANT
- *Approve changes to credit rating bands for deposit limits* - **ARC**
- *Approve temporary increase to investment counterparty deposit limit* - IRRELEVANT
- *Approve new permitted investment instrument* - IRRELEVANT
- *Propose investment of surplus cash balances* - **Dealing Panel**
- *Approve investment of surplus cash balances* - **Various (see 6.11)**

POL00401626

7 Foreign Exchange Exposure Management

Business Context

7.1 Foreign exchange risk principally arises from holding foreign currency note inventory in branches and cash centres to meet "on demand" requirements from customers. All currencies are purchased from FRES. The exchange risk arises from the time of purchase from FRES to the sale of currency to the customer. The size of balances on hand is determined by demand. POL holds note inventory balances in approximately 70 currencies. On average, currency holdings are c. £60m but can peak at over £100m during holiday periods.

Risk Management Objectives

7.2 The objective of the foreign exchange exposure management policy is to minimise the impact on the Group's income statement of foreign currency exposures arising from its day-to-day operations.

Main Policy Statement

7.3 Through a combination of periodic monitoring of foreign exchange exposures and entering into hedges within approved hedging bands the Group will ensure its exposure to fluctuations in exchange rates is minimised.

Supporting Policy Guidelines

7.4 The Head of Travel Money analyses the report of foreign currency note holdings in the network which is prepared by Supply Chain and the daily reports of foreign currency holdings provided by Treasury.

7.5 A monthly meeting of the FX Committee is held, attended by: the Managing Director Post Office Money; the Finance Director Financial Services and Telecoms; and the Head of Travel. The meeting is held to confirm the value of hedges and timescales of hedges in accordance with the FX risk management policy outlined below.

7.6 Detailed foreign exchange risk management policy statements

7.6.1 EUR and USD holdings will be hedged 100%; currencies with exposures over £1.5m will be hedged 90% to 100%; other currencies with exposures over £1 million will be hedged 70%.

7.6.2 At least 80% and no more than 120% of qualifying exposures will be hedged based on the average of (1) the previous period's actual holdings and (2) the forecast for one month forward.

7.6.3 Hedges will be closed out and reset to periods between two weeks and five weeks. Longer-dated hedges will be set to mature at a monthend and will be revalued at each intervening month end based upon the mark-to-market valuation provided by the hedging bank.

7.6.4 Hedging will be conducted with counterparties approved by the Treasury Committee (see 5 Counterparty Credit Risk Management).

7.6.5 Trades will be executed at a pre-arranged margin with all counterparties.

7.6.6 The maturity of financial instruments used to hedge foreign exchange exposures will normally be about a month but can be no longer than three months.

7.6.7 Permitted Instruments - Foreign currency exposures can only be hedged using foreign currency outright forwards or swaps.

7.6.8 FX hedging instruments can only be used to hedge exposures generated by holding currencies to meet on-demand transactions by customers.

POL00401626

7.7 Latest currency holdings and hedges will be reviewed at the end of each period immediately before the maturity of the monthly hedges by Financial Director Financial Services and Telecoms and the Head of POL Travel.

7.8 On a monthly basis the Finance Director Financial Services and Telecoms will report to the Treasury Committee on the gain or loss on foreign currency holdings.

7.9 Any proposed changes to the policies above will be presented to the ARC Committee for approval.

7.10 **Delegated Authorities**

- *Execute FX hedge trades, within policy, in accordance with instructions issued by FX Committee* - **Treasury**
- *Approve new permitted FX hedging instrument* - IRRELEVANT
- *Approve FX hedge trades for exposures not created by currency note inventory holdings – up to £50m* - IRRELEVANT
- *Approve FX hedge trades for exposures not created by currency note inventory holdings – above £50m* - **Board**

POL00401626

8 Interest Rate Exposure Management

Business Context

8.1 The Group is exposed to changes in interest rates via its Libor-linked funding and the returns it earns on cash balances. Increases in interest rates will increase the Group's cost of funding and increase the return it earns on cash, mainly linked to Post Office card account ("POca") balances.

8.2 The Group's funding is via the BEIS Facility maturing in 2021 and the NRF. Interest rates on both facilities are linked to Libor. POL also earns commission (credited to revenue) on the balances of benefit payments held by JP Morgan, the POca cash balances. The commission interest received is also linked to Libor. The interest receivable on the POca cash balances has historically exceeded the interest payable on POL's borrowings and is expected to do so for the foreseeable future, despite the long-term decline of POca cash balances. The interest payable on POL's funding is a natural hedge of the commission interest receivable.

Risk Management Objectives

8.3 The objective of the interest rate risk management policy is to minimise exposures to income statement impacts of changes in interest rates.

Main Policy Statement

8.4 The Group will monitor its exposures to changes in interest rates on a regular basis and recommend hedging strategies, if appropriate.

Supporting Policy Guidelines

8.5 Treasury will obtain forecasts of interest payable / commission receivable and the net interest rate exposure will be monitored by Treasury and, if appropriate, a proposal to hedge the exposure will be put to the Treasury Committee prior to approval by the Board.

8.6 The suitability and effectiveness of the interest rate risk management policy will be reviewed at each Treasury Committee meeting. Any proposed changes will be reported to the ARC Committee for approval and submission to the Board.

8.7 Permitted Instruments - Hedging will be by way of interest rate swaps. Other instruments may be approved by the ARC on a case-by-case basis.

8.8 The Government's Managing Public Money Guidelines allow organisations to consider the use of derivatives but require them to consider their use carefully especially to assess value for money. The Guidelines require POL to consult its sponsoring department / HM Treasury before executing any derivative for the first time.

8.9 **Delegated Authorities**

- *Approve new permitted interest rate hedging instrument* - **ARC**
- *Approve execution of interest rate hedging strategy* - **Board**

POL00401626

9. Bank Relationship Management

Business Context

9.1 Good long-term relationships with banks are crucial to the success of the Group around its corporate treasury activities. The Group requires support from banks across all its treasury activities and this support is particularly important for the provision of: short-term liquidity, including operational overdrafts; credit facilities to enable continued participation in the Note Circulation Scheme; and, FX instruments and other derivatives, requiring credit to be extended.

9.2 Due to the UK-focused nature of the Group, the limited requirement for external funding and a small amount of ancillary treasury business, the Group has historically focussed on building relationships with a small group of UK clearing banks.

Risk Management Objective

9.3 The objective of the bank relationship management policy is to establish, maintain and develop efficient and effective banking relationships with a core group of banks to provide the Group with long-term banking support irrespective of short-term business conditions and financial market turbulence.

Main Policy Statement

9.4 The Group will seek to build long-term relationships with two to three of the UK clearing banks.

Supporting Policy Guidelines

9.5 It is the Group's policy to build long-term relationships with providers of banking services and facilities in order to maximise mutual advantage. In allocating new business opportunities, preference will generally be given to banks where a relationship already exists, but this does not preclude the use of other banks identified by Treasury should it be appropriate. Any new relationships will be reported to the Treasury Committee in the monthly Treasury Report for approval.

9.6 Current counterparty relationships, including banks, are listed in Appendix B.

9.7 Management of the Group's bank relationships is the responsibility of the IRRELEVANT and the IRRELEVANT IRRELEVANT. Bank selection will be determined by a number of factors, including service, price, product range, geographic spread and willingness to provide services. The decision to develop a new relationship will rest with the Treasury Committee.

9.8 From time to time POL may require that banking partners enter into Non-Disclosure Agreements ("NDAs") to protect Group-sensitive information. Approval will be required by the IRRELEVANT

9.9 **Delegated Authorities**

- *Approve entering into relationship with new bank* - **Treasury Committee**
- *Approve entering into relationship with new bank (prior to Treasury Committee approval)* - IRRELEVANT
- *Approve entering into NDA with bank* - IRRELEVANT

POL00401626

10 Commodity Price Exposure Management

Business Context

10.1 The Group is exposed to movements in the price of diesel, gas and electricity used throughout the business.

Risk Management Objectives

10.2 The objective of the commodity price exposure management policy is to minimise income statement volatility due to changes in commodity prices.

Main Policy Statement

10.3 Treasury will monitor exposures to these commodities and forecast price movements and may recommend hedging action to the Treasury Committee or directly to the IRRELEVANT to protect the Group from adverse price movements.

Supporting Policy Guidelines

10.4 The IRRELEVANT is authorised to hedge each commodity, where it is believed to be economic to do so, up to a maximum of 3 years based on forecast future usage.

10.5 Permitted Instruments - permitted hedging instruments are spot purchases, currency deposits, forward contracts, call options, matched options (e.g. cylinders) and swaps. Futures will not be used without specific authority of the IRRELEVANT

10.6 The Group will designate commodity cash flow hedges against forecast underlying exposures. Unrealised gains and losses on hedges will be deferred in reserves. This will be recycled to the income statement when the hedge matures to match forecast expenditure.

10.7 The suitability and effectiveness of the commodity price exposure management policy will be reviewed at each Treasury Committee meeting. Any proposed changes will be reported to the ARC Committee for approval and submission to the Board.

10.8 **Delegated Authorities**

- *Execute commodity price hedges within policy* - **Treasury**
- *Approve new commodity price hedge counterparty* - IRRELEVANT
- *Approve execution of commodity price hedge within policy* - IRRELEVANT

POL00401626

Other Guidelines

11. Operational Banking

11.1 Bank Facilities

11.1.1 Treasury is responsible for the negotiation of all operational banking facilities and any changes to existing operational facilities. Such facilities include overdrafts, fx lines, BACS limits, intra-day limits and any similar arrangements. Directorates do not have the authority to negotiate or commit to any new operational banking facilities without prior approval from Treasury and are not authorised to undertake any discussions regarding credit lines.

11.1.2 All changes to existing operational banking facilities or any new operational banking facilities must be agreed by the IRRELEVANT

11.2 Interest and Bank Charges

11.2.1 Bank transaction charges will be negotiated by Treasury to ensure minimum cost to the Group. Charges incurred will be reviewed by Treasury to ensure that the activity levels and unit costs applied by the banks to calculate charges are in accordance with agreed tariffs. Errors are to be notified directly to the bank.

11.3 Bank Accounts

11.3.1 It is the Group's policy to minimise the number of bank accounts it operates. Treasury will conduct a bi-annual audit to ensure it has an accurate record of bank accounts. Accounts not being utilised should be closed. This will be reconciled back to internal and bank records.

11.3.2 All new bank accounts will be approved by the IRRELEVANT

11.3.3 Where possible all accounts should be within a cash pooling arrangement. It is recognised that certain constraints apply to POMS cash, where restrictions may preclude pooling.

11.4 Bank Mandates

11.4.1 It is the Group's policy to standardise bank mandates wherever possible. Treasury will manage and administer all bank mandates centrally. Each bank account must be supported by a written, up-to-date mandate which is checked against a list of those colleagues leaving the business on a monthly basis.

11.4.2 Authority levels relating to internet banking systems will be documented separately.

11.4.3 Sole signatory on a bank account is not permitted except for cheques where one signatory may sign for amounts of up to £50,000.

11.5 Reconciliations

11.5.1 The Financial Accounting & Governance Manager is responsible for bank reconciliations.

11.5.2 The reconciliation process around certain bank accounts has been assigned to Treasury. For those accounts, Treasury will ensure that all bank accounts are reconciled to the underlying accounting records and all reconciling items are identified and cleared as appropriate, in a timely manner.

11.5.3 The IRRELEVANT will ensure that all Treasury-owned reconciliations have been properly carried out and provided to the relevant staff members reporting to the IRRELEVANT in accordance with prescribed deadlines.

POL00401626

11.6 **Delegated Authorities**

- *Approve amendments to existing operational banking facilities* - IRRELEVANT
- *Approve new operational banking facilities* - IRRELEVANT
- *Approve opening of new bank account* - IRRELEVANT
- *Approve closure of bank account* - IRRELEVANT

POL00401626

12 Payments

12.1 Manual Payments

12.1.1 Signing mandates are managed by Treasury and must be in place with a bank for any account on which cheques or similar manual payment instructions (e.g. direct debit mandates) are issued.

12.1.2 Cheques or other manual payment instructions up to £50,000 may be signed by one signatory. Cheques or other manual payment instructions greater than £50,000 must be signed by two signatories.

12.1.3 It is the responsibility of the paying department to ensure that there is adequate segregation of duties with regard to the preparation of manual payment instructions and cheques and that written procedures governing the processing of payments are in place.

12.1.4 Cheque books should be kept in a secure place.

12.1.5 Paying-in books should also be kept in a secure place. To prevent credits being made to unauthorised accounts, only pre-printed paying-in slips should be used when paying in cheques.

12.1.6 **Delegated Authorities**

- *Sign manual payment instruction - < £50k* - **Any 1 member of Banking Authorisation Panel**
- *Sign manual payment instruction - > £50k* - **Any 2 members of Banking Authorisation Panel**

12.2 Computer-Generated Cheque Payments

12.2.1 There should be adequate physical security over the hardware and software used for the preparation of computer-generated cheques. Detailed records should be kept of cheque stationery utilised and any missing cheque numbers investigated. A monetary limit should be set for the maximum value of any computer-generated or machine-signed cheque.

12.3 Manually-Instructed Payments

12.3.1 Where any use is made of electronic payment systems via a bank, staff must ensure that adequate written control procedures exist to ensure that the bank will only respond to verified requests from authorised personnel, these include:

- the use of code words;
- answer-back arrangements with the bank calling back to an authorised signatory (other than an authorised signatory who has signed the request);
- requests by telephone for transfers to be supported by a written request, signed in accordance with the mandate, received by the bank prior to dispatch of funds;
- transfer requests should only be sent on company headed notepaper, or pre-printed forms unique to the Group.

12.3.2 Treasury must approve any proposal to start using an internet banking platform and undertake a detailed security review.

12.3.3 If a bank requests any Group employee to sign an indemnity giving protection to the bank in respect of payment instructions actioned by the bank, then this document must be forwarded to Treasury for review and approval prior to signature.

POL00401626

12.4 Electronic Transfers

12.4.1 Electronic Funds Transfer (BACS/CHAPS/Faster Payments) is the preferred means of payment. Where internet banking systems are used to make such payments, care must be taken to ensure that there is adequate physical security over the system to prevent unauthorised access. The networking of internet banking systems should be approved collectively by the Treasury and IT departments.

12.4.2 It is the responsibility of Treasury to ensure that there is adequate segregation of duties in relation to initiating, authorising and releasing payments.

12.4.3 The authorisation process must be fully documented. Non-compliance with the agreed authorisation procedures will be referred to the CFOO and ARC Committee and is considered a serious breach of control.

12.4.4 BACS limits will be negotiated with the bank by Treasury and will be communicated to the relevant business unit. Any request for an increase to a BACS limit must be made by Treasury.

12.4.5 Any recommendations by a bank providing an internet banking system with regard to the control environment surrounding that system must be adhered to in all respects.

12.4.6 Treasury must approve any proposal to start using internet banking systems or other host-to-host solutions to initiate payments and ensure that a security review has been undertaken if appropriate.

12.4.7 **Delegated Authorities**

- *Release payment from Internet Banking System - < £50k* - **Any 1 Payment Panel (Internet Banking System)**
- *Release payment from Internet Banking System - > £50k* - **Any 2 Payment Panel (Internet Banking System)**
- *Release payment from Treasury Management System / SAP* - **Various (see Appendix C)**

POL00401626

13 Guarantees and Indemnities / Group Support

13.1 POL Support for POMS

13.1.1 POL may be asked to provide a letter of comfort, a letter of awareness or a direct guarantee or indemnity to a third party to support the activity of POMS. Although a guarantee creates a contingent liability on POL it does not increase the overall liabilities of the Group. It is considered reasonable to meet such requests on behalf of a wholly-owned subsidiary such as POMS.

13.1.2 Requests of this type will be reviewed on a case-by-case basis and POL will also consider whether it is more appropriate to issue a letter of comfort or letter of awareness. Generally such a guarantee will not have a cost for POL. The authority to approve and sign a direct guarantee to a commercial third-party for the benefit of POMS is delegated to the CFOO.

13.1.3 For the avoidance of doubt 13.1 does not apply to guarantees provided by POL in favour of POMS in connection with the raising of third-party finance by POMS. All such guarantees must be considered by the Board.

13.1.4 **Delegated Authorities**

- *Approve and execute a direct guarantee or indemnity to a commercial third party for the benefit of POMS* - IRRELEVANT

13.1.5 As of 2018 POMS is the only wholly-owned subsidiary of POL. In the event that new subsidiaries are introduced into the Group structure then, provided such subsidiaries are wholly-owned, then 13.1 will also be applicable for guarantees or indemnities for the benefit of those subsidiaries.

13.2 Bank Guarantees

13.2.1 POL may provide a counter-guarantee to a bank to support a guarantee made by that bank to a third party (a "bank guarantee") on behalf of POL. Such a bank guarantee may be used to support financing provided by a third party or to support a commercial arrangement. Such an arrangement may create a contingent financial exposure for the Group.

13.2.2 *To Support Financing* - Where the bank guarantee is used to support a financing arrangement approval will be by the POL Board.

13.2.3 *To Support Commercial Activity* - Where the bank guarantee is being provided to support commercial activity the authority to approve and sign the guarantee to the bank is delegated to the CFOO.

13.2.4 **Delegated Authorities**

- *Approve bank guarantee to support financing arrangement* - **Board**
- *Approve bank guarantee to support commercial arrangement* - IRRELEVANT
- *Execute counter-guarantee to bank in support of commercial arrangement* - IRRELEVANT

13.3 Government Support for the Group

13.3.1 From time-to-time the Group may be asked to obtain a letter of comfort, a letter of awareness or a guarantee from Government to support its activities. Such arrangements do not create a contingent liability of the Group.

13.3.2 Requests will be considered on a case-by-case basis and will require POL Board approval.

POL00401626

14 Regulatory Obligations

14.2 European Market Infrastructure Regulation ("EMIR")

14.2.1 Effective from January 2018, as a result of the changes introduced by MiFID II, the Group's derivative activity is subject to the requirements of EMIR.

14.2.2 POL is classified as a Non-Financial Counterparty "-" (an "NFC –")

14.2.3 As an NFC – EMIR places certain obligations on POL, namely:

a) *Reporting Obligations* – POL must report its derivative contracts to a trade repository no later than the working day after execution.

b) *Risk Mitigation Techniques* – POL must: (i) confirm trades in a timely manner; (ii) have dispute resolution processes in place; and (iii) engage in portfolio reconciliation.

14.2.4 POL will delegate reporting to its counterparty in derivatives transactions and will only execute derivative transactions with counterparties with which it has the appropriate delegated trade reporting agreements in place.

14.2.5 All trades will be confirmed by the end of the second day after execution.

14.2.6 POL will have ISDA agreements in place with all derivative counterparties to ensure that dispute resolution and portfolio reconciliation processes are documented.

POL00401626

15 ISDA Master Agreements

15.2 POL enters into ISDA[2] Master Agreements with potential derivative counterparties. The ISDA is an industry-standard agreement which governs the relationship between derivative counterparties and each transaction entered into under the ISDA. The key provisions of the ISDA include terms relating to payment and delivery obligations, termination rights, the close-out netting of transactions on termination, and representation and warranties. When executing derivative transactions POL enters into confirmations pursuant to the ISDA, which contain the economic terms of each transaction.

15.3 POL will only enter into derivative transactions with counterparties with which it has an ISDA agreement in place. POL will ensure that ISDA agreements are broadly similar in all material respects across counterparties. It is policy to standardise ISDAs where possible.

15.4 Only Treasury can negotiate ISDAs on behalf of POL.

15.4 **Delegated Authorities**

- *Agree changes to an ISDA Schedule* - IRRELEVANT
- *Approve and execute ISDA agreement on behalf of POL* - IRRELEVANT

[2] *ISDA – International Swaps and Derivatives Association*

POL00401626

Section III - Governance and Reporting

16 Treasury Governance and Reporting

16.1 Governance

16.1.1 PO Treasury risks are governed through the following structures:

16.1.2 **POL Board:** Authority to approve policies and approval limits relating to treasury risk management resides with the Board. Treasury risk management includes but is not limited to the following: short-term liquidity management, long-term funding, counterparty risk management, foreign exchange exposure management and interest rate risk management. The Board will delegate authorities to facilitate the operation of treasury risk management and the daily operation of the Treasury function.

16.1.3 **ARC Committee**: Financial risk management policies and approval limits are recommended to the Board for approval by the ARC Committee.

16.1.4 **Treasury Committee:** Is part of the Operations Board and meets on a monthly basis to review the Treasury Report, review financial risks, report on headroom and working capital, and report on and recommend changes to policy to the ARC Committee as required. The Treasury Committee is composed of the CFOO, the POL FD, the HoTTI and Finance Director Financial Services. Other members of the Operations Board may attend from time-to-time.

16.1.5 **FX Currency Hedging Committee**: Meets monthly or more frequently as required from time-to-time to confirm the value of hedges and timescales of hedges in accordance with the FX risk management policy. The committee is composed of: the Managing Director Post Office Money; the Finance Director Financial Services and Telecoms; and the Head of Travel.

16.1.6 The Board has delegated the following specific authorities to the IRRELEVANT

IRRELEVANT

- Approval of investment instrument limits
- Approval of counterparty selection criteria
- Approval of counterparties
- Approval of counterparty limits

- Approval of counterparties
- Approval of counterparty limits (within approved investment instrument limits)

16.1.7 The daily operation of treasury activity is delegated to the panels as shown on Appendix D. In all cases members of these panels will be appointed by the Treasury Committee.

16.1.8 Authority levels for write-offs are shown in Appendix F.

16.2 Treasury Management Reporting

16.2.1 The Treasury Report will be produced on a monthly basis. The contents of the report will include analysis of: note and coin inventory and how it is funded; insurance limits in cash centres; network cash holdings and inward rems; a monthly forecast update, including variance analysis for the prior period; Facility Headroom and Security Headroom; balances held in bank accounts; the net NRF Cap position; fx gains and losses; exposures to interest rate risks; treasury controls; as well as a summary of any project work currently being undertaken by Treasury.

16.2.2 The Treasury Committee will meet on a monthly basis as part of the Operations Board. It will review the Treasury Report and consider any other treasury risk management issues as required and make recommendations to the ARC.

16.2.3 Policy breaches will be immediately reported to the CFOO.

POL00401626

16.2.4 Treasury KPIs will be reviewed regularly.

16.2.5 Authorities to drawdown under established facilities are laid out in Appendix E.

16.2.6 An additional authority matrix is shown in Appendix F that relates to various items which arise during the normal course of business and for which individual write-off authorities are required. Examples of such items, which will normally be provided for, include:

- ATM cash trapping and retract fraud;
- Travelers' Cheque fraud;
- Camelot scratch cards failures in stock control due to master data errors.

Alisdair Cameron
March 2018

POL00401626

Appendix A: Summary of Counterparty Relationships, Services & Exposures

IRRELEVANT

POL00401626

Appendix B: CHAPS Banks

Bank of America (N.A)

Bank of England

Bank of Scotland (HBOS)

Barclays Bank PLC

Citibank N.A

CLS Bank International

Clydesdale Bank PLC

The Co-operative Bank PLC

Danske Bank

Deutsche Bank A.G

HSBC Limited

J.P. Morgan Chase Bank

Lloyds TSB Bank PLC

National Westminster Bank PLC

The Royal Bank of Scotland PLC

Santander UK PLC

Standard Chartered

State Street Bank

UBS A.G.

POL00401626

Appendix C: Delegated Authorities for Authorisation Panels

	Authorisation Panel	Delegated Authorities	Current Composition
Investment of Surplus Cash	Treasury Authorisation Panel	Approve investment of surplus cash balances - within policy Approve drawdowns - under existing credit facilities (up to 1 day)	Matrix securely maintained centrally by Treasury
	Dealing Panel	Propose investment of surplus cash balances Propose drawdowns - under credit existing facilities	Matrix securely maintained centrally by Treasury
Manual Payments	Banking Authorisation Panel *	Sign manual payment instruction (1) - < £50k - any 1 Banking Authorisation Panel member - > £50k - any 2 Banking Authorisation Panel members	Matrix securely maintained centrally by Treasury
Electronic Transfers	Payment Panel - (Internet Banking Systems) *	Release payment from internet banking system (2) - < £50k - any 1 Payment Panel (Internet Banking System) member - > £50k - any 2 Payment Panel (Internet Banking System) members	Matrix securely maintained centrally by Treasury
	Payment Panel - (Treasury Management System) ** *[BEIS Facility, NRF and file gateway payments]*	Release payment from TMS (2) - any 1 Treasury check AND - any 1 Banking Authorisation Panel OR Payment Panel member	Matrix securely maintained centrally by Treasury
	Payment Panel - (SAP) ** *[release of BACS payments]*	Release payment from SAP (2) - any 1 Amalgamated payment proposal AND - any 1 payment authoriser	Matrix securely maintained centrally by Treasury

(1) Cheques and direct debit instructions to bank - Banking Authorisation Panel members in accordance with mandates held by banks
(2) Aligned to authorisation rights in Internet Banking Systems / Treasury Management System / SAP

* *In respect of both the Banking Authorisation Panel and the various Payment Panels the lists are extensive and complex owing to the number of bank accounts used within the Group. The full listings are therefore not replicated here but are maintained and held securely by Treasury.*

** *In respect of the Treasury Management Systems and SAP, the controls around changes to master data (bank details), in particular around segregation of duties, are deemed to be strong enough that a two stage authorisation is not needed.*

POL00401626

Appendix D: Delegated Authorities for Drawdowns Under Credit Facilities

1. Approval of Drawdowns under BEIS Facility

Drawdown Amount	< £950m	< £950m	< £950m
Period of Drawdown	Up to 1 day	Over 1 day and up to 12 mths	over 12 mths
Delegated Authority	*1 member from Treasury Authorisation Panel*	**IRRELEVANT**	

2. Approval of Drawdowns Under Other External Borrowings

Drawdown Amount	< £50m	< £50m	< £50m	< £50m
Period of Drawdown	Overnight	Up to 1 wk	up to 6 mths	over 6 mths
Delegated Authority	*1 member from Treasury Authorisation Panel*	**IRRELEVANT**		

3. Leasing and Contract Hire

Amount	< £50m	< £50m
Maturity	Up to 8 years	Over 8 years
Delegated Authority	**IRRELEVANT**	**IRRELEVANT**

POL00401626

Appendix E: Individual Write-off Authority Levels

Authorities to write off provided-for items relating to external fraud and data errors:

Amount	< £1k	£1k to £10k	£10k to £100k	> £100k
Delegated Authority	**IRRELEVANT**			

POL00401626

Appendix F: Summary of Delegated Authorities

Separate attachment.

POL00401626

POST OFFICE LIMITED - Treasury Risk Management Framework, Policies and Authorities
Appendix F - Summary of Delegated Authorities - from March 2018

	Reserved Matter	Ref.	Notes	Shareholder Consent	POL Board	Audit, Risk & Compl. Comm.	Treasury Comm.	FX Currency Hedging Comm.	CFOO	POL FD	Head of Treasury, Tax & Insuranc	Treasury Manager	Authorisation Panels: Treasury Authorisation Panel	Authorisation Panels: Dealing Panel	Payment Panels: Banking Auth. Panel	Payment Panels: Internet Banking Systems	Payment Panels: Treasury Mgt. System	Payment Panels: SAP
GENERAL	**General**																	
	Approve treasury risk management framework, policies and authorities	2.7	Must be			√												
	Approve amendments to or derogations from treasury risk management framework, policies and authorities (1)	2.7	Must be			√												
3. SHORT-TERM CASH AND LIQUIDITY MANAGEMENT	**Bank Account Structures**																	
	Approve addition of bank account to existing pooling arrangement	3.4.2	Any 1 from						√	√	√							
	Approve removal of bank account from existing pooling arrangement	3.4.2	Any 1 from						√	√	√							
	Approve creation of new pooling arrangement	3.4.2	Any 1 from						√	√								
	Committed Short-term Funding																	
	Approve change to Investment Reserve																	
	- in the range nil to £20m / for up to 2 weeks	3.6.8	Any 1 from						√	√	√							
	- up to £50m / for more than 2 weeks	3.6.8	Must be						√									
	Propose drawdown - under existing credit facilities	3.6.8	Any 1 from											√				
	Approve drawdown - under BEIS Facility																	
	- up to 1 day	3.6.8	Any 1 from						√	√	√		√					
	- over 1 day and up to 12 months	3.6.8	Any 1 from						√	√								
	- over 12 months	3.6.8	Must be						√									
	Approve drawdown - under Other External Borrowings (up to £50m)																	
	- overnight	3.6.8	Any 1 from						√	√	√		√					
	- up to 1 week	3.6.8	Any 1 from						√	√	√							
	- up to 6 months	3.6.8	Any 1 from						√	√								
	- over 6 months	3.6.8	Must be						√									
	Short-term Cash & Liquidity Arrangements with POMS																	
	Approve margin on intra-group loans to/from POMS on behalf of POL	3.7.8	Must be both						√		√							
	Execute documentation for intra-group loans to/from POMS on behalf of POL																	
	- up to £50m and up to 3 months	3.7.8	Must be						√									
	- over £50m or over 3 months	3.7.8	Must be		√													
4. MEDIUM AND LONG-TERM FUNDING MANAGEMENT	**Headroom**																	
	Approve amendment to Facility Headroom Buffer	4.8.4	Must be		√													
	Borrowing Policy																	
	Approve new medium and long-term funding	4.9.4	Must be both	√	√													
5. COUNTERPARTY CREDIT RISK MANAGEMENT	**Counterparty Credit Risk Management**																	
	Approve new financial institution counterparty	5.11	Must be			√												
	Approve financial institution counterparty limit	5.11	Must be			√												
	Approve temporary increase to financial institution counterparty limit	5.11	Must be						√									
6. INVESTMENT RISK MANAGEMENT	**Investment Risk Management**																	
	Approve new investment counterparty - within approved credit rating bands	6.14	Any 1 from						√	√								
	Approve changes to credit rating bands for counterparties	6.14	Must be			√												
	Approve temporary increase to investment counterparty deposit limit	6.14	Must be						√									
	Approve new permitted investment instrument	6.14	Must be						√									
	Propose investment of surplus cash balances	6.14	Any 1 from											√				
	Approve investment of surplus cash balances																	
	- Amount - < £300m / Term - up to 1 month	6.14	Any 1 from						√	√	√		√					
	- Amount - < £100m / Term - up to 3 months	6.14	Any 1 from						√	√	√		√					
	- Amount - < £50m / Term - up to 6 months	6.14	Any 1 from						√	√	√		√					
	- Amount - < £300m / Term - up to 1 year	6.14	Any 1 from						√	√								
	- Amount - < £50m / Term - up to 1 year	6.14	Must be both *		√				√									
	- Amount - < £50m / Term - up to 1 year	6.14	Must be		√													
7. FOREIGN EXCHANGE EXPOSURE MANAGEMENT	**Foreign Exchange Exposure Management**																	
	Execute FX hedge trades, within policy, in accordance with instructions issued by FX Committee	7.10	Any 1 from											√				
	Approve new permitted FX hedging instrument	7.10	Must be						√									
	Approve FX hedge trades for exposures not created by currency note inventory holdings																	
	- up to £50m	7.10	Must be						√									
	- above £50m	7.10	Must be		√													
8. INTEREST RATE EXPOSURE MANAGEMENT	**Interest Rate Exposure Management**																	
	Approve new permitted interest rate hedging instrument	8.9	Must be			√												
	Approve execution of interest rate hedging strategy	8.9	Must be		√													
9. BANK RELATIONSHIP MANAGEMENT	**Bank Relationship Management**																	
	Approve entering into relationship with new bank	9.9	Must be				√											
	Approve entering into relationship with new bank - prior to Treasury Committee approval	9.9	Must be						√									
	Approve entering into NDA with bank	9.9	Must be						√									
10. COMMODITY PRICE EXPOSURE MANAGEMENT	**Commodity Price Exposure Management**																	
	Execute commodity price hedges within policy	10.7	Must be											√				

Data: Confidential

Last Edit: 02/03/2018 10:02
Prepared By: Mark DIXON
F_Delegated Authorities_03.2018 Final.xlsx

POL00401626

POST OFFICE LIMITED - Treasury Risk Management Framework, Policies and Authorities
Appendix F - Summary of Delegated Authorities - from March 2018

	Reserved Matter	Ref.	Notes	Shareholder Consent	POL Board	Audit, Risk & Compl. Comm.	Treasury Comm.	FX Currency Hedging Comm.	CFOO	POL FD	Head of Treasury, Tax & Insuranc	Treasury Manager	Authorisation Panels: Treasury Authorisation Panel	Dealing Panel	Payment Panels: Banking Auth. Panel	Internet Banking Systems	Treasury Mgt. System	SAP
	Approve new commodity price hedge counterparty	10.7	Must be						√									
	Approve execution of commodity price hedges within policy	10.7	Any 1 from						√	√	√							
OTHER	**Operational Banking**																	
	Approve amendments to existing operational banking facilities (2)	11.6	Any 1 from						√									
	Approve new operational banking facilities (2)	11.6	Any 1 from						√									
	Approve opening of new bank account	11.6	Must be						√	√	√							
	Approve closure of bank account	11.6	Must be						√	√	√							
	Payments																	
	Sign manual payment instruction - < £50k	12.1.6	Must be 1 from												√			
	Sign manual payment instruction - < £50k	12.1.6	Must be 2 from												√			
	Release payment from Internet Banking System - < £50k	12.4.7	Must be 1 from													√		
	Release payment from Internet Banking System - > £50k	12.4.7	Must be 2 from													√		
	Release payment from Treasury Management System	12.4.7	Must be Treasury check and 1 from												√			
	Release payment from SAP	12.4.7	Must be 1 from															√
	Guarantees / Group Support																	
	Approve and execute a direct guarantee to a commercial third party for the benefit of POMS	13.1.4	Must be						√									
	Approve bank guarantee to support financing arrangement	13.2.4	Must be		√													
	Approve bank guarantee to support commercial arrangement	13.2.4	Must be						√									
	Execute counter-guarantee to bank in support of commercial arrangement	13.2.4	Must be						√									
	ISDA Master Agreements																	
	Agree changes to an ISDA Schedule	15.4	Any 1 from						√	√	√							
	Approve and execute ISDA agreement on behalf of POL	15.4	Must be						√									

** Must be CFOO and one other POL Board member*

(1) unless specifically stated as the Board (2) including overdrafts, fax lines, BACS limits, intra-day limits and similar arrangements

Data: Confidential

Last Edit: 02/03/2018 10:02
Prepared By: Mark DIXON
F_Delegated Authorities_03.2018 Final.xlsx

POL00401626

Document Retention and Disposal Policy

Author: Jules Harris Sponsor: Jane MacLeod Meeting Date: 13 Mar 2018

Executive Summary

Context

1. Post Office is subject to a number of legal and regulatory requirements regarding the retention and disposal of different types of data and documents. These include requirements under the Companies Act relating to statutory and financial records, the Financial Services and Markets Act relating to customers with regulated products, Telecoms in relation to Privacy and Electronic Communications (PECR), in relation to customers who have bought telephony products, as well under data protection legislation relating to documents which contain personal data.
2. Accordingly, Post Office needs to update its processes to ensure compliance. The draft Document Retention and Disposal Policy sets out the framework for compliance, and this paper sets out the steps to be taken to progressively implement the policy.

Questions addressed in this paper

- Why the policy is needed and what is incorporated
- Stakeholder inclusion in developing the policy
- How we will implement the policy
- How we will communicate the policy to staff
- Impact of delaying approval

Conclusion

3. The ***Document Retention and Disposal Policy*** has been created to:
   - Satisfy the requirements of the relevant legislation to ensure that information and documents which are subject to specific legal and regulatory requirements can be identified, retained for the correct periods, and then destroyed or disposed of;
   - Direct employees to useful resources via 'links' to provide support; and
   - provide advice to assist employees, and data owners and Departmental Data Stewards to make the right decisions;
4. A sub-project will be established as part of the GDPR programme to aid the business to identify relevant categories of information and documents, and ensure that there are proportionate processes in place to manage compliance.

POL00401626

Input Sought

The RCC is asked to approve the Document Retention and Disposal Policy, and the intended implementation plan.

POL00401626

The Report

Why the policy is needed, and what is incorporated

5. Both Post Office Limited and Post Office Management Services Limited ('POMS') are subject to the requirements of the Companies Act, various tax legislation and similar legal and regulatory requirements that require information and stated documents to be retained for a minimum period. Additionally certain types of products sold by both Post Office Limited and POMS are subject to specific regulatory requirements setting out minimum retention periods for documents and certain types of information.
6. Proportionate and appropriate document/data retention policies will assist Post Office and POMS to manage legal risk arising from excessive retention periods, as well as to minimise storage costs of documents, information and data that is no longer required to be held. It appears that a similar policy was approved within Royal Mail/Post Office in about 2011 however this is no longer embedded in business practices.
7. It is good business practice to determine what documents (both physical and electronic) are created in the ordinary course of business, and set guidelines as to how they will be used and stored, how long they will be retained for and in what format, and when and how they will destroyed/deleted. These practices aid compliance with applicable laws and regulations, reduce the risk of information and documents being unnecessarily retained, and reduces the likelihood of data breach, or other information security incident, as colleagues are clear about the sensitivity of any documents they access as part of their day to day business.
8. The risk appetite in relation to not complying with law and regulations or deviation from its business conduct standards, is Averse. In the absence of effective policies and procedures to manage this risk, we are therefore outside risk appetite, and this will become increasingly relevant – specifically in relation to personal data - once GDPR comes into force in May 2018. We therefore propose to establish a work stream within the GDPR programme to work with both Post Office and POMS to identify relevant legal and regulatory requirements, determine the categories of information and documents to which those requirements apply, and develop proportionate retention schedules, procedures and storage practices, as well as enhance awareness across the business of the need to understand and embed document management and storage protocols.
9. The policy contains a set of definitions which are aligned with the Data Management approach, and will be widely used within Post Office in the future.
10. Once created, these processes will be embedded into the change process.
11. The programme will also consider whether data retention requirements should be incorporated into contracts with our third party suppliers.

POL00401626

Stakeholder inclusion in developing the policies

12. The policies have been developed by Information Protection and Assurance (IPA), Head of MI, Analytics & Data Strategy, IT Security; in conjunction with Legal, Risk and Governance, and the Data Protection Officer.

How will we implement the policy?

13. The implementation of this policy will be undertaken by a separate workstream within the GDPR programme.
14. Funding proposals to be brought through the Change governance processes for funding in 2018-19 will include the cost of a small team to design the implementation plan, provide advice and guidance to the business in developing the required retention schedules. Priority will be given to documents and information relating to regulated products (e.g. within POMS and the wider FS & T business unit) as well as personal data held in relation to employees and agents.
15. The creation of Departmental Data Stewards is part of the Data Management programme being run by the Head of MI, Analytics & Data Strategy.
16. Many of the minimum control standards at 2.3 within the policy are dependent on the creation of Data Owners, and their acceptance of their responsibilities. The Head of MI, Analytics and Data Management and Head of Information Protection and Assurance are presenting to GE on this subject in April. Appropriate training for key roles will be developed and delivered. IPA will raise a risk exception to address the current risks. Nevertheless it is important for GDPR compliance.
17. Embedding the policy will be a significant exercise in order to bring Post Office within risk appetite. Post Office need to have the policy in place before GDPR implementation.

How will we communicate the policy to staff?

18. The mini project will:
    - Develop generic guidelines to support all staff in the interim pending roll out to specific areas, and these will be communicated via a 'One' Communication update on the Post Office Intranet;
    - update the policies on the SharePoint site for staff reference;
    - communicate the existence of the new policies in the all-staff Monthly Information Security Update publication;
    - create the area on SharePoint to store the retention schedules (and we will look at ways of creating and storing these schedules digitally rather than through Word or Excel schedules) ;
    - aid Company Secretariat in creation of relevant processes and procedures to maintain the SharePoint site, and
    - Provide targeted training and support to each business area as the protocols are rolled out.

POL00401626

Impact of delaying approval

19. Post Office is already outside its stated risk appetite for regulatory risk. Failure to address these issues could not only have financial implications in the event of regulatory involvement, however it also means that Post Office cannot take advantage of potential cost savings which should arise as a result of a more rigorous approach to deletion/destruction of documents and data at the end of retention periods.
20. Post Office also has contractual and certification requirements to have up-to-date policies and to review them annually. Further delay to the adoption of this policy could lead to issues in retaining our certifications, for example our ISO27001 Certification.

POL00401626



DRAFT

GROUP POLICIES

Document Retention and Disposal Policy

Version – V0.1

POL00401626

1. Overview 3
1.1. Introduction by the Policy Owner 3
1.2. Purpose 3
1.3. Core Principles 3
1.4. Application 4
1.5. Definitions 4
1.6. Legislation 5
1.7. Industry Guidance 5
2. Risk Appetite and Minimum Control Standards 6
2.1. Risk Appetite 6
2.2. Policy Framework 6
2.3. Minimum Control Standards 7
3. Tools – Retention Schedules 13
3.1. Functional Retention Schedules 13
4. Where to go for help 15
4.1. Additional Policies 15
4.2. How to raise a concern 15
4.3. Who to contact for more information 15
4.4. How to request an exception 15
Appendix A – Legislation details 16
Appendix B – Example Retention Schedule 18
5. Control 19
5.1. Policy Version 19
5.2. Policy Approval 19
4.3. Who to contact for more information ..... **Error! Bookmark not defined.**
5. Control ..... **Error! Bookmark not defined.**
5.1. Policy Version ..... **Error! Bookmark not defined.**

DRAFT

POL00401626

1. Overview

1.1. Introduction by the Policy Owner

This policy sets out Post Office's[1] commitment to the proper and lawful retention and disposal of its information assets. Information held for longer than is necessary carries additional risk and cost. Conversely, information not kept for long enough leaves Post Office vulnerable to knowledge or evidence gaps and sanctions from some of our regulators. Post Office recognises that failure to follow these principles will negatively impact business efficiency, and the ability to protect its interests as well as those of its customers and stakeholders.

1.2. Purpose

The Document Retention and Disposal Policy is a cornerstone for good information management in Post Office. Information management supports the delivery of Post Office services in an efficient and accountable manner, helping to maintain its position as a trusted provider, retaining information for operational use while ensuring adherence to the laws and regulations concerning them. The objective of this policy is to keep important information for future use or reference, to organize information so it can be searched and accessed at a later date and to dispose of information that is no longer needed. Retention and disposal requirements are mandated by a number of pieces of legislation and regulation to which Post Office is subject to.

This policy defines a set of high level principles to manage the retention and disposal of Post Office's information assets in a timely and secure manner according to business needs and legal and regulatory requirements.

All employees[2] have a responsibility to understand the requirements set out in this policy and seek clarification from their line manager or the Departmental Data Steward in the case of any uncertainty. A list of Data Owners and Departmental Data Stewards will be maintained on the Data Management area of the intranet and will be updated when staff change, or new ones are added. The address for the Data Management Site is:
https://poluk.sharepoint.com/sites/Extranet/FandO/DG/Data%20Glossary%20Wiki/Home.aspx

1.3. Core Principles

Compliance with this policy will assist in meeting the following principles:

Protection – Information that is needed to minimise the risk to Post Office from investigations, litigation or disputes will be easier to locate and will be retained systematically.

---

[1] [1]In this Policy "Post Office" and "Group" mean Post Office Limited and Post Office Management Services Limited.

[2] In this policy employee means employees permanent employees, temporary including agency employees, contractors, consultants and anyone else working on behalf of Post Office.

POL00401626

Employees will have clear guidelines for the secure disposal of information, protecting against misuse and data breaches.

Information that contributes to the Post Office's story in society will be protected, supporting corporate memory and brand identity through heritage.

Compliance – Post Office is subject to many laws and regulations which have information retention requirements. Compliance with these requirements will significantly reduce the risk of financial penalties, prosecution or reputational damage.

Accountability – Properly managed retention and disposal of information will allow Post Office to defend its actions by evidencing document destruction. Retention schedules and destruction/transfer documentation will underpin auditable disposal processes. In particular, this will support compliance with the Freedom of Information Act and the Data Protection Act as updated by GDPR and DPA 2018.

Efficiency – Timely disposal of information will lead to financial savings for document storage, as well as day to day efficiency savings when retrieving information.

1.4. Application

This policy applies to employees and, where applicable, Third Party Supply Chain.

1.5. Definitions

Information

'Information' is defined as a collection of data in the form of documents or other artefacts (such as spreadsheets, flow diagrams or reports) on which the business makes decisions.

Data

'Data' is defined as the elements that form part of systems and processes that are created or pass through our systems.

Documents

'Documents' are specifically a type of information which has been used to form the basis of decisions, or to support business processes, in the normal day to day running of Post Office.

Information assets

'Information assets' are collectively all of the above.

Departmental Data Steward

'Departmental Data Steward' is the person allocated by a Data Owner to undertake the day to day processes associated with the controls required by the Data Owner

Data Owner

'Data Owner' is the person (usually GE or GE-1) who is accountable for a data entity (or multiple data entities)

Data Entity

DRAFT

POL00401626

'Data Entity' is the term used to describe a concept in a data repository that is a container of data & relationships to other objects – such as Branch, Customer, Employee, Product etc.

Third Party Supply Chain

'Third Party Supply chain' refers to the organisations who provide services holding, storing or processing Post Office Information Assets.

Structured and Unstructured Data

'Structured Data' has pre-defined data models or schema within a database or system file. 'Unstructured Data' consist all those that do not have pre-defined data models or schemas thus can't be so readily classified and fit into a neat box. Unstructured data files often include text and multimedia content: photos and graphic images, videos, webpages, PDF files, PowerPoint presentations, emails, blog entries, wikis and word processing documents.

Document Retention Schedule

'Document Retention Schedule' is the document detailing the various requirements of the data owner in regard to documents under their sphere of control. An example of one is shown at Appendix B

1.6. Legislation

The following non-exhaustive list of legislation concerning the creation, management, disposal, use and re-use of documents and information is applicable to Post Office (a more extensive, but not definitive, list is available in Appendix):

- Postal Services Act 2000
- Data Protection Act (1998) [General Data Protection Regulations (Regulation (EU) 2016/679)]
- Freedom of Information Act (2000)
- Companies Acts (1985, 2004, 2006)
- Limitation Act (1980)
- Public Records Acts (1958, 1967)
- Financial Services and Markets Act (2000)

1.7. Industry Guidance

This policy is based on the international standard for records management, ISO 15489 and the Code of Practice on the management of records under Section 46 of the Freedom of Information Act 2000.

DRAFT

POL00401626

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

A Risk Appetite is the extent to which the group will accept that a risk might happen in pursuit of day to day business transactions. It therefore defines the boundaries of activity and levels of exposure that the group are willing and able to tolerate.

The Group takes its legal and regulatory responsibilities seriously and consequently has:

- **Averse** risk appetite in relation to not complying with law and regulations or deviation from its business conduct standards, of which this standard forms part
- **Averse** risk appetite in relation to any serious impact to the confidentiality, integrity and availability of information, leading to financial loss, business disruption, public embarrassment or legal consequences in line with risk impacts
- **Tolerant** risk appetite for legal and regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality
- **Averse** risk appetite for litigation in relation to high profile cases/ issues
- **Averse** risk appetite for data loss/ leakage that can lead to customer, commercial or reputational damage
- **Averse** risk appetite for inaccurate and unreliable processing of data
- **Averse** risk appetite for inefficient or ineffective or prolonged failure of, governance and control processes, critical financial reporting processes, critical supply chain and business continuity processes.

2.2. Policy Framework

This policy forms part of the Information Protection and Assurance (IPA) and IT Security Policy Set which is located here:

https://poluk.sharepoint.com/sites/postoffice/inside/Pages/Information-security.aspx

DRAFT

POL00401626

2.3. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

At Document/System Creation

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Product or service entity	Systems may not adequately support implementation of retention schedules and timely destruction of data. It may not be technically possible to permanently delete data or it may require a manual process.	As part of the design of a new product or service, or where a product or service is being updated, product or service risks must be considered, mitigated and documented before completion of design phase. This must include updating of any related Document Retention Schedules. The integrity and accuracy of data must be ensured at the point of collection.	Product manager Product manager/Data Owner	During design phase/ annually/ anytime there is a change During design phase/ annually/ anytime there is a change
Data Flows	Systems further down the process chain may not understand or implement the correct retention schedules.	As part of the design of projects or implementation of systems like new products or services, or where a product or service is being updated, product or service risks must be considered, mitigated and documented before completion of design phase. Understand what entities are within the system for which they are Data Owner and	Product Manager Data Owner	During design phase/ annually/ anytime there is a change Ongoing

POL00401626

		how these flow to other system or product entities. Ensure Departmental Data Stewards and Line Managers understand the full implications of implementing change within the systems for which they are designated Data Owner.	Data Owner/Departmental Data Steward	As part of sign-off of new or updated product sets.
Retention Schedules	Lack of creation or updating of retention schedules means that colleagues may not be aware of their obligations leading to inappropriate usage or retention of documents. This can cause Post Office to be fined or suffer reputational damage.	All Data Owners and Line Managers must ensure that the retention schedules for their area are up to date. This is especially important when changes are being implemented to business processes.	Data Owner/Line Manager	Ongoing

During Use of a document or system

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Risks to Information	Lack of understanding of the importance or sensitivity of the information flowing through a department could mean that employees do not perform the required actions on it.	Data Owners must ensure that all employees who view or process the information within their sphere of control understand the importance of that data.	Data Owners	Every 6 months in the Director assertions.
		Data Owners need to understand the designs of systems or products such that they can fully understand the scope of their entity. Data Owners may pass this to Departmental Data Stewards, but they retain accountability.	Data Owners	Ongoing
		Data Owners must ensure evidence of any decisions are retained.	Data Owners	Ongoing
		Data Owners must understand the complete information lifecycle (creation, capture, index, manage, access, retrieve, administer, repurpose, share, retain, dispose, preserve) for all data within their sphere of control.	Data Owners	Ongoing

POL00401626

Information Security	Inadequate access controls may lead to unauthorised deletion of information including sensitive or business critical information.	Line Managers must assess and assure risks relating to employee access to systems and files, especially those containing sensitive or business critical data. Data Owners must ensure that extra training on information security and data protection is provided to their Departmental Data Stewards.	Line Managers/ IT Data Owners	Ongoing Annually
Personal Data	Due to inadequate training, there is a risk of unintentional misuse of Personal Data, resulting in punitive penalties, reputational damage and a loss of licence to process personal data.	Data Owners must ensure all employees within their areas understand their responsibilities in regard to the protection of personal data. IPA must ensure that suitable training is made available to Data Owners and employees.	Data Owners IPA	Ongoing Annually
Employees	Due to inadequate training, there is a risk of under, or over, retention of information and failure to follow retention schedules, leading to punitive penalties or reputational damage.	All employees must undertake the annual Information Security and Data Protection training. They must also read and understand the Acceptable Use Policy, the Information Classification Standard and this document. 3rd party suppliers must ensure that all employees with access to Post Office data and information undertake Post Office agreed information management training. Ensure annual training contains adequate information on information management Ensure the IPA and IT Security Policy Set contains adequate information on Information management.	All employees 3rd party suppliers IPA IPA & IT Security	Annually/ within 3 weeks of starting Annually/ within 3 weeks of starting Annually Annually
Document Management	Failure to keep information evidencing appropriate destruction will increase time spent handling public access requests and will fail to protect Post Office in disputes around	Data Owners must ensure that they have defined the storage requirements for the data under their sphere of control, and that this has been documented and agreed. This particularly applies where encryption is	Data Owners	Annually/when a change occurs

DRAFT

POL00401626

	information rights regulations (such as Freedom of Information Act and Data Protection Act).	required. This is a field within the retention schedule.		
Retention Schedules	Lack of communication of required retention schedules may mean that incorrect decisions are made by employees regarding information which could lead to regulatory fines or inability to answer a request to find or correct data.	Data Owners must ensure that correct retention schedules are in place for the systems or product entities within their sphere of control. These are required to be created at project initiation. Line managers must ensure that they and all their employees are aware of the retention schedules in place for the data/information they process. Line Managers s must remain aware of relevant regulatory and legislative requirements for document retention and must regularly review and update retention schedules in line with these as well as functional changes to their area.	Data Owners Line Managers Line Managers	Annually/ when a need is identified Annually/ when a need is identified Annually/ when a need is identified
Incident Management	Failure to understand the implications of an incident can lead to poor decision making or regulatory sanctions	Data Owners must ensure that they are aware of any incidents to their data, and are satisfied with the resolutions	Data Owners	During an incident
Processes and Procedures	Incorrect processes and procedures can lead to employees incorrectly using data.	Data Owners / Departmental Data Stewards are responsible for ensuring all processes which access the information within their sphere of control are adequate and appropriate.	Data Owners & Departmental Data Stewards	Annually / when a new process or procedure is written
Governance	Lack of governance over documents could lead to incorrect usage of data and thus result in fines or reputational damage to Post Office.	All employees implementing document management practices consistent with this Policy. Preserving documents as required under this Policy. Properly disposing of information at the end of its retention period. Monitoring compliance with this Policy.	All employees All employees All employees	Ongoing Ongoing Ongoing

POL00401626

		Educating employees in document management practices. Maintaining the repository of retention schedules.	Head of MI, Analytics and Data Strategy IPA Company Secretariat	Ongoing Annually Ongoing
Legal/ Regulatory Framework	Failure to understand the requirements of any legal or regulatory issues by the Data Owner may lead to Post Office receiving sanctions where documents or entities have not been controlled appropriately	Ensure when creating their Document Retention Schedules all regulatory or legal requirements have been considered.	Data Owners	Annually

During Document/System Disposal

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Risks to Information	Incorrectly disposing of information could mean that, through lack of continued controls being implemented for a defunct system/document, Post Office may suffer a data breach.	Data Owners must ensure that they enforce the clauses within a contract at the end of its term. Data Owners must ensure that all users of the entities or documents under their sphere of control understand what actions are to be taken at the end of a retention period. All employees must ensure they understand what needs to be done with a document or system at the end of its retention period.	Data Owners Data Owners All Employees	When a contract closes Ongoing Ongoing
Document Management	Failure to keep information evidencing appropriate destruction will increase time spent handling public access requests and will fail to protect Post Office in disputes around information rights regulations (such as Freedom of Information Act and Data Protection Act).	The Destruction or transfer of information must be authorised by the Data Owner or Departmental Data Steward and documented so that an audit trail exists.	All employees/Data Owners/ Departmental Data Steward	Ongoing

POL00401626

DRAFT

POL00401626

3. Tools – Retention Schedules

Retention schedules will ensure that retention of information is considered prior to its creation. Some record types can be identified as having definite long-term business or historical value due to the activities they arise from. For others, their value may change over time, or an event (such as an audit or legal action) may require that their scheduled disposal is put on hold. All disposal of information must therefore be approved by the Data Owner before it is actioned and records must be reviewed where this is necessary to make a decision.

Disposal of information at the end of its assigned retention period means either destruction or transfer. Destruction of information must follow Post Office procedures as defined by the Data Owner / Departmental Data Steward in order to prevent a data breach (procedures apply to destruction of hard copy documents, electronic information and hardware). Where documents have been identified as suitable for transfer to The Postal Museum archive Departmental Data Stewards must ensure they comply. This should not be confused with transfer of semi-current or inactive documents to off-site storage facilities. Documents at the end of their retention period must not be transferred to off-site storage facilities unless they are subject to a hold on disposal.

Duplicate documents should be destroyed as soon as possible. Where information has been regularly shared between business units, only the original documents should be retained. Care should be taken that seemingly duplicate documents have not been annotated. Where Post Office shares information with other bodies, Post Office must ensure that they have adequate procedures in place so that the information is managed in accordance with the relevant legislation and regulatory guidance.

3.1. Functional Retention Schedules

Retention schedules set out the groups of documents that Post Office functions will maintain and when these are due for review, transfer to The Postal Museum or secure destruction.

Information on retention schedules will fall into three main categories:

1. Destroy after an agreed period – where the useful life of a group of documents can be easily pre-determined (for example, destroy 3 years after creation; destroy 6 years after the end of the financial year).

2. Automatically select for permanent preservation – where certain groups of documents can be readily defined as worthy of permanent preservation and transferred to The Postal Museum.

3. Review – examine documents to determine whether they should be destroyed, retained for a further period or transferred to The Postal Museum for permanent

POL00401626

preservation. Documents which fall under category 1 may need to be reviewed for potential legal hold if they pertain to an active case.

Retention periods and actions are based on informational value, evidential value, legal or regulatory requirements, and historical value.

DRAFT

POL00401626

4. Where to go for help

4.1. Additional Policies

This policy is one of a set of policies. The full set of IPA and IT Security policies can be found at:

https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx

The full set of Post Office Policies can be found at:

https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx

4.2. How to raise a concern

Any Post Office employee who suspects dishonest or fraudulent activity has a duty to:

- Discuss the matter fully with their Line Manager; or,
- Report their suspicions by telephoning Grapevine on GRO
- If either or both are not available, staff can contact the Post Office's General Counsel, who can be contacted by email at: whistleblowing GRO or by telephone on: GRO.
- Alternatively staff can use the Speak Up service available on GRO
- or via a secure on-line web portal: http://www.intouchfeedback.com/postoffice

Post Office encourages members of the public or people not employed by us who suspect [*activity in breach of policy*] to write, in confidence, to the **Chief Executive's Office, Finsbury Dials, 20 Finsbury St, London EC2 9AQ**.

4.3. Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact Information Protection and Assurance via ipa GRO or IT Security via ITSecurity GRO

4.4. How to request an exception

If there is anything within this policy that causes business impact, please contact IPA via ipa GRO and we will process an exception. Any exceptions are presented to the Information Security governance body for ratification.

POL00401626

Appendix A – Legislation details

Postal Services Act 2000

The Postal Services Act requires postal companies operating in the UK to be licensed. The Licence sets out quality standards and the rules by which licensees are permitted to operate. Postcomm has strong powers to investigate compliance and Licence Condition 17 obliges Post Office to furnish any information that the regulator requires to fulfil its function. Therefore, it is in Post Office's interest to retain and dispose of information systematically in order to provide evidence of compliance.

Data Protection Act (1998) [General Data Protection Regulations (Regulation (EU) 2016/679)]

The Data Protection Act governs how personal details must be handled and gives individuals rights over their personal information including access and processing. There is an explicit obligation under the Act that personal data processed for any purpose shall not be kept for longer than is necessary for that purpose. Therefore, documents containing personal data must always be allocated a retention period, and must never be held indefinitely.

The Law provides that, apart from any statutory and regulatory retention periods, employers should adopt a risk analysis approach to deciding the retention period appropriate for employee's personal information. Employee files should be reviewed on a regular basis to clear out irrelevant, excessive and/or out of date information. Once the employment relationship has ended, employers should destroy information which is no relevant.

Freedom of Information Act (2000)

The main purpose of the Freedom of Information Act (FOI) is to open the actions and decisions of Post Office up to legitimate public scrutiny. The Act gives anyone the right to ask for information, be told whether or not Post Office have it and, if so, to be given the information unless covered by a relevant exemption. It applies to all recorded information (including email correspondence) held by or on behalf of Post Office, regardless of when, where or why it was created.

FOI does not itself change the length of time that documents are kept. However, being able to demonstrate a clear and coherent document retention policy assists compliance, and the systematic and timely disposal of information is also important in preventing the release of confidential information.

The Freedom of Information Act extends the definition of personal data to include any unstructured personal information. Individuals, and sometimes third parties, may therefore have a right to see any data held about them irrespective of where it is stored.

Companies Acts (1985, 2004, 2006)

The Companies Act requires public companies to keep accounting details for a minimum of 6 years from the date they were made. The Act also requires companies to keep statutory registers (e.g. of Directors' interests) and to file statutory returns at Companies House.

The Companies (Audit, Investigations and Community Enterprise) Act 2004 requires that documents relating to transactions and accounting practices is auditable, and permits auditors and the Secretary of State to request company information from any employee.

DRAFT

POL00401626

Limitation Act (1980)

The Limitation Act sets out the time periods within which various kinds of legal proceedings must be brought. The risk of claims and their limitation period must be taken into account when deciding how long documents should be kept.

Public Records Acts (1958, 1967)

Post Office is subject to obligations under the Public Records Acts (PRA) which require public bodies to select documents of historical interest for permanent preservation. Under PRA, documents of historical value must be identified and transferred to The Postal Museum archive for permanent retention no later than 20 years after they were created.

Financial Services and Markets Act (2000)

The key statute that regulates the financial services industry in the UK

DRAFT

POL00401626

Appendix B – Example Retention Schedule

Retention Schedules should be stored in the Data Retention Schedule area as a spreadsheet. The example below is a small portion of the Company Secretariat one to show fields and suggested usage.

	Record Category	Record Type	Local Record Name	Record Format	Record Location	Retention Period	Authority	Information Asset Owner	Storage Instructions	End of Period Action	Record of Historical Value?	Notes
1	**ACTIVITY: Corporate Governance** Records related to incorporation and organisation of POL and its subsidiaries, ownership, boards and committees, shareholders, strategy, planning and policy.											
1.1	Board of Directors and Senior Committee Meetings	Records related to proceedings of the board of directors, board committees and shareholders. Includes meeting minutes and meeting notices, shareholder decisions.				Ten years from date of meeting.	S.248(2) CA 2006			Transfer to Postal Museum Archive.	Y	
1.2	Business Organisation and Incorporation	Records related to the creation, structure, and governance of POL and its subsidiaries. Includes incorporation documention, articles and memorandum of association, and name change certificates.				Permanent.	S.32 CA 2006			Transfer to Postal Museum Archive.	Y	
		Copies of forms filed at Companies House.				No requirement to retain. Good practice to retain copies for two years.	CA 2006			Destroy	N	
		Statutory registers.	Register of members	Electronic	Blueprint	Permanent. Entries for former members must be retained for at least ten years from the date when they ceased to be members.	S.114 CA 2006			Transfer to Postal Museum Archive.	Y	
			Register of Directors and Secretaries	Electronic	Blueprint	Permanent.	S.162 CA 2006					

DRAFT

POL00401626

5. Control

5.1. Policy Version

Date	Version	Updated by	Change Details
26/02/2018	0.1	IPA & CoSec	First draft Version
04/03/2018	0.2	IPA & Head of MI, Analytics and Data Strategy	Edits following peer review.
07/03/2018	1.0	General Counsel	First Final Version

5.2. Policy Approval

Group Oversight Committee: Risk and Compliance Committee (RCC)
Sign-off Authority: Risk and Compliance Committee (RCC)
Policy Sponsor: Jane MacLeod, Group Director of Legal, Risk & governance
Policy Owner: Head of Information Protection and Assurance
Policy Author: Jules Harris
Approved by: Post Office Management Services Limited RCC
Post Office Ltd RCC

Approved: Xx xxx 18
Next review: Xx xxx 19

DRAFT

POL00401626

IT Security Policy

Author: Hazel Freeman | Sponsor: Jane MacLeod | Meeting Date: 13 March 2018

Executive Summary

Context

1. To support the GDPR project a new policy is being presented for review. This is titled 'IT Security Policy' and replaces the Business Information Systems policy and Business Information Systems Framework. The policy has been aligned to the COBIT5 project and the IT Risk register maintained by Financial Control.

Questions addressed in this paper

1. Why is the policy required?
2. Changes to the policy and the value of those changes
3. Stakeholder inclusion in developing the policies
4. How we will communicate the policies to third parties?
5. Implications of the policy changes to our staff and the wider business
6. Impact of delaying approval

Conclusion

2. The IT Security Policy has been created to provide a set of minimum controls needed to mitigate the following risks to Post Office data;
   - Poor design of business applications or lack of consideration regarding security requirements during the design process can lead to the introduction of security vulnerabilities and subsequently result in breaches of data, loss of integrity or data being accessed by unauthorised individuals.
   - Having inappropriate access controls to data owned or processed by Post Office could lead to inappropriate access by unauthorised individuals.
   - If the design of systems supporting or running security services for Post Office are not securely designed to the highest standards, those functions cannot be assured and Post Office systems and data may be open to attack, causing data breach or loss of confidentiality, integrity and availability.
   - If networks supporting the flow of Post Office information are not designed with security in mind, then those networks themselves may contain vulnerabilities causing a loss of confidentiality, integrity or availability of systems and or data.
   - Poorly controlled mobile and removable devices may lead to a data breach causing a loss of confidentiality, integrity or availability, reputational damage and/or fines from the regulator.

POL00401626

- If Post Offices devices (laptops, mobiles, network devices, servers etc) are poorly configured or maintained and those vulnerabilities are exploited then this could lead to a loss of confidentiality, integrity or availability, reputational damage and/or fines from the regulator
- Post Office's environment is compromised due to lack of, or poorly configured cyber threat protection solutions which could lead to a loss of confidentiality, integrity or availability, reputational damage and/or fines from the regulator.

Input Sought

The RCC is asked to approve the new IT Security Policy

POL00401626

The Report

Why is the policy required?

3. This is a new policy that is required to support the GDPR program. It supports section (f) of Article 5 of the regulation:

   GDPR requires that personal data shall be:

   "f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Changes to the policy and the value of those changes.

4. The policy has been created using the new template, the controls are clearly linked to the risks that they are mitigating.
5. The policy is supported by a number of standards that are currently under review, these include:
   - Access control Standard
   - Network Security Standard
   - BYOD Standard
   - Wireless Standard
   - Cloud Computing Standard
   - Portable Device Standard
   - Remote Access Standard
   - Logging and Monitoring Standard
   - SDLC standard
   - Encryption Standard
   - Anti Malware Standard
   - Patch Management Standard
   - Configuration Standard
   - Cyber Incident Response Standard
   - Threat Management Standards
   - IT Security Standard

Stakeholder involvement in developing the policies

6. The policies have been developed by - Information Protection and Assurance (IPA), IT Security; in conjunction with - Legal, Risk and Governance. Data Protection Officer, and Financial control (COBIT5 project).

How we will communicate the policies to third parties?

POL00401626

7. IT Security will:
   - update the policies on the SharePoint site for staff reference
   - engage with suppliers to inform them of the new policy set
   - perform workshops with suppliers so they understand what is required of them
   - perform a gap analysis with the suppliers to understand where we have gaps
   - work with the suppliers to create a remediation plan
   - communicate the existence of the new policies in the all-staff Monthly Information Security Update publication

Implications of the policy changes on our staff and the wider business

8. This policy is mainly directed at suppliers of IT Services to Post Office, and not colleagues. Within IT colleagues in the architecture space are required to ensure that these policies have been adhered to as part of any designs received from our third party suppliers.
9. Over the next 12 months, IT security will work with our suppliers to understand where our gaps are and remediate them.
10. The introduction of the Minimal Control Requirements supports third parties in understanding what is required of them.

Impact of delaying approval

11. The GDPR deadline is fast approaching (May 2018), we have already updated Schedule 16 of the standard contract to include the IT Security Policy as a requirement.

POL00401626

GROUP POLICIES

IT Security Policy

Version – V0.3

POL00401626



1. Overview 3
1.1. Introduction by the Policy Owner 3
1.2. Risk Appetite 3
1.3. Purpose 3
1.4. Core Principles 3
1.5. Application 4
1.6. Legislation 4
1.7. Industry Guidance 5
1.8. Policy Framework 5
1.9. Who must comply? 5
2. Minimum Controls 6
3. Where to go for help 10
Additional Policies 10
3.1. How to raise a concern 10
3.2. Who to contact for more information 10
4. Control 11
4.1. Policy Version 11
4.2. Document Control 11

POL00401626

1. Overview

1.1. Introduction by the Policy Owner

Post Office is committed to protecting its employees, customers, Third Party Supply Chain and information assets from damaging or illegal actions by individuals, either knowingly or unknowingly. Post Office enables this through the development and deployment of policies, standards and guidelines which are aligned to international best practices. Effective cyber and information security is a team effort involving everyone in Post Office.

1.2. Risk Appetite

There follows a list of applicable Risk Appetite statements for this policy:

- **Averse risk appetite** in relation to not complying with law and regulations or deviation from its business conduct standards, of which this standard forms part.
- **Averse risk appetite** in relation to any serious impact to the confidentiality, integrity and availability of information, leading to financial loss, business disruption, public embarrassment or legal consequences in line with risk impacts.
- **Tolerant risk appetite** for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality.
- **Averse risk appetite** for litigation in relation to high profile cases / issues.
- **Averse risk appetite** for unethical behaviour including staff misfeasance.
- **Averse risk appetite** for data loss/leakage that can lead to customer, commercial or reputational damage
- **Neutral risk appetite** for operational IT services.
- **Averse appetite** for inaccurate and unreliable processing of data.
- **Averse risk appetite** for inefficient or ineffective or prolonged failure of, governance and control processes, critical financial reporting processes, critical supply chain and business continuity processes.

Post Office acknowledges however that in certain scenarios even after extensive controls have been implemented a risk may still sit outside the agreed Risk Appetite. In exceptional circumstances a Risk Exemption waiver may be granted

1.3. Purpose

The purpose of this document is to detail the minimum IT controls required to reduce the Post Offices exposure to information security threats such as:

- threats from the internet (cyber threat)
- threats from internal staff (either malicious or accidental)
- threats from third parties (either malicious or accidental)

1.4. Core Principles

Compliance with this policy will ensure that the following principles are met:

POL00401626

- External suppliers to be identified and categorised such that a risk based approach can be facilitated in assessing the suppliers security controls.
- Security arrangements can be agreed and embedded into service agreements and contracts.
- Security controls can be validated prior to services commencing and on an ongoing basis.
- Termination of third party relationships can be effectively managed so as not to expose Post Office to additional Risks.

1.5. Application

This policy relates to all Post Office information assets, including critical business information systems, as defined by Post Office, and as amended from time to time, and applies to all employees[1]

Post Office information assets and systems include, but are not limited to:

- Business environments;
- Business processes;
- Business applications (including those under development);
- Information systems; and
- Networks

1.6. Legislation

Post Office seek to comply withall relevant UK legislation and regulatory requirements including (but not limited to):

- General Data Protection Regulation (2017)
- Data Protection Act (1998 and 2017).
- Freedom of Information Act (2000).
- Privacy and Electronic Communication Act (2003).
- Regulation of Investigatory Powers Act (RIPA) (2000).
- Copyright, Designs and Patents Act (1988).
- Computer Misuse Act (1990).
- Human Rights Act (1998).
- Terrorism Act (2006).
- Limitation Act (1980).
- Malicious Communication Act 1988).
- Digital Economy Act (2010).
- Privacy and Electronic Communications (EC Directive) (Amendment) Regulations (2011).
- Counter-Terrorism and Security Act (2015).

[1] In this policy employee means employees permanent employees, temporary including agency employees, contractors, consultants and anyone else working on behalf of Post Office.

POL00401626

1.7. Industry Guidance

Post Office is a member of the Information Security Forum (ISF) which is used to provide input to Information Protection and Assurance (IPA) and IT Security developments.

1.8. Policy Framework

This policy forms part of the IPA and IT Security Policy Set which is located here:

https://poluk.sharepoint.com/sites/postoffice/inside/Pages/Information-security.aspx

1.9. Who must comply?

Compliance with this policy is mandatory for all Post Office services. All third parties who do business with Post Office, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this standard or have their own equivalent policy.

POL00401626

2. Minimum Controls

A minimum control is an activity which must be in place in order to manage the risks within the defined Risk Appetite statements contained within the table below. To comply with this, mechanisms must be in place within each business unit or product to demonstrate compliance. The minimum controls can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk, and the required minimum controls. The subsequent page defines in greater detail terms used:

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Secure Development of business applications	Poor design of Business applications or lack of consideration regarding security requirements during the design process can lead to the introduction of security vulnerabilities and subsequently result in breaches of data, loss of integrity or data being accessed by unauthorised individuals.	All projects and programmes must liaise with IT Security and the IT Architecture teams for advice and guidance on the security aspects of their designs. All development must comply with SDLC and Secure Coding and Testing standards (e.g All data used in testing must be cleansed).	Business Unit CIOs, Project & Programme Managers, and procurement.	At project design phase and during change.

POL00401626

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Identity and Access Management	Having inappropriate access controls to data owned or processed by Post Office could lead to inappropriate access by unauthorised individuals	All systems must comply with the Access Control Standard.	Data Owners, Line Managers, Business Unit CIOs, Project and Programme managers, and procurement	Whenever a new system is being designed or procured, or when significant change is being applied.
Security Infrastructure	If the design of systems supporting or running security services for Post Office are not securely designed to the highest standards, those functions cannot be assured and Post Office systems and data may be open to attack, causing data breach or loss of confidentiality, integrity and availability.	All projects and programmes must liaise with IT Security and the IT Architecture teams for advice and guidance on the security aspects of their designs. All infrastructure must comply with the Platform Security standard	Business Unit CIOs, Third party supply chain of IT Services where systems are hosting or processing Post Office Data	All the time, and evolving with new best practice.

POL00401626

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Network Management	If networks supporting the flow of Post Office information are not designed with security in mind, then those networks themselves may contain vulnerabilities causing a loss of confidentiality, integrity or availability of systems and or data.	All network designs must adhere to the Network Security standard.	Business Unit CIOs, Third party supply chain of IT Services where systems are hosting or processing Post Office Data	All the time, and evolving with new best practice.
Mobile and removable devices	Poorly controlled mobile and removable devices may lead to a data breach causing a loss of confidentiality, integrity or availability, reputational damage and/or fines from the regulator.	All mobile and removable devices must adhere to the BYOD and Portable device standards.	All staff	All the time

POL00401626

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Vulnerability Management	If Post Offices devices (laptops, mobiles, network devices, servers etc) are poorly configured or maintained and those vulnerabilities are exploited then this could lead to a loss of confidentiality, integrity or availability, reputational damage and/or fines from the regulator	All devices must adhere to the patch management and configuration management standards, and also any hardening documentation. All devices must comply with the Vulnerability Management Standards	IT Security and IT Architecture, Third party supply chain of IT Services where systems are hosting or processing Post Office Data	All the time
Cyber Threat Protection	Post Office's environment is compromised due to lack of, or poorly configured cyber threat protection solutions which could lead to a loss of confidentiality, integrity or availability, reputational damage and/or fines from the regulator	All of Post Office's cyber security protection solutions must adhere to the Threat Protection Standards	IT Security and IT Architecture, Third party supply chain of IT Services where systems are hosting or processing Post Office Data	All the time

POL00401626

3. Where to go for help

Additional Policies

This Policy is one of a set of policies and standards. The full set of policies and standards can be found at:

https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx

3.1. How to raise a concern

Any Post Office employee who suspects dishonest or fraudulent activity has a duty to:

- Discuss the matter fully with their Line Manager; or,
- Report their suspicions by telephoning Grapevine on GRO
- If either or both are not available, staff can contact the Post Office's General Counsel, who can be contacted by email at: whistleblowing GRO or by telephone on: GRO.
- Alternatively staff can use the Speak Up service available on GRO
- or via a secure on-line web portal: http://www.intouchfeedback.com/postoffice

Post Office encourages members of the public or people not employed by us who suspect [*activity in breach of policy*] to write, in confidence, to the **Chief Executive's Office, Finsbury Dials, 20 Finsbury St, London EC2 9AQ**.

3.2. Who to contact for more information

If you need further information about this standard or wish to report an issue in relation to this standard, please contact Information Protection and Assurance via ipa GRO or IT Security via ITSecurity GRO

POL00401626

4. Control

4.1. Policy Version

Date	Version	Updated by	Change Details
06/02/2018	0.1	IT Security	First draft for review
05/03/2018	0.2	IT Security & IPA	Updated post JH Comments
09/03/18	0.3	IT Security	Updated post peer review

4.2. Document Control

Group Oversight Committee: Risk and Compliance Committee (RCC)
Sign-off Authority: Risk and Compliance Committee (RCC)
Policy Sponsor: Rob Houghton, Group CIO
Policy Owner: Head of IT Security
Policy Author: Hazel Freeman
Approved by: Post Office Ltd RCC

Approved: Xx xxx 18
Next review: Xx xxx 19

POL00401626

IT POLICIES

IT Disaster Recovery Policy

Version – V0.1

POL00401626

Group Oversight Committee:	Risk and Compliance Committee (RCC)
Sign-off Authority:	Risk and Compliance Committee (RCC)
Policy Sponsor:	Rob Houghton Group CIO
Policy Owner:	IT Security and Service Director
Policy Author:	Head of IT Risk & Compliance
Approved by:	Post Office Management Services Limited RCC Post Office Ltd RCC
Approved:	
Next review:	

POL00401626

1. Overview 4
1.1. Introduction by the Policy Owner 4
1.2. Purpose 4
1.3. Core Principles 4
1.4. Application 5
1.5. Impact of loss of service 5
1.6. Legislation 5
2. Risk Appetite and Minimum Control Standards 6
2.1. Risk Appetite 6
2.2. Policy Framework 6
2.3. Who must comply? 6
2.4. Minimum Control Standards 7
3. Where to go for help 10
3.1. Additional Policies 10
3.2. How to raise a concern 10
3.3. Who to contact for more information 10
3.4. How to request an exception 10
4. Version Control 11

POL00401626

1. Overview

1.1. Introduction by the Policy Owner

Post Office's Board and Group Executive (GE) recognise that with the ever increasing threat landscape, the possibility and the impact of events caused by human action or natural disasters must be planned for.

The GE are committed to developing a strategic response to current and emerging threats to enable Post Office to achieve its objectives, whilst preserving the Post Office brand, commercial image, reputation, competitive advantage, revenues, profitability, legal, regulatory and contractual compliance.

Employees have a responsibility to understand the requirements set out in this policy, if there is any misunderstanding, the employee must gain clarification from the IT Service Performance team.

1.2. Purpose

The purpose of this document is to detail the IT controls required to reduce exposure to the Post Office brand in the event of Disaster Recovery incident occurring within the Post Office estate.

Disaster recovery focuses on the IT or technology systems supporting critical business functions, as opposed to business continuity, which involves keeping all essential aspects of a business functioning despite significant disruptive events. Disaster recovery is therefore a subset of business continuity.

Disaster Recovery is where our catastrophic loss over services hosting site occurs and invocation and recovery is needed from an alternate location, this is different from resilience which is the mechanism that is designed in to keep systems available in the event of component failure loss at the same location.

Resilience should be measured in no loss to the system disaster recovery is where a recovery exercise needs to occur to invoke and set up a system post a catastrophic host location loss.

1.3. Core Principles

Compliance with this policy will aid in adhering to the following principles:

- Maintain and enhance shareholder/stakeholder value.
- Protect revenue streams and business profitability.
- Improve governance.
- Ensure that IT DR postponement is managed by exception.
- Compliance with Legal and Regulatory requirements.

POL00401626

1.4. Application

This policy applies to employees[1]and, Third Party Supply Chain.

1.5. Impact of Loss of Service

The inability to recover service will result in a Loss of Service to our customers.

Data loss can lead to financial loss through fines from regulators, damage the reputation of Post Office though negative coverage in the media and result in loss of trust by our customers and suppliers.

1.6. Legislation

Post Office seek to comply with all relevant UK legislation and regulatory requirements.

ISO/IEC 27031:2011

ISO 22301

ISO/IEC 24762:2008

[1] In this policy employee means employees permanent employees, temporary including agency employees, contractors, consultants and anyone else working on behalf of Post Office.

POL00401626

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

There follows a list of applicable Risk Appetite statements for this policy:

- **Averse risk appetite** for inefficient or ineffective prolonged failure of governance and control processes, critical supply chain and business continuity processes.
- **Averse risk appetite** for any serious impact to the confidentiality, integrity and availability of information which may result in financial loss, business disruption, public embarrassment or legal consequences.
- **Averse risk appetite** for data loss/leakage that can lead to customer, commercial or reputational damage

Post Office acknowledges that in certain scenarios, even after extensive controls have been implemented, a risk may still sit outside the agreed Risk Appetite. In exceptional circumstances a Risk Exemption waiver may be granted.

2.2. Policy Framework

This policy forms part of the IT Policy Set. IT Policies are currently under review.

2.3. Who must comply?

Compliance with this policy is mandatory for all Post Office employees and applies wherever in the world Post Office business is undertaken.

All IT Services, Systems and Infrastructures will have IT Disaster Recovery criteria agreed, that conforms to the business needs and the IT Disaster Recovery Framework.

All new IT services must have an agreed IT Disaster Recovery criteria with the IT Security and Service Director prior to transition to the live service.

POL00401626

2.4. Control Standards

The control standards described below are derived from the IT Controls Framework (COBIT 5). The controls are in place to manage the risks within the defined Risk Appetite statements, as contained within the table below. To comply with this, mechanisms are in place within IT to demonstrate compliance.

The table below sets out the relationships between identified risk, and the required minimum control standards.

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Identify areas of continuity that need addressing	Failure to define an IT business continuity plan may result in inability to restore critical applications within defined timelines in line with business need.	• Disaster Recovery Framework in place. • (BIA) is performed on a periodic basis which considers the impact of a disruption to critical business functions. • ITSCM Monthly reviews are in place, outputs of DR to be discussed and manage any escalations. • Obtain the defined RTOs and RPOs for key PO applications and understand if both the business and IT have agreed the recovery timeframe.	IT Service & Performance. SISD IT Service Continuity Manager	Annual
Develop and implement a business continuity response	Failure to define a PO IT business continuity plan may result in inability to restore critical applications within defined timelines in line with business need.	• The DR Framework will show the last test date/scheduled tests. • ITSCM Monthly reviews are in place, outputs of DR to be discussed and manage any escalations. • Exception process in place in place to prevent cancellation/postponement of DR tests without authorisation. • Forward Schedules to be provided by third-parties to prevent any failover tests clashing with other suppliers.	IT Service & Performance. SISD IT Service Continuity Manager. Head of IT Risk & Compliance	Monthly
Exercise, test and review	Failure to exercise and test the business continuity plan	• Third-party suppliers ensure regular test occur in accordance to their contracts.	IT Service & Performance.	Annual

POL00401626

Post Office Limited Risk and Compliance Committee-13/03/18

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
the DR Framework	in line with the PO IT business continuity strategy may result in inability to restore critical applications within defined timelines in line with business need.	• Any conflicting dates to be rearranged and scheduled.	SISD IT Service Continuity Manager Third party suppliers	
Develop and implement a business continuity response	Absence of a defined and communicated training strategy for business continuity response may result in: a) Business interruption and delays in recovery of business operations which fail to meet business needs. b) Misalignment of priorities for recovery of services.	• DR Framework to be communicated to Business Stakeholders. • Any misalignment of priorities for recovery of services will be reviewed at the Monthly ITSCM.	Head of IT Services. IT Service & Performance. SISD IT Service Continuity Manager. Head of IT Risk & Compliance	Quarterly
Manage backup arrangements	Absence of a defined process for review of backup schedules and compliance with PO IT policy may result in non-compliance with policy and failure to identify backup schedules not being setup to business requirements.	• Recovery point objectives in place where applicable. • DR Framework includes high level contractual requirements of suppliers. • Stakeholder reviews in place and confirm if the requirements for recovery are correct. • Monitored at the monthly ITSCM.	Head of IT Services. IT Service & Performance. SISD IT Service Continuity Manager.	Monthly
Conduct post-resumption review	Absence of a defined process to test and review restoration of backup and archived data may result in: a) Failure to restore from backups resulting in loss of business critical information when a disaster has occurred.	• Continuity test, understand the effectiveness of the plan, continuity capabilities, roles and responsibilities, skills and competencies. • Understand the steps required for improvement and validate if remediation plans have been put in place. • Obtain evidence that these changes were processed via the enterprise change control process.	IT Service & Performance. Change Management.	As appropriate

POL00401626

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
	b) Failure to recover applications in line with business need when a disaster has occurred.			

Post Office Limited Risk and Compliance Committee-13/03/18

POL00401626

3. Where to go for help

3.1. Additional Policies

This policy is one of a set of policies.

3.2. How to raise a concern

Any Post Office employee who suspects that a serious event is taking place is required to:

- Report this to the IT Service Desk.

3.3. Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact IT Security & Service Director.

3.4. How to request an exception

If there is anything within this policy that causes business impact, please contact Head of IT Risk & Compliance who will process the exception. Any exceptions are presented to the Information Security governance body for ratification.

POL00401626

4. Version Control

Date	Version	Updated by	Change Details
13/03/2018	V0.1		Sign off required at RCC

POL00401626

Disaster Recovery Framework

	Fujitsu	Network Banking Service (POCA/Vocalink/Santander)	Network	Debit Card System	On-line Transaction processing Service (Horizon POS)	Automated Payments Outpay (APOP)	Bureau Service	Web Services including Moneygram	Logistic Feeder Service (LFS)	Automated Payments Service (APS)	Department of Vehicle Licensing Authority - Post Office MOT Enquiry	Electronic Top-ups Service	Postal Address File (PAF) service	Transaction Enquiry Service (TES)	Track and Trace	PODG	Collect & Return Web Service
Gold Service (recovery within 5 hours)		✓	✓	✓	✓											✓	
Silver Service (recovery within 24 hours)						✓		✓		✓							✓
Bronze Service (recovery time within 96 hours)							✓		✓		✓	✓	✓	✓	✓		
Busines Impact Analysis		✓	✓	✓	✓	✓	✓				✓					✓	
Contracted Recovery Time Objective (RTO)		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Recovery Time		2 hours	2 hours	2 hours	2 hours	2-5 hours	2 hours	2 hours	2 hours	2-5 hours	2-5 hours	2-5 hours	2-5 hours	2-5 hours	2-5 hours	2-5 hours	2-5 hours
Contracted Recovery Point Objective (RPO)		n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a		n/a
Recovery Point		n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a		n/a
Managed By Atos		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DR Test frequency confirmed		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DR Tests up to date		✓	✓								✓			✓		✓	
Last Tested		Oct-17	Oct-17	May-13	May-13	May-13	May-13	May-13	May-13	May-13	May-16	May-13	May-13	May-13	May-13	Jun-17	May-13
Scheduled Test		Jul-18	Jan-18														

Key

Red box denotes risk/gap

* Verizon dates have been received and are currently being re-aligned to avoid tests already scheduled from other Suppliers.

POL00401626

Disaster Recovery Framework

	MDM (production environment)	Credence (production environment)	POLSAP (production environment)	Gemalto	Biometric Application, Enrolment and	Fres	Travel Money Card	Bureau Service	Computacenter	DHCP	Active Directory	Email	OneDrive	Sharepoint	Skype	Ricoh Printer Server	Admin LAN
Gold Service (recovery within 5 hours)	✓	✓	✓		✓					✓	✓	✓	✓	✓	✓	✓	✓
Silver Service (recovery within 24 hours)							✓										
Bronze Service (recovery time within 96 hours)								✓									
Busines Impact Analysis	✓	✓	✓				✓	✓									
Contracted Recovery Time Objective (RTO)	✓	✓	✓		✓					×	✓	×	×	×	×	×	×
Recovery Time	2-5 hours	2-5 hours	2-5 hours		4 hours					n/a	4 hours	n/a	n/a	n/a	n/a	n/a	n/a
Contracted Recovery Point Objective (RPO)					n/a					×	✓	×	×	×	×	×	×
Recovery Point					n/a					n/a	15 mins	n/a	n/a	n/a	n/a	n/a	n/a
Managed By Atos	✓	✓	✓		✓		×	×		✓	✓	✓	✓	✓	✓	✓	✓
DR Test frequency confirmed	✓	✓	✓		✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
DR Tests up to date		✓	✓		✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Last Tested	May-13	Jun-17	##		###		May-17	###		Jun-17	Jun-17	Jun-17	Jun-17	Jun-17	Jun-17	Jun-17	Jun-17
Scheduled Test					###					Jul-18	Jul-18	Jul-18	Jul-18	Jul-18	Jul-18	Jul-18	Jul-18

POL00401626

Disaster Recovery Framework

	Firewall and DDoS	Core network	Wifi	VPN	**Accenture Back Office**	Credence (software)	Core Finance	Financial Management Information	MDM	SAPHR	TransTrack	Automated	POLSAP (Software)	**Accenture CDP**	CDP Web platform	**Atos**	Service Desk	SDM12 (management tool)	**NCR**	Self Service Kiosk
Gold Service (recovery within 5 hours)	✓	✓	✓	✓		✓							✓		✓		✓			
Silver Service (recovery within 24 hours)																		✓		✓
Bronze Service (recovery time within 96 hours)																				
Busines Impact Analysis						✓							✓							
Contracted Recovery Time Objective (RTO)	×	×	×	×		✓	✓	✓	✓	✓	✓	✓	✓		✓		×	×		
Recovery Time	n/a	n/a	n/a	n/a		4 hours	4 hours	4 hours	4 hours	4 hours	4 hours	48 h	4 hours		21.4 hou		n/a	n/a		
Contracted Recovery Point Objective (RPO)	×	×	×	×		✓	✓	✓	✓	✓	✓	✓	✓				×	×		
Recovery Point	n/a	n/a	n/a	n/a		1 hour	1 hour	1 hour	1 hour	1 hour	1 hour	1 ho	1 hour		n/a		n/a	n/a		
Managed By Atos	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓		×
DR Test frequency confirmed	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓					
DR Tests up to date	✓	✓	✓	✓		×	✓	✓	×	×	×	✓	✓		✓					
Last Tested	Jun-17	Jun-17	###	Jun-17			May-17	May-17				###			###					
Scheduled Test	Jul-18	Jul-18	###	Jul-18		Oct 18 (p)	Oct 18 (p)	Oct 18 (p	Oct 18 (	Oct 18 (p)	Oct 18 (p)	Oct	Oct 18 (p)		###					

POL00401626

Disaster Recovery Framework

	Verizon	Branch Network	Voice Services	Mobiles Phones	WAN Service between Data Ce	WAN Service to all Administratic	WAN Service to all Branch Sites	LAN Service for all Administratic	LAN Service for all Branch Sites	Wireless LAN Service for Admin	Gateway Service including Perim	Third Party and business-to-bus	Branch Firewall service	Remote Access Service	Network Access Control	Threat Detection Service
Gold Service (recovery within 5 hours)		✓														
Silver Service (recovery within 24 hours)																
Bronze Service (recovery time within 96 hours)			✓	✓												
Busines Impact Analysis																
Contracted Recovery Time Objective (RTO)		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Recovery Time					1 hour	12 hours	12 hours	12 hours	12 hours	12 hours	1 hour	1 hour	12 hours	4 hours	12 hours	12 hours
Contracted Recovery Point Objective (RPO)		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Recovery Point					15 mins	15 mins	15 mins	15 mins	15 mins	15 mins	15 mins	15 mins	15 mins	15 mins	15 mins	15 mins
Managed By Atos		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DR Test frequency confirmed		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DR Tests up to date		✓	✓													
Last Tested		Feb-17	Feb-17													
Scheduled Test		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*

WAN Service between Data Centres
WAN Service to all Administration Sites
WAN Service to all Branch Sites
LAN Service for all Administration Sites
LAN Service for all Branch Sites
Wireless LAN Service for Administration Sites
Gateway Service including Perimeter security
Third Party and business-to-business Gateway Service including Perimeter security
Branch Firewall service
Remote Access Service
Network Access Control
Threat Detection Service
Voice Service for business Users
Voicemail Service for Corporate Users
Audio Conferencing Service for Corporate Users
Mobile Service for Corporate Users
IVR Service for Contact Centres
Call Routing and ACD Service for Contact Centres
Historic Reporting Service for Contact Centres
Voice Recording Service for Contact Centres
Workforce Management for Contact Centres
Outbound Dialling Service for Contact Centres

POL00401626

Disaster Recovery Framework

	Voice Service for business User	Voicemail Service for Corporate	Audio Conferencing Service for	Mobile Service for Corporate Us	IVR Service for Contact Centres	Call Routing and ACD Service f	Historic Reporting Service for C	Voice Recording Service for Cor	Workforce Management for Con	Outbound Dialling Service for Co	**Ingenico**	Paystation	**Itron**	Paystation Support	**Moneygram**	Moneygram service	**Qmatic**	Branch Queue System	**Vocalink**	Link Network Switch	**POCA**	Post Office Card Account services Contact centre	Post Office Card Account services Cheque Printing	Post Office Card Account services Banking Engine
Gold Service (recovery within 5 hours)																✓				✓			✓	✓
Silver Service (recovery within 24 hours)																✓						✓		
Bronze Service (recovery time within 96 hours)												✓		✓				✓						
Busines Impact Analysis																								
Contracted Recovery Time Objective (RTO)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		×						✓		✓		✓	✓	✓
Recovery Time	12 hours	12 hours	12 hours	12 hours	1 hour	1 hour	12 h	12 hours	12 h	12 hours		n/a						4 hours		4 hours		50% 4 hours	2 hours	3 hours
Contracted Recovery Point Objective (RPO)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		×						✓		×				
Recovery Point	15 mins	15 mins	15 mins	15 mins	15 mins	15 mins	15 n	15 mins	15 m	15 mins		n/a						2 hours		n/a				
Managed By Atos	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		×		×		✓		✓		×	×	×
DR Test frequency confirmed	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓						✓		✓		✓	✓	✓
DR Tests up to date												✓								✓		✓	✓	✓
Last Tested												###						Aug-16		Jun-17		Jul-17	Jul-17	Jul-17
Scheduled Test	*	*	*	*	*	*	*	*	*	*		###						Feb-18				May-18	May-18	May-18

POL00401626

Disaster Recovery Framework

	Post Office Card Account services Document Processing
Gold Service (recovery within 5 hours)	
Silver Service (recovery within 24 hours)	
Bronze Service (recovery time within 96 hours)	✓
Busines Impact Analysis	
Contracted Recovery Time Objective (RTO)	✓
Recovery Time	24 hours
Contracted Recovery Point Objective (RPO)	
Recovery Point	
Managed By Atos	x
DR Test frequency confirmed	✓
DR Tests up to date	✓
Last Tested	Jul-17
Scheduled Test	May-18

POL00401626

Business Continuity & Crisis Management Update

Author: Tim Armit Sponsor: Jane MacLeod Meeting date: 13 March 2018

Executive Summary

Context

Business Continuity capability continues to improve across Post Office. There are gaps across all areas but awareness and levels of ability to respond to incidents is increasing. Levels of resilience and recovery capability is improving in Bolton, Chesterfield, Supply Chain and the Banking Framework.

Questions this paper addresses

- Can the new Business Continuity Policy be approved?
- What is the capability to recover of Post Office key sites?
- How have recent incidents been managed?

Input Sought

The Committee is requested to note the report.

POL00401626

Conclusion

Approval of the updated Business Continuity Policy

1. Attached is a revised Business Continuity Policy, this is primarily a reformatting of the Policy approved last year with a few minor changes. As part of the policy, The Policy should be reviewed and approved annually.
2. The committee is asked to approve the Policy.

What is the current capability of key locations to recover?

1. Post Office has had a contract with SunGard for the provision of work space recovery solutions for a number of years. This contract provides desks, PC's, telephones, network connections, meeting rooms and facilities to Post Office within 3 hours of a major incident and this can be used for up to 3 months. This contract was set to only support Chesterfield and was scaled to lower numbers of staff.
2. The contract is now being upgraded to include doubling the number of desks available for Chesterfield (120 positions) and providing Bolton (50 positions), Bristol (20 positions) and London (20 positions).
3. The SunGard solution requires a fixed VPN link to Post Office systems. This is being implemented in March 2018 and will enable all offices at all SunGard locations to be able to access Post Office systems.
4. Chesterfield will test this solution on March 23rd with staff relocating from the Post Office to the SunGard site to work in a normal manner for a day.
5. Bolton has identified the impacts it could suffer if unable to work and is implementing team based recovery plans. Initial reports show that a 2 day down time would have minimal operational impact, this is to be robustly challenged across the business. Payroll is key but can be mitigated by using last months data at BACS. The SunGard solution for this will be tested by the end of April 2018.
6. Bristol Inventory call centre supports branch orders of cash into Supply Chain. A recovery solution to support this is being implemented in the new contract and will enable the team to relocate and continue to operate.
7. London relies upon home working as its primary recovery solution and this was tested in 2017 and during the recent snow. The 20 positions are to enable crisis management to be controlled and to bring together teams over the following weeks after an incident where groups need to work together.
8. Supply Chain review has been completed and the report is with management for presentation and agreement in April 2018. This has identified a number (154) of challenges and requirements to ensure resilience is in place across the depots. Supply Chain and Business Continuity are now reviewing these to prioritise, assess impact and agree solutions.
9. Banking Framework has worked with Business Continuity to identify risks and impacts of failures in the processes. The cycle of a cheque or cash from customer to reconciliation relies on a number of third party suppliers and now this flow has been captured and detailed the risk in this supply chain can be challenged and the plans in place with third parties confirmed. This report will be reviewed and the next steps to ensure supplier plans are in place will be undertaken by May 2018.

POL00401626

10. The Grapevine invocation of the Post Office crisis management system, called the Business Protection Team continues to improve. This was used quickly during the Verizon call centre failure and regularly across the adverse weather conditions once it was clear there was a significant impact to operations. The calls are focussed, short and effective. The system was not invoked during the explosion in Farnham and the lock out from the London cash centre as the decision was to manage these as operational issues and the impact was at a local level and not across multiple Post Office business areas. This system has now been fully rolled out to POMS and is being implemented across all of Supply Chain.

11. There still remains key IT systems that are vulnerable to being lost in a major incident and IT are aware of these. They include the Swindon based systems to support all warehouse activity and the APOP system in Chesterfield to manage all Payments Out. The data is not secured on these systems and there is no recovery capability. The business owners are aware and are working with IT to develop solutions. This risk has been reported in many forums for over a year and progress to secure the data and implement a recovery solution is critical.

How successful was the management of significant incidents?

12. The adverse weather between February 27th and March 3rd impacted operations across all parts of Post Office. The response from staff was exceptional and the BPT met multiple times each day to report on the situation and manage any areas of risk. Across the period a number of Supply Chain depots were impacted either being closed or having to deliver to only local urban areas. Branches did a tremendous job with only around 200 being closed from 11,500 at the worst periods. Chesterfield call centre and Bristol had to close early on a couple of days but with no visible signs of impact. Mail and Cheques were not collected regularly from many branches, Royal Mail suspended guarantees on Special Delivery and ParcelForce did the same. No POCA issues were reported and no cash outs happened. All staff were reported safe at all times.

13. Verizon Puzzel system failed on February 22nd across the UK failing all Post Office call centres and all other Verizon UK customers. This was down for over 2 hours and Verizon could not determine the root cause. As this happened later in the day the impact was minimal but the failure of operations was total. The BPT worked well to support communications and liaison with IT. IT are working with Verizon to determine how this could happen and why their recovery capability was so poor.

14. There was an explosion in the Farnham branch on March 4th which is believed to be related to appliances in the kitchen. No one was hurt, there was a significant police and media immediate response but once it was found to be an accident this went away very quickly. The branch opened the next day.

15. The London Cash Centre could not be opened on March 5th. A power failure locally defaulted the doors to the site to locked and the manual over ride and generator support did not work. Entry was delayed for a number of hours impacted the delivery to branches on that day. This has happened before and Facilities and Supply Chain are now working urgently with CBRE on a solution.

POL00401626

Appendix 1
Status of progress

Action	*Update*	*Owner*	*Target Date*
Further training and education for the Business Protection Team including improvement of the procedure to invoke the Business Protection Team	Initial changes made to invocation in place. Second workshop planned for April	Tim Armit	4/18
Development and implementation of a recovery strategy for Bolton	Cost for Sungard solution agreed and budget, meeting with Bolton lead team to agree solution being planned for March with a test in April.	Joe Connor / Tim Armit	4/18
Stay Calm manual needs to be simplified and training provided as to its use	Training across Supply Chain depots underway. Agreement to restructure Stay Calm is in place with key users within Supply Chain. Review of documentation complete. Draft new approach out for pilot now, once approach agreed new approach to be rolled out in April. Restructured document in place by year end.	Tim Armit / Marcia Bourne	4/18
Resilience levels across all key locations and facilities needs to be tested, improvements identified and implemented.	Chesterfield solution in place and approach to PC's being reviewed for improvement by IT. Finsbury Dial home working proven in a controlled manner in August 2017 and more realistic exercises will develop from this in the summer of 2018. Supply Chain solutions being reviewed. The levels of resilience will continue to be reviewed whilst plans and strategies are developed across all areas led by Tim Armit but owned by each business lead. This will take until June 2018	Paula Jenner / Tim Armit / Russell Hancock	6/18

Detailed plans across all sites and business areas are in place and can be presented during a deep dive into business continuity capability and status.

POL00401626

Business Continuity Management Policy Review

Approval Sought

Please find attached an updated version of the Business Continuity Policy. This has been approved and implemented in previous year and should be reviewed and re-approved annually, this is what is required.

The policy has been transferred to the new Post Office policy template and slightly simplified but with no other material changes.

The key approach steps are taken directly from the ISO Standard and ensures we are working to best practice and that when challenged by customers or suppliers we can demonstrate an approach which meets their expectations.

Within Post Office at this time the current status against the policy is shown at a high level below:

- The impact on the business areas of IT systems failing has been completed.
- Impact analysis of Bolton operations has been completed for a first review.
- Impact analysis on Chesterfield has been completed for a first review.
- Impact analysis on LRG operations has been completed for a first review.
- Banking Framework processes impact on supplier failure has been completed for first review. Suppliers must now be challenged by Banking to prove their recovery capability meets Post Office requirements.
- Risk analysis on all key locations has been completed by CBRE
- Current status of recovery strategies and recovery capability for Supply Chain has been completed for first review. Key risks in terms of Swindon and contingency strategies for depots are to be worked through.
- Incident management processes are in place and proven within the BPT approach.
- BPT training has been completed.
- Initial Gold Team training has been completed.
- Testing of Chesterfield has been completed and is planned again for March 2018
- Testing for Bolton is planned for April
- Working from home test for Finsbury Dials has been undertaken
- A recovery capability for Bristol, Chesterfield, Bolton and London is being implemented with Sungard

All work is being managed against the Policy approach. A wide scope has been undertaken to run multiple stream projects across many areas of Post Office simultaneously to reduce the risk many areas are exposed to.

The aim is for you to please approve the attached policy.

Tim Armit

Business Continuity Manager

POL00401626



Business Continuity Management Policy

Version – V2.2

DRAFT

POL00401626

1 Overview 3
1.1 Introduction by the Policy Owner 3
1.2 Purpose 3
1.3 Core Principles 3
1.4 Business Continuity Objectives 4
1.5 Application 4
1.6 The Risk 4
1.7 Legislation 5
1.8 Industry Guidance 5
2 Risk Appetite and Minimum Control Standards 6
2.1 Risk Appetite 6
2.2 Policy Framework 7
2.3 Who must comply? 7
2.4 Minimum Control Standards 8
2.4.1 Threats 11
2.4.2 Approach 11
2.5 Implementation 12
2.5.1 Satisfying BCMS Requirements 12
3 Tools & Definitions 14
3.1 Tools 14
3.2 Definitions 14
4 Where to go for help 15
4.1 Additional Policies 15
4.2 How to raise a concern 15
4.3 Who to contact for more information 15
5 Governance 16
5.1 Governance Responsibilities 16
6 Control 17
6.1 Policy Version 17
6.2 Policy Approval 17

DRAFT

POL00401626

1 Overview

1.1 Introduction by the Policy Owner

The Business Continuity Manager has overall accountability to the Board of Directors for the design and implementation of controls to prevent or deter failures in normal operations. The Business Continuity Management Policy details the approach to implementing strategies and plans to minimise the impact to operations and restore operations in a time to meet business requirements. This approach ensures the risks to operations are known, the impact to operations of failure are understood and recovery priorities are based upon the tolerance to impact. The Policy is an agenda item for the Audit and Risk Committee and the Post Office board is updated as required.

1.2 Purpose

This Policy has been established to set the minimum operating standards relating to the management of the Business Continuity risks. It is one of a set of policies which provide a clear risk and governance framework and an effective system of internal control for the management of risk and continuity of operations across the group. Compliance with these policies supports the Group in meeting its business objectives and to balance the needs of shareholders, employees and other stakeholders.

1.3 Core Principles

Post Office adopts the Business Continuity Institute's Good Practice Guidelines definition of business continuity as: "A holistic management process that identifies potential threats to an organisation, and the impacts to business operation those threats, if realised, might cause, and provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities."

This Policy is consistent with "ISO22301", which is the Business Continuity International Standard. The purpose is to define the Group's policy with regard to business continuity management that is appropriate to its aims and objectives. This includes a framework for:

- setting business continuity objectives;
- satisfying appropriate legal, regulatory and contractual requirements;
- continual improvement of the Business Continuity Management System ('BCMS'); and
- key controls in respect of business continuity.

This policy should also be read in conjunction with other Post Office resilience, health & safety, and physical security related policies and procedures.

DRAFT

POL00401626

The following areas of Post Office's business are within the scope of the policy:

- All customer support centres including but not limited to, Finsbury Dials, Chesterfield and Bolton office
- All Supply Chain Locations
- All Directly Managed Branches
- All other Post Office Operational centres
- All external/outsourced Supply Chain Capability.

Out of Scope of this Policy:

- All IT systems – these are covered within the ITDR Policy

This policy's effective date will be determined by the date on which final approval is given by the appropriate governance forum

1.4 Business Continuity Objectives

Based on the requirements and factors set out in this document, the following major objectives are set for business continuity:

- Objective 1 - Comply with health and safety legislation at all times
- Objective 2 – Maintain stakeholder confidence
- Objective 3 – Maintain customer service levels
- Objective 4 – Minimise loss of revenue

The success of the BCMS will be judged on its ability to meet these overall objectives.

1.5 Application

This Policy is applicable to all areas within the Group and defines the minimum standards to control financial loss, customer impact, regulatory breaches and reputational damage in line with the Group's Risk Appetite.

The risk to the Group from Business Continuity is reviewed by the board annually.

1.6 The Risk

The Business Continuity Policy is designed to help mitigate the risk that normal operations are interrupted and not restored in a controlled and timely manner with the consequence that:

- staff and Customers safety is at risk;
- customers are unable to be served;
- regulatory requirements are not met;
- legal and contractual breaches occur;
- income is affected; and
- confidence in the Post Office's reputation is harmed.

POL00401626

1.7 Legislation

The Group is subject to a variety of legal and regulatory requirements which either apply directly or are imposed through contractual arrangements with key clients. These include, but are not limited to:

- Health and Safety legislation;
- Payment Card Industry – Data Security Standard compliance;
- Financial Services legislation;
- National and international standards e.g. ISO9001; ISO270001; and
- Consumer protection legislation.

1.8 Industry Guidance

ISO22301 is the accepted International Standard for Business Continuity. There are other Standards on Operational Risk, Information Security, Crisis Management and IT Disaster Recovery.

The Business Continuity Institute issues good practice guidelines

The FCA issues best practice guidelines

DRAFT

POL00401626

2 Risk Appetite and Minimum Control Standards

2.1 Risk Appetite

The following risk appetite statements are relevant to Business Continuity:

> ***Averse*** appetite for taking risks which might result in failure to maintain the service commitment in respect of customers in line with our social purpose and Government's policy on subsidy**.**
>
> ***Neutral*** risk appetite for dissatisfaction related to BAU services recognising that in a complex business there will be a level of dissatisfaction as part of the normal course of business of achieving our commercial objectives.
>
> ***Averse*** appetite for risk taking which would alienate or lose significant groups of profitable customers
>
> ***Tolerant*** risk appetite for customer dissatisfaction caused by transformation, innovation and customer selection/profitability decisions.
>
> ***Neutral*** appetite for risk taking which would have a detrimental impact on vulnerable customers. Post Office will take a balanced view, reflecting commercial implications of introducing safeguards and controls to protect vulnerable customers and the needs of those customers.

Post Office takes its legal and regulatory responsibilities seriously and consequently has:

> ***Tolerant*** risk appetite for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality
>
> ***Averse*** risk appetite for not complying with law and regulations or deviation from business' conduct standards
>
> ***Averse*** risk appetite for unethical behaviour including staff Misfeasance, failure of, governance and control processes, critical financial reporting processes, critical supply chain and business continuity processes.

Post Office is committed to safeguarding the wellbeing of its people and therefore has:

> ***Averse*** risk appetite associated to the health, safety and wellbeing of POL customers and colleagues in everything we do. This is paramount to every aspect of POL operation. This includes; loss of life, serious injury and non-compliance to regulation and policy

DRAFT

POL00401626

Post Office is committed to exploiting technological benefits to achieve market advantage. In recognition of this, Post Office has:

> ***Averse*** appetite for data loss/leakage that can lead to customer, commercial or reputational damage
>
> ***Neutral*** appetite for operational IT services
>
> ***Averse*** risk appetite for any serious impact to the confidentiality, integrity and availability of information, leading to financial loss, business disruption, public embarrassment or legal consequences.

Post Office recognises that it cannot completely eliminate business continuity risks. However, this policy sets out controls to reduce and/ or mitigate such risks.

This level of risk appetite will be applied to the risk assessments that are carried out as part of the BCMS and will determine the actions that need to be taken to mitigate risk to an acceptable degree.

2.2 Policy Framework

Post Office has established a suite of resilience and risk policies, on a risk sensitive approach which are subject to regular review. Other policies which may be relevant to business continuity include the following:

- IT Disaster Recovery
- Information Security
- Data protection

2.3 Who must comply?

Compliance with this Policy is mandatory for all Post Office employees and applies wherever the Group's business is undertaken. All third parties who do business with the Group, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this Policy with their own equivalent Policy.

Where non-compliance is identified the matter must be referred to the Director of Risk and Compliance and the Group Legal Director. Any investigations will be carried out in accordance with the Investigations Policy. Where is it identified that that an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary offence.

The next page sets out the minimum control standards that the Group has implemented to control these risks.

DRAFT

POL00401626

2.4 Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
All	BCMS is not fit for purpose.	Annual review of the BCMS content and effectiveness. Internal Audit review	Business Continuity Manager Audit Manager	Annually
All	Risks the business and locations are exposed to are not known or are inadequately mitigated.	ISO22301 defines managing Business Continuity risks to include an assessment of : • Threats; • Vulnerabilities; • Impact & likelihood before risk treatment; • Risk treatment (e.g. reduction, removal, transfer); • Function responsible/ owner; and • Timescale and review frequency.	Business Continuity Manager. IT DR Manager. Facilities Manager. Location PICS. Business Leads.	Annually
All	The impact on operations of a business continuity incident is not clearly understood.	Impact is measured against agreed metrics and agreed times to ensure business areas can be compared and strategies implemented which are compatible with the risk and impact the operational area is exposed to.	Business Continuity Manager. Business Leads	Every two years or on change.

DRAFT

POL00401626

All	Recovery strategies do not meet business needs	Annual tests of strategies in place to ensure business has confidence and understanding in the capability	Business Continuity Manager All business leads	Annually
All	Contingency plans are not in place or available.	Plans in place must be assessed by internal audit and annually the status presented to the RCC. Plans must be held by all managers and available in a single accessible repository.	All business leads Business Continuity Manager	Annually
BPT	BPT does not know the process to respond to a crisis	All BPT members are contacted and involved in crisis conference calls and undergo training.	Business Continuity Manager BPT members	Twice yearly
All	Staff are unaware of how to respond to a crisis	All staff are briefed and made aware of their responsibilities	Business Continuity Manager All business leads	Ongoing
Building unavailable	Any key operational site may become unavailable for its purpose.	Risk assessments of sites are carried out annually by CBRE and POL. Strategies for the recovery of key operations per site are in place and annually tested.	Business Lead. Facilities Manager. Business Continuity Manager.	Annually. Upon moving in.
IT system failure	Any IT system can fail at any time.	This is managed under the IT DR policy and the IT COBIT process. All systems are documented and the impact of them failing documented. Resilient and DR capability is in place and managed by IT. This is tested annually.	CIO IT DR lead Business Leads Business Continuity Manager	Annually. Upon Change. Upon implementation
Supply Chain distribution failures	Depots, Vans and operations may fail leading to routes and deliveries and collections not meeting business needs.	Plans and strategies to mitigate failures are in place and tested. Contingency planning for the loss of all forms of assets are tested.	Supply Chain lead Depot Leads Business Continuity Manager	Annually
Outsourced or supplier failure	Post Office relies heavily on suppliers and outsourcing to achieve its day to day operations. Any of these could fail or go out of business.	Part of the contract allocation and contract management covers business continuity. All suppliers commit to meet business continuity requirements and to test these. Contracts must contain appropriate BC and DR capability statements. Suppliers should demonstrate their recovery capability before a contract is signed, on review of the contract and if necessarily post any incident that	Contract owner. Area dependent on contract. Business Continuity Manager. IT DR manager	Annually

Post Office Limited Risk and Compliance Committee-13/03/18

POL00401626

		affects them. Capability to restore operations in stated timeframes must be tested annually by all key suppliers. Suppliers to be categorised according to the risk their failure presents to Post Office. Many key suppliers will be within IT and the business consequence of an IT supplier failing must be shown to be mitigated by IT DR tests within these suppliers.		
Staff unavailable	Post Office staff are the key to the success of operations. At any time due to weather, health or any scenario staff may be unable to work.	Identification of single point of failure staff is undertaken within the contingency planning. Key roles must be documented and where possible dual role training undertaken. As a working example the dependency on skilled drivers is key to supply chain and this is mitigated by the Rapid Response Team when required.	All business leads. HR leads Business Continuity Manager.	Ongoing.

DRAFT

POL00401626

2.4.1 Threats

Post Office plans for the worst case scenario and does not work to specific threats unless they are beyond the scope of the risks planned for. Threats continue to vary and these will be used to define scenarios for exercises. Threats include:

- Weather related events
- Infrastructure failure
- Pandemic
- Cybercrime
- Environmental disasters
- Terrorism
- Industrial Action

2.4.2 Approach

In the approach to implementing, managing and reviewing business continuity capability the Post Office will:

- Create a Business Continuity Management System in line with ISO Standards showing the detailed approach to implementing and managing business continuity;
- Complete Risk and Impact assessments of tangible and intangible losses. To include an understanding of contractual and regulatory obligations, potential causes of risks, and impact of events both in terms of direct financial loss, cash flow interruption, customer impact, operational consequences, reputational impact and legal/regulatory impact. These assessments allow prioritisation of time and resource to implement recovery solutions;
- Develop and document strategies and plans to address key risks;
- Implement plans and recovery strategies (eg resilient IT, offsite recovery locations etc);
- Manage the central and local storage of plans;
- Annually (or more frequently) review plans;
- Consider impact of change activity on plans as part of major change activity;
- Create, manage and facilitate Post Office crisis response;
- Report all incidents and their impact;
- Test all strategies to ensure they meet business requirements;
- Integrate with IT recovery capability to ensure it meets business requirements;
- Train staff in the contingency plans and their roles and responsibilities;
- Complete root cause analysis when there is a (material) incident and review the control framework to include 'lessons learned';
- Embed appropriate and proportionate contractual requirements in contracts with suppliers and outsourcers including reporting, audit and rectification rights;
- Ensure there is regular oversight/testing of supplier and outsourcer obligations;
- Report twice yearly on progress against these approach steps.

POL00401626

2.5 Implementation

The approach to implement business continuity within Post Office are defined within this Policy. These are the fundamental steps required which are led by business areas, facilitated by the Business Continuity Manager and are not subject to frequent change. The Post Office GE will ensure that adequate funding is available for activities identified in the implementation and ongoing support of the business continuity process.

Amendments to the Business Continuity objectives will be managed through the standard Post Office change management process if required.

2.5.1 Satisfying BCMS Requirements

Senior Managers commit to the provision of the appropriate resources to establish and maintain the BCMS and its outputs.

Regular review of the BCMS. This is conducted by the Business Continuity Manager on an annual basis, ensuring that objectives are being met. Evaluation of the current capability is undertaken and any issues identified through this audit programme and management processes are reported to the RCC. Management review includes departmental and other management meetings and document review.

Role definition and responsibilities are defined in the BCMS and reviewed by the Business Continuity Manager to ensure that colleagues understand the roles they are required to fulfil, and that they have the appropriate skills and competences to do so. These controls are necessary to ensure the continued BCMP success and to mitigate risk. Training will be provided where gaps in competency are identified and regular reviews of staff capability will be undertaken within departmental exercises.

Use of third parties. Post Office uses third parties, both internal and external, in the delivery of products and services. The ability to continue to provide these services or restore them should a supplier fail is key to Post Office operations and part of all contracts. This supplier capability will be evidenced by documentation and records, including contracts, meeting minutes and IT DR and BC test reports.

Continual improvement:

To ensure the approach to implementing and managing the BCMS is enhanced in an ongoing manner Post Office will:

- Consider effectiveness of the BCMS across all business areas and end to end systems, processes within scope;
- Enhance current processes to bring them in to line with best practice (as defined within ISO 22301);
- Increase the level of proactive continuity planning across Post Office;

POL00401626

- Achieve an enhanced understanding of and relationship with the business units to which the BCMS applies;
- Review relevant metrics (impacts, risk etc) on an annual basis to assess their appropriateness, or to make changes to them based on collected historical data and feedback or in response to incidents;
- Obtain ideas for improvement via regular review meetings with stakeholders.

Ideas for improvement may be obtained from any source, including but not restricted to: Customers; Suppliers; Colleagues; Risk Assessments & Audits.

In order to evaluate any proposed improvements to the BCMP, the following criteria would be applied:

- Cost;
- Business benefit;
- Risk;
- Implementation timescale; and
- Resource requirement.

Accepted improvement proposals will be prioritised, and planned according to standard project management principals.

DRAFT

POL00401626

3 Tools & Definitions

3.1 Tools

None in place

3.2 Definitions

Term or Acronym	Description
BCMS	Business Continuity Management System, the set of controls in line with ISO22301 to implement and manage business continuity
BC	Business Continuity
ITDR	IT Disaster Recovery, the recovery of IT systems and data
ISO 22301	The International Standard for Societal Security (Business Continuity).

DRAFT

POL00401626

4 Where to go for help

4.1 Additional Policies

This Policy is one of a set of policies. The full set of policies can be found at:

https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx

4.2 How to raise a concern

Any Post Office employee who has concerns about a failure to comply with this policy has a duty to:

- discuss the matter fully with their Line Manager; or,
- discuss it directly with their Head of Business Unit; or,
- Report their suspicions by telephoning Grapevine on GRO.
- If either or both are not available, staff can contact the Post Office's General Counsel, who can be contacted by email at: whistleblowing GRO or by telephone on: GRO.
- Alternatively staff can use the Speak Up service available on GRO
- or via a secure on-line web portal: http://www.intouchfeedback.com/postoffice

Post Office encourages members of the public or people not employed by us who suspect [activity in breach of policy] to write, in confidence, to the Chief Executive's Office, Finsbury Dials, 20 Finsbury St, London EC2 9AQ.

4.3 Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact Tim Armit – Business Continuity Manager by email at GRO

DRAFT

POL00401626

5 Governance

5.1 Governance Responsibilities

Post Office's Board of Directors have overall responsibility for ensuring that Post Office has a framework to ensure compliance with legal, regulatory and contractual requirements. The Board is kept abreast of relevant matters relating to the management of business continuity by reports from its committees including its ARC Committee. The key individuals and their specific responsibilities in relation to this policy are:

- The General Counsel is a member of the Post Office Executive team and is the Group Executive Owner and Policy Sponsor, accountable to the Board.
- The Group Business Continuity Manager is the Policy Owner who is responsible for:
    - day to day implementation of and compliance with this policy and is accountable in this regard to the General Counsel;
    - ensuring that there is an annual review of this Policy and tests compliance across the Group.
    - providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee.

Post Office's internal systems of business continuity risk control ensure that controls are regularly independently assessed for effectiveness, suitability and adequacy. In addition, Internal Audit will periodically test compliance with this policy.

DRAFT

POL00401626

6 Control

6.1 Policy Version

Date	Version	Updated by	Change Details
19th May 2016	1.0	Jon Waples	First signed version
25th Feb 2018	2.0	Tim Armit	For review and signature

6.2 Policy Approval

Group Oversight Committee: Risk and Compliance Committee and Audit and Risk Committee

Committee	Date Approved
POL R&CC	
POMS R&CC	
POL ARC	
POMS ARC	

Policy Sponsor: Jane Macleod

Policy Owner: Tim Armit

Policy Author: Tim Armit

Next review: *date of next review 01 02 2019*

DRAFT

Company Details

Post Office Limited and Post Office Management Services Limited are registered in England and Wales. Registered numbers 2154540 and 08459718 respectively. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.

Post Office Management Services Limited is authorised and regulated by the Financial Conduct Authority (FCA), FRN 630318. Its Information Commissioners Office registration number is ZA090585.

Post Office Limited is authorised and regulated by Her Majesty's Revenue and Customs (HMRC), REF 12137104. Its Information Commissioners Office registration number is Z4866081.

POL00401626

Analysis of performance of RCC against requirements

Verbatim Extracts from TOR		Meeting Dates & topics of papers reviewed					
Responsibilities -		**May-17**	**July-17**	**Sep-17**	**Nov-17**	**Jan-18**	**Mar-18**
Risk Management Framework							
a. Review the effectiveness of the risk management framework and maintain oversight of the development and implementation of the components of the risk management framework.		Supply Chain pilot of the Placemat; Business Continuity and Crisis Management update;	LRG Placemat; Risk Incidents;	LRG Placemat; Finance & Operations Placemat;	Risk Placemat	Risk Update	Risk Placemat
b. Maintain oversight of the current risk exposures of Post Office and advise on future risk strategy.		Top Risks & Risk Appetite for the ARA.					
c. Review the identification and effective management of current key risks and identified mitigating actions and regular reviews of emerging risks.			JML update; DR Testing of IT systems;			EUM Update; SuccessFactors Update; Joiners, Movers and Leavers; GDPR Update;	GDPR Programme Update;

POL00401626

Verbatim Extracts from TOR Responsibilities -		Meeting Dates & topics of papers reviewed					
		May-17	**July-17**	**Sep-17**	**Nov-17**	**Jan-18**	**Mar-18**
d. Consider and review areas of risk, which should include, but is not limited to, sufficient coverage of: (see i. – ix. in Terms of Reference)		IT Controls; Financial Controls; Financial Crime; FS Conduct; Health and Safety; Transformation.	FS Conduct Risk; Change Risk; Financial Crime; Annual Gifts & Hospitality Report; IT Controls & IT Tube Map; Finance Controls; Health and Safety; Business Continuity; DR Testing of IT systems;	FS Conduct; Change; Financial Crime; IT Controls Framework & DR; Finance Controls; Business Continuity	FS Conduct; Change; Financial Crime (including G & H update); IT Controls Framework; Financial Reporting Controls; Business Continuity	FS Conduct; Change; Financial Crime; IT Controls Framework; Financial Reporting Controls; Business Continuity; Health and Safety; Information Protection and Assurance	Financial Reporting Controls; FS Conduct Risk Update; Change; Financial Crime Risk Update; Product Risk: Gift Card; IT Risk Management Update; IT Risk Transformation Programme Update; Cyber Security & Information Assurance Update
e. Receive and review risk reports from the following management Sub-Committees: i. Transformation ii. Information Security iii. Security iv. Business Continuity		Business Continuity and Crisis Management update; Transformation;	Change Risk; Business Continuity;	Change; Business Continuity;	Change; Business Continuity;	Change; Business Continuity; Information Protection and Assurance;	Change; Business Continuity Planning;
The Committee will receive and review the draft annual risk management plan for onward reporting to the Board Audit, Risk and Compliance Committee.							

POL00401626

Verbatim Extracts from TOR		Meeting Dates & topics of papers reviewed					
Responsibilities -		**May-17**	**July-17**	**Sep-17**	**Nov-17**	**Jan-18**	**Mar-18**
The Committee will receive and review the draft annual internal audit plan for onward reporting to the Board Audit, Risk and Compliance Committee.							Audit Plan 2018/19
Internal Controls and Assurance							
a. Consider and review the adequacy of the Company's internal controls and make recommendations for the improvement of the Company's internal controls, processes and systems.		IT Controls; Financial Controls	IT Controls & IT Tube Map; Finance Controls	Camelot lessons learned; IT Controls Framework & DR; Finance Controls;	IT Controls Framework; Financial Reporting Controls;	IT Controls Framework; Financial Reporting Controls;	Financial Reporting Controls
b. Monitor the implementation of key recommendations and management action plans.		Internal audit report;	Internal audit report;	Internal audit report;	Internal audit report;	Internal audit report;	Internal audit report;
c. Review the adequacy of policy governance and recommend changes.			Vulnerable Customers; Financial Crime; Anti-Bribery and Corruption; Protecting	AML & CTF; Whistleblowing; Data Protection; Code of Business Standards	Acceptable Use Policy; Cyber and Information Security Policy;	Supplier Relationship Management;	Business Continuity Policy; Treasury Risk Management Framework, Policies and

POL00401626

Verbatim Extracts from TOR		Meeting Dates & topics of papers reviewed					
Responsibilities -		**May-17**	**July-17**	**Sep-17**	**Nov-17**	**Jan-18**	**Mar-18**
			Personal Data; Code of Business Standards				Authorities; Document Retention and Disposal Policy; IT Security Policy
Fraud, Theft and Ethics							
a. Review with management their fraud assessment, detection measures and their investigation of illegal acts, as appropriate.		Identity Fraud Incident Report; Financial Crime;	Financial Crime;	Financial Crime;	Financial Crime;	Financial Crime;	Financial Crime;
b. Review any summary of frauds, thefts and other irregularities of any size.		Identity Fraud Incident Report;					
c. Review with the internal auditors the results of any review of the compliance with the Company's codes of ethical conduct and similar policies including whistleblowing.		Whistleblowing Report;	Annual Gifts & Hospitality Report;		Financial Crime (including G & H update);		
Compliance							

POL00401626

Verbatim Extracts from TOR		Meeting Dates & topics of papers reviewed					
Responsibilities -		**May-17**	**July-17**	**Sep-17**	**Nov-17**	**Jan-18**	**Mar-18**
The Committee will monitor compliance with legal and regulatory obligations, including any significant breaches.		Horizon Scan; Modern Slavery Act; Whistleblowing Report; Identity Fraud Incident Report.		Regulatory Framework; Procurement Compliance reporting; Criminal Finances Act; Horizon Scan	Procurement; Criminal Finances Act;	Procurement; Tax Update; Annual Legal Risk Report; Legal and Regulatory Horizon Scanning;	Legal and Regulatory Horizon Scanning; Compliance with Payment Card Industry Data Security Standards; Procurement Compliance Reporting;

POL00401626

Company no. 8459718 – Strictly Confidential

RCC 18/1– 18/12

POST OFFICE MANAGEMENT SERVICES LIMITED (Company)
RISK, COMPLIANCE AND CONDUCT COMMITTEE (RCCC)
(A committee of the Executive)

Minutes of an RCCC meeting held at
Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ
On 31 January 2018 at 10.30am – 12.00pm

Present:	Ian Holloway (Chair)	POMS Risk and Compliance Director
	Russell Tavener (RT)	Chief Operations Officer
	Stephen Gaines (SG)	POMS Compliance Manager
	Nick McCowan (NM)	Head of General Insurance
	Sanjeeve Thakrar (ST)	Risk Manager
	Alberto Zannatta (AZ)	Audit Manager Corporate Services
	Jules Harris (JH)	Head of IPA
	Sally Smith (SS)	Head of Financial Crime
	Renata Prywerek (PK)	Legal Counsel
	Michael Brown (MB)	Deputy for Head of Commercial
	Elizabeth McMenemy (EM)	Compliance Advisor
	Dan Tremain (DT)	Senior Product Manager Life
	Ann Young (AY)	Compliance Advisor
Apologies:	Beverley Turner (BT)	Senior Product Manager GI
	Francisco Couto (FC)	Head of FS Legal
	Ryan Griffin (RG)	Head of Protection
	Gill Craig (GC)	Deputy for Head of Travel
	Paul Paddock (PP)	Head of Travel
	Ehtsham Ali (EA)	Senior Compliance Manager IPA

RCCC 18/1 **WELCOME, QUORUM AND CONFLICTS OF INTEREST**

(a) The Chairman declared the meeting quorate and open. The Chairman extended a welcome to all persons attending the RCCC meeting for the first time.

RCCC18/2 **MINUTES OF THE MEETING HELD ON 19 December 2017**

(a) The minutes of the meeting held on 19 December 2017 were approved and the Chairman was authorised to sign them as a true record of the meeting.

.

RCCC 18/3 **RISK AND INCIDENT MANAGEMENT**

(a) ST confirmed that there were no reportable incidents recorded in December.

(b) ST confirmed that there were 82 items on the EXCO risk dashboard, 5 of which were outside of appetite

- AR – IH confirmed that there was a framework now in place to address the concerns and that the AR risk is expected to be within appetite by the end of the year
- Strategy – Business plan. There is a meeting scheduled and an

POL00401626

update to be provided at the next meeting

- Duck Creek reconciliation - Finance are working with change to spec out controls re premium flows. Currently 6 new controls and reconciliations have been identified of which internal consistency (billing to policy) & understanding how network cash can be reconciled are priorities.
- Marketing lack of infrastructure - Recommendation for CVM pilot being scoped for approval including data, communications and capability.
- Marketing lack of resource -Recruitment of additional 10 POMS dedicated staff to sit within central marketing structure.

(c) GDPR project was discussed and IH confirmed that the delivery date for GDPR is 9 February. This is to ensure that relevant documentation is produced.

RCCC 18/4

1st LINE COMPLIANCE REPORT

(a) MB confirmed the overall trend for December was generally positive. The upheld rate for complaints remains high with Claims related complaints still the top category. Root cause analysis has been provided by Collinson and will be reviewed. POMS will be looking the timeline and the products

(b) The £50 promotional vouchers remain the top category for Life. Q4 Life protection marketing campaign went live on 8th January 2018 and will run to the 31 March 2018. It is anticipated that changes to the way the customer incentive is positioned will lead to a reduction in the number of complaints relating to customer incentives particularly in branches. Complaints volumes will be monitored throughout the campaign. POMS to review processes around customer eligibility and mailing of gift vouchers.

Action MB

(c) MB will provide an update/ paper for the next Committee on the actions being taken to reduce the volume of complaints being received in respect of the Life voucher offer.

2nd LINE COMPLIANCE REPORT

RCCC18/5

(a) IH provided an update on the compliance monitoring completed in the branch network. Where issues are identified at branch level via mystery shopping or branch review clear local actions are developed and tracked to completion. However processes to ensure that systemic trends are managed across the network currently require further enhancement. For example, branch based reviews often identify incomplete travel application forms and a network wide action plan is required to ensure that this issue is addressed. The need for clear, time bound actions with clear accountabilities to address systemic issues has been raised with the Network Management. A summary of current systemic issues has also been provided. A response has been requested by 15 February 2018

(b) EM provided an update on the Quality Monitoring undertaken in Webhelp and the variances found. There were five variances in which there could have been customer detriment. EM confirmed that the

POL00401626

customers had been contacted in all instances.

Action RT

(c) RT asked if the new scorecard had been introduced in Webhelp and EM confirmed that it had not. RT will arrange for a discussion with SG, Nichola Hazard and EM.

RCCC18/6

ASSURANCE ACTIVITY

(a) RT confirmed that all the queries raised from the Collinson audit had been answered.

(b) RT confirmed that a Devitts' complaints audit was currently underway.

(c) RT advised that the Assurance Calendar for supplier audits is ready to be shared.

(d) ST confirmed that the Compliance Monitoring plan will presented to the RCCC prior to submission and approval at the ARC.

(e) AZ advised that the Change Management review would be starting next week.

Action AZ

(f) AZ also confirmed that there is to be a review on the progress of the GDPR project. IH requested an early draft of the review.

RCCC 18/7

POLICIES AND PROCEDURES

(a) SG confirmed that an updated Compliance Manual is to be issued.

(b) ST is looking at all the POL and POMS procedures.

(c) SS reminded the meeting that all gifts and hospitality either given or received must be recorded including the gifts that are declined.

Action NC

(d) NC confirmed that a price change governance report is to be presented to the RCCC.

RCCC18/8

FINANCIAL CRIME

(a) SS confirmed that the annual training draft must be completed by Feb 28. SS also advised the meeting that last year 22 branches were switched off for failing to complete their training and to date 8 branches remain "switched off".

(b) SS advised that due to new fit and proper regulation, there would be a more rigid approach will be adopted and branches will be switched off if it is decided that the branch cannot demonstrate evidence that it complies with the fit and proper regulation.

(c) SS also advised that they would be looking at the training currently provided and ensuring that the questions are more appropriate.

RCCC18/9

INFORMATION PROTECTION & ASSURANCE

(a) Hexaware SMP document, JH advised that they are looking to baseline

POL00401626

this document with Hexaware over the coming days and then proceed to arranging an assessment of the controls Hexaware have in place.

(b) POMS PCI compliance are planning sign a contract with Global Pay this will bring them out of the current PCI certification with Post Office.

(c) The number of Cyber Attacks doubled in 2017* named as the worst year ever for data breaches and cyber incidents worldwide. Key points from report are:

- Ransomware led the way in terms of the form of attack
- Ransomware doubled in the last year to 160K
- 93% of the breaches could have been avoided using simple basic IT Hygiene.

* According to Online Trust Alliance

RCCC 18/10

INTERNAL AUDIT

(a) AZ confirmed that there were currently 8 internal audit actions open for POMS. 5 actions are recorded for Compliance and RT has 3 actions

(b) The internal audits in progress are as follows

- Travel insurance –Assessment of control framework – Reporting Phase
- MI Discover Phase- Fieldwork started
- Change Management Process – Starting 5th Feb
- Readiness to European GDPR – Planning phase

RCC18/11 **OUTSTANDING ACTIONS LIST**

(a) **Action 17/77 (b)** Home claim report – RT is to continue to ask for clarity on the Home Claim report produced by Junction RT confirmed that IC will produce this report **–Open**

(b)

Action 17/93 (d) Repudiated claim on Home Insurance. BT confirmed that she has asked Junction to provide further information - **Open**

(c) **Action 17/95 (b)** TIF Audit – RT confirmed that TIF are open to POMS conducting a review but are resistant to the use of a third party to conduct the review. RT further confirmed that following the Quarterly Business review RT would be looking to instigate formal actions or sanctions if this is not resolved. RT confirmed that TIF may allow an audit but are still insisting that it is not done by a third party– **Open**

(d) **Action 17/99 (a)** IDD – IH confirmed that he will provide a fuller update in Jan 2018. A brief update was provide to the meeting. There is continued pressure on the Network to provide IDD training for the sales force. IH is reasonably confident that the deadlines will be met. There will be a greater focus on Travel insurance. There is focus on the training record keeping and there will be a manual process until EUM commences in July. The records should be electronically stores by Feb 2019. There is will an update in March 2018 **Open**

POL00401626

RCCC 18/12 **ANY OTHER BUSINESS**

(a) SG asked if there was any monitoring being completed on the new Easy Life sales. DT confirmed that all the sales will be monitored by FSRisk by FAD and will ensure that sales are completed by branches who have been trained

(b) There was no other business raised. There being no further business the meeting was closed.

(c) The next meeting of the RCC will be held on 28 February 2018 at 14.00 pm.

Chairman.. **Ian Holloway** ..... Date 6/02/18.....

POL00401626

POL00401626

Post Office Ltd
Post Office Limited Risk and Compliance Committee
13 March 2018

Location:

1.19 Wakefield, The Boardroom, Finsbury Dials, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ, United Kingdom

ATTENDANCE LIST

ATTENDEES	SIGNATURE
MacLeod, Jane	
Cameron, Alisdair	
Houghton, Rob	
Kirke, Martin	
Mark, Davies	
Paula, Vennells	
Woodley, Owen	

Also in attendance

Koniarski, Sarah	

Apologies for absence

Smith, Debbie

Additional access

Branton, Veronica	
CoSec	
Fahey, Jane	

POL00401626

Post Office Risk and Compliance Committee Agenda

Date
13 March 2018

Start Time	Finish Time
13.00 hours	16.00 hours

Location
1.19 Wakefield, Finsbury Dials

Present	In Attendance		Apologies
Jane MacLeod (Chair)	Johann Appel	Richard Williams (5.1)	Debbie Smith
Paula Vennells	Jonathan Hill	Deana Herley (5.1)	
Al Cameron	Michael Passmore (3 & 4.1)	Ashish Singh (5.2)	
Mark Davies	Jenny Ellwood (4.3)	Barbara Brannon (8.1)	
Rob Houghton	Sally Smith (4.4, 4.4.1 & 5.2)	Clare D'Netto (7.1)	
Martin Kirke	Keith Maple (4.4 & 4.4.1)	Nicholas Spicer (7.2)	
Owen Woodley	Mick Ebsworth (4.6 & 9.3)	Mark Dixon (9.1)	
Tom Moran (On behalf of DS)	Jules Harris (4.6, 7.2 & 9.2)	Mick Mitchell (9.3 & 9.4)	
Sarah Koniarski (Secretary)	Ian Holloway (5.1)	Tim Armit (10.1 & 10.2)	

Agenda Item	Action Needed	For ARC	Purpose	Lead	Time
1. **Welcome and Conflicts of Interest**			Members to declare any conflicts of interest.	Chair	13.00 – 13.05 (5 minutes)
2. **Minutes and Action Lists**	Approval		To approve the minutes of the meeting held on 18th January and update on actions.	Chair	
3. **Internal and External Audit Procurement Plan**	Questions & Noting	✓	Verbal update on the plan for procuring internal and external audit services.	Michael Passmore / Johann Appel	13.05 – 13.10 (5 minutes)
4. **Key Operational Risks**	Discussion & approval		To review the management of key operational risks and agree for onward submission to the ARC.		13.10 – 13.50
4.1 Financial Reporting Controls		✓		Michael Passmore	(5 minutes)
4.2 FS Conduct Risk Update		✓		Jonathan Hill	(5 minutes)
4.3 Change Risk Update		✓		Jenny Ellwood	(5 minutes)
4.4 Financial Crime Risk Update		✓		Sally Smith	(5 minutes)
4.4.1 Product Risk: Gift Card				Keith Maple	(5 minutes)
4.5 IT Risk Update		✓		Rob Houghton	(10 minutes)
4.6 Cyber Security & Information Assurance Update		✓		Mick Ebsworth / Jules Harris	(5 minutes)

CONFIDENTIAL

POL00401626

Post Office Risk and Compliance Committee Agenda (cont.)

Agenda Item		Action Needed	For ARC	Purpose	Lead	Time
5.	**Risk Update**					
	5.1 Risk Placemat, Including an Update on Risk Exceptions and the Rollout of the Placemat	Questions & Noting	✓	To review progress on the rollout of the Placemat.	Richard Williams / Deana Herley / Ian Holloway / Owen Woodley / Tom Moran / Jonathan Hill	13.50 – 14.20 (20 minutes)
	5.2 Financial Crime Pilot			To review the progress of the pilot.	Ashish Singh / Sally Smith	(10 minutes)
6.	**Internal Audit**					14.20 – 14.35
	6.1 Audit Report	Questions & Noting	✓	To note the Internal Audit Report and Internal Audit Plan for onward submission to the ARC.	Johann Appel	(15 minutes)
	6.2 Audit Plan 2018/19		✓			
7.	**Updates for Noting**					14.35 – 14.55
	7.1 GDPR Programme Update	Questions & noting	✓	To note the GDPR Programme Update.	Clare D'Netto	(10 minutes)
	7.2 Compliance with Payment Card Industry Data Security Standards	Questions & noting	✓	To receive an update on compliance with PCI DSS.	Nicholas Spicer / Jules Harris	(10 minutes)
8.	**Compliance**					14.55 – 15.00
	8.1 Procurement Compliance Reporting	Noting		To review the Procurement Compliance report and forward view.	Barbara Brannon	(5 minutes)
9.	**Policies for Approval**					15.00 – 15.30
	9.1 Treasury Risk Management Framework, Policies and Authorities	Approval	✓	To agree for onward submission to the ARC.	Mark Dixon	(10 minutes)
	9.2 Document Retention and Disposal Policy	Approval	✓	To agree for onward submission to the ARC.	Jules Harris	(10 minutes)
	9.3 IT Security Policy	Approval	✓	To agree for onward submission to the ARC.	Mick Mitchell / Mick Ebsworth	(5 minutes)
	9.4 IT Disaster Recovery Policy	Approval	✓	To agree for onward submission to the ARC.	Mick Mitchell	(5 minutes)

CONFIDENTIAL

POL00401626

Post Office Risk and Compliance Committee Agenda (cont.)

Agenda Item		Action Needed	For ARC	Purpose	Lead	Time
10.	**Business Continuity**					15.30 – 15.50
	10.1 Business Continuity Planning	Noting	✓	To agree the BCP report and Business Continuity Policy for onward submission to the ARC.	Tim Armit	(20 minutes)
	10.2 Business Continuity Policy	Approval	✓			
11.	**Governance**					15.50 – 15.55
	11.1 RCC Effectiveness Review	Noting		To review and agree the committee's performance against its terms of reference.	Chair	(5 minutes)
	11.2 Update on Terms of Reference for RCC / ARC	Noting		Verbal update on a review of the terms of reference.		
12.	**Updates from Subsidiaries**					15.55
	12.1 POMS RCCC Minutes	Noting		To receive the minutes of the POMS RCC meeting held on 31 January 2018.	Chair	
13.	**Any Other Business**				Chair	15.55 – 16.00
	Close					16.00

CONFIDENTIAL

POL00401626

Post Office Limited
Risk and Compliance Committee Meeting

MINUTES OF A MEETING OF THE RISK AND COMPLIANCE COMMITTEE (THE "COMMITTEE") OF POST OFFICE LIMITED (THE "COMPANY") HELD ON 18 JANUARY 2018 AT 20 FINSBURY SREET, LONDON EC2Y 9AQ AT 1.00PM

Present:	Jane MacLeod	Chairman	
	Paula Vennells (PV)	Group Chief Executive	
	Al Cameron (AC)	Chief Financial and Operations Officer	
	Debbie Smith (DS)	Chief Executive, Retail	
	Rob Houghton (RH)	Group Chief Information Officer	
	Martin Kirke (MK)	Group HR Director	
	Mark Davies (MD)	Group Communications, Brand & Corporate Affairs Director	
	Martin Edwards (ME)	Group Strategy Director	
In Attendance:	Johann Appel (JA)	Senior Manager, Internal Audit	
	Ashish Singh (AS)	Interim Head of Risk	
	Owen Woodley (OW)	Managing Director, Post Office Money	
	Jane Fahey (JF)	Deputy Company Secretary	
	Sally Smith (SS)	Head of Financial Crime	3.3
	Jules Harris (JH)	Head of Information Protection and Assurance	*3.8 & 4*
	Clare D'Netto (CDN)	GDPR Programme Manager	*4*
	Chris Russell (CR)	Data Protection Officer	*4*
	Richard Williams (RW)	Senior Risk Manager	*5*
	Barbara Brannon (BB)#	Procurement Director	*6 & 7*
	Ben Foat (BF)	Legal Director	*9*
	Mark Dixon (MD)	Head of Treasury, Tax and Insurance	*11*
Apologies:	Nick Kennett	Chief Executive – Financial Services & Telecoms	

ACTION

by telephone

1. WELCOME, INTRODUCTION AND CONFLICTS OF INTEREST

1.1 The Chairman welcomed DS, Chief Executive, Retail, to the meeting.

2. MINUTES AND ACTION LIST

2.1 Minutes of the meeting of the Board held on 8 November 2017 were approved and authorised for signature by the Chairman.

2.2 The Action List Status Report was noted as accurate. Save for the following, there were no actions due which had not been addressed in advance of the meeting or through the meeting papers:

(a) 1789 – Compliance Requirements: The Chairman advised that discussions were now underway with HMRC on the impact of likely enhanced anti money laundering ("AML") and fit and proper requirements. PV stressed the importance of ensuring this action was

POL00401626

closed by the next meeting; and

(b) 1788 – Financial Crime Risk assessment: The Chairman confirmed that the Financial Crime workshops for Product Managers ("PMs") had been held, however the PMs had yet to complete the follow-up work. **DS agreed to raise the matter with the relevant PMs.** **DS**

3. KEY OPERATIONAL RISKS

3.1 Financial Services Conduct Risk

The Financial Services Conduct Risk Update was noted.

AC highlighted inconsistencies in risk ratings between this report and the Company's financial performance pack presented in other governance forums. The Chairman explained that this was due to lack of alignment in the metrics used to produce the reports and agreed on the importance of consistent reporting.

3.2 Change Risk

The Change Risk Update was noted.

The Chairman advised that Carla Stent, Chairman of the Company's Audit, Risk and Compliance Committee ("ARC") had requested further detail as to the lessons learned from Change activity over the past three years, and a forward view as to where the principal risks would arise. The paper should be updated to reflect this request.

AC invited the Committee to submit any additional comments on the content of the paper to him in advance of the ARC.

SS joined the meeting.

3.3 Financial Crime Risk

SS noted that her report included the Money Laundering Reporting Officer annual review for 2017 which addressed various statutory and regulatory requirements. SS advised that due to the size and complexity of the Post Office network, and the diverse range of products and services provided in both face to face and digital environments, the key financial crime risk control was staff training and awareness. The current training model was inefficient, and while work was underway with Learning and Development to address this, further support from the Group Executive ("GE") and senior leadership population would be required in order to drive completion rates.

RH submitted that it was not sufficient to address this risk through education alone, and that, in order to address the root cause, systems needed to be redesigned to incorporate the right controls. SS responded that no system could entirely address the risk due to the complexity of the network. Therefore, education would remain the key control. PV challenged this, stating that while the issues caused by the network structure were large in scale, they were not necessarily complex. The launch of HGNT would help ensure that agents complied with financial crime-related requirements. In addition, she submitted that there were certain products which should be reviewed to ensure that the benefits they brought to the business outweighed the associated financial crime risk.

In response to a question from DS as to where the legal accountability lay for

POL00401626

financial crime compliance, the Chairman explained that it was her accountability to ensure that there were effective systems and controls to prevent money laundering and counter terrorist financing. However, on a day-to-day basis, responsibility for implementing these controls lay with the business. Training was one aspect of this, as was having processes to ensure products were designed with fraud prevention in mind. Agents were contractually obliged to comply with Post Office rules. She added that twenty agents had recently been suspended for failure to comply with these rules. In response to a further question from DS as to the position of the risk environment, the Chairman clarified that cases of non-compliance were mostly historical. However, as the management information ("MI") in this area had been largely developed over the past two years, it was not possible to provide a definitive, long-term assessment as to whether the risk environment was improving.

SS advised that under requirements introduced during 2017, the Company would be required to demonstrate the fitness and propriety of all agent entities to HMRC. In response to a question from DS as to how compliance with these requirements would be demonstrated, SS explained that this would be achieved through reporting metrics currently under development.

AC queried whether the resourcing and budget required for the recommendations outlined in the paper had been planned for with sufficient detail. JM advised that a detailed project plan had been prepared which was funded to the extent necessary. SS highlighted the importance of ensuring Product Information Packs were complete to demonstrate a full risk assessment. **OW agreed to follow up with the PMs in question.** **OW**

The Committee noted the Money Laundering Reporting Officer's (MLRO) annual report on compliance with The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 and The Terrorism Act 2000, which was included in the report.

SS left the meeting.

3.4 **IT Risk Update**

The IT Risk Update was noted.

3.5 **Financial Reporting Controls**

The Financial Reporting Controls Update was noted.

3.6 **Business Continuity and Crisis Management**

The Business Continuity and Crisis Management update was noted.

In response to a query from AC as to whether sufficient resources were being provided to this crucial area, the Chairman advised that resourcing requirements over the next twelve months were currently under review.

3.7 **Health and Safety**

The Health and Safety Update was noted.

JH joined the meeting.

POL00401626

3.8 **Information Protection and Assurance**

JH introduced the Information Protection and Assurance Update. AC submitted that while the need to improve the management of data was critical, it was important to ensure that all data management needs were consolidated into one programme. In response, the Chairman advised that all programmes related to data were aligned.

RH commented that the control improvement actions to mitigate insider threat and external malicious attack, as detailed in the appendix to the paper, were somewhat vague. He suggested that GE members be assigned responsibility for identifying owners for the various categories of data, and the actions required to increase the Company's maturity level in this area. **JH agreed to develop a draft proposal.** **JH**

MK requested that **the appendix to the paper be amended to reflect the fact that the HR Director was accountable for, rather than the owner of, the Joiners, Movers and Leavers ("JML") programme.** **JH**

PV requested that **the appendix be updated to provide further detail on how the control improvement actions outlined would be applied in practice.** **JH**

CDN and CR joined the meeting.

4. GDPR PROGRAMME UPDATE

The Chairman introduced the General Data Protection Regulation ("GDPR") Update. She advised that a GDPR training session would be provided to the ARC on the 29 January 2018, and that the matters covered in this paper would form the basis of that session.

CDN explained that the GDPR programme had from inception flagged that it was unlikely to achieve full compliance by May 2018. Instead the programme has taken a risk-based approach to achieve 'effective compliance'. New activity would be compliant on or before 15 May 2018. In addition, remediation of existing activities which were high risk/high priority would be completed by May 2018.

RH highlighted that the challenge to achieving effective compliance by the May 2018 deadline was in meeting change lead times. There was still uncertainty as to what needed to be achieved and when, and consequently whether the necessary operational and technical changes could be delivered in time. For those instances where the requirements were known, it was not clear that the programme was progressing sufficiently quickly to deliver them. **He requested that a clear articulation of the "known unknowns" be prepared, including details of the key stakeholders, and where prioritisation calls may be required.** PV challenged this position, querying whether the volume of change required by the programme between now and May, which was incremental to the existing change agenda, was truly significant. The Chairman advised that it was not, with most of the change involving marketing activity. However, remediating legacy issues would take another approximately 12-18 months following the deadline. **CDN/CR**

POL00401626

MK highlighted that there was a lack of awareness of the issues raised by GDPR across the business **and asked the programme team to consider how they could drive understanding.** **CDN/CR**

JH, CDN and CR left the meeting. RW joined the meeting.

5. RISK UPDATE

RW introduced an update on the Risk Placement, including an update on Risk Exceptions. Rollout of the Risk Placemat was on track to be completed by June 2018. Since the November 2017 meeting, the approach had been further rolled-out within Financial Services and Retail. In parallel, a methodology was being created to test the integrity, and formalise the governance framework, of principal risks for post-Placemat implementation.

The Committee reviewed the current Risk Exception Status and commented on the following in particular:

(a) AC advised that an IT solution for the risk of loss of data/service due to the RPA software running on stand-along desktop machines was still being awaited; and

(b) RH advised that he would need to determine the extent to which Salesforce software was being used across the business prior to making any decision on contract renewal. He expressed frustration at the fact the contract was due to expire on 29 April 2018, which did not give sufficient time for transition, should that be determined the correct option. AC commented that while he was aware of the issue, he had not until now been aware of the April deadline. **He would work with Barbara Brannon to ensure early escalation of these matters going forward. PV requested that RH bring a report on the use of Salesforce across the organisation to GE.** If it were concluded that the software was used exclusively by Customer Relationship Managers ("CRMs"), then she was content to carry any risk until the Company's strategy with regard to CRMs was finalised. **BB** **RH**

RW left the meeting. BB joined the meeting.

6. COMPLIANCE

6.1 Procurement Compliance Report

BB presented the Procurement Compliance Report. She reported that since the last meeting in October 2017 there had been a total of seven non-compliant contract awards, with a total value of GBP9,388,000. Three of these were currently pending imminent contract signature. During that period, a number of large value procurements had been completed and brought into compliance, bringing the overall value down from GBP19 million in October 2017 to GBP15 million in January 2018.

The Committee expressed concern at the level of non-compliance detailed in the report. AC queried whether instances of non-compliance were being escalated to the GE in a sufficiently timely manner. The Chairman submitted that there seemed to be a relaxed culture within the business regarding procurement compliance and

POL00401626

that more could be done to address this. BB responded that while there was room for improvement, it was not necessarily a matter of the business being apathetic where compliance was concerned. There were large parts of the business which were very proactive in working with Procurement and who had a clear understanding of their requirements and the lead times involved. However, there were other part of the business who, for a variety of reasons, found articulating their requirements more challenging and therefore decision-making proved difficult. AC reiterated his request that such instances be escalated earlier.

7. POLICIES

7.1 Supplier Relationship Management

BB recalled for the Committee that, in order to help evidence good supplier management, she and the Chairman had been given an action to create a Supplier Relationship Management Policy (the "Policy"). In doing so, they had endeavoured to create an easy-to-follow guide which defined the minimum standards to manage the day-to-day supplier relationship once the supplier is on board and providing services. She explained that between now and the end of March 2018, Procurement would work the business to create supplier relationship terms, and a timetable would be signed off by each GE member as to how mandatory activities would be delivered over the next 12 months. This would involve identifying the tools and systems to evidence that the required degree of oversight existed. The Committee discussed the merits of Traction system, noting that while it would be relatively simple and cost-effective, it did not hold any data, and merely provided a system to acknowledge completion of the tasks assigned. After discussion, it was agreed in principle that Traction be utilised.

Subject **to a request from RH that the policy be amended to standardise role titles**, the Committee approved the policy. It was agreed that the policy did not require further approval by the ARC. **BB**

BB left the meeting.

8. AUDIT

8.1 Internal Audit Report

The Committee noted the Internal Audit Report.

JA advised that reports for four Internal Audit reviews were currently being drafted or cleared through management. These included reviews of compliance with the Banking Framework and AML compliance for MoneyGram. With regard to the Banking Framework review, a number of areas, namely Information Protection, Data Security, and Business Continuity, required significant improvement in order to demonstrate compliance. The Chairman commented that an assumption had been made at the time of signing the Banking Framework that the requirements under the agreement had been clearly communicated to the relevant teams, which had not been the case. However, the changes required to demonstrate compliance were not material. AC stressed the importance of taking the lessons learned from this, **and requested that a copy of the full report be circulated to the Committee.** After discussion, it was agreed that that the **JH**

POL00401626

Banking Framework report should be submitted for consideration at the March 2018 ARC. **PV requested that OW provide his view on the report from a Post Office Money perspective.** **OW**

JA reported that audit actions were generally being completed on time and 107 actions had been completed year to date, which demonstrated an improvement in the cultural approach of the business. As at 31 December 2017, 36 actions remained open, two of which were overdue. These were being tracked closely.

BF joined the meeting.

9. DEEP DIVES

9.1 Annual Legal Risk Review

BF introduced the Annual Legal Risk Review for 2017 (the "Review"). He outlined the main legal risks for Post Office as follows:

(a) Contract Management
Improvements had been made over the last 12 months to the contracts management and procurement processes, through the introduction and enhancement of a number of controls. These included the enhancement of a central repository of contracts utilising the existing Bravo procurement system. However, there remained further work to enforce a compliant culture in the business. AC advised that it had been agreed earlier in the meeting that Traction would be used to assist with overseeing compliance with contractual terms, and that the Review should be updated to include this.
PV challenged the language used in the Review concerning the number of material arrangements in which services were being provided without a written contract in place. While she agreed that it was unacceptable for there to be no written contract in place, the Review did not detail the significant progress that had been made in managing down the number of such contracts. **AC added that the actions being taken to mitigate any risk arising from the remaining cases should also be clearly spelled out.** **BF**

(b) Competition Rules
There needed to be better understanding of the potential implications of commercial activities, such as acquisitions or joint ventures ("JVs"). The legal department ("Legal") had developed Compliance Guidance and FAQs to support operational managers in understanding this risk, together with bespoke training.

(c) Corporate acquisitions and JVs
Corporate M&A knowledge was dependent on a few core individuals. Legal was developing a Corporate Acquisition Checklist and challenge process aimed at enhancing risk management of these projects.

(d) Litigation
As a result of the Postmaster litigation, the recovery of agent losses and prosecutions have become significantly more challenging, thereby

POL00401626

increasing the risk that the deterrent effect of such recovery actions or prosecutions will be diminished. In addition, there was a risk of default judgments due to Legal not being notified of service of proceedings received in the network. Proper communications were required to ensure documents were scanned and emailed to Legal promptly.

(e) Branding and IP Enforcement
While basic controls were in place, such as cease and desist letters, brand infringements largely went unchallenged. Further enhancement could be achieved through a formal process with appropriate funding. PV responded that these cases should be dealt with on a case by case basis. If a significantly serious instance, or increase in infringement cases were seen, Legal should escalate appropriately.

BF advised that Legal's focus for 2018/19 Legal would centre on enhancing the legal maturity of Post Office through the introduction of enhanced controls, and the delivery of further training to assist managers to better understand core areas of legal risk and develop necessary processes.

10. HORIZON SCANNING

10.1 FCA Report –Ageing Populations and Financial Services

The FCA Report on Ageing Populations and Financial Services was noted.

10.2 Legal and Regulatory Horizon Scanning

The Legal and Regulatory Horizon Scanning report was noted.

MD joined the meeting.

11. INTEREST RATE SWAP UNDER NEW POCA CONTRACT

11.1 Mark Dixon recalled for the Committee that at the July 2017 Board meeting the Group CFOO, following ARC approval, was authorised to execute an interest rate swap, if considered advantageous. A paper setting out the rationale for the transaction, an update on pricing, and how to manage the risks associated with swap execution, was subsequently presented to the ARC in September 2017. He reported that as approval had now been received from the Department of Business, Energy and Industrial Strategy and HM Treasury to enter into an interest rate swap for the purposes of hedging its floating rate exposures linked to the POca cash balances, approval would be sought to do so at the upcoming ARC. The current pricing levels for the swap were then outlined.

After discussion, the Committee noted the paper for onward submission to the ARC.

POL00401626

12. PAPERS FOR NOTING

12.1 Minutes from the meetings of the POMS RCC held on 11 October 2017, 29 November 2017 and 19 December 2017 were noted.

12.2 The EUM Programme Update was noted.

12.3 The SuccessFactors Risk Exception Report was noted.

12.4 JM **agreed to circulate an update on Jointers, Movers and Leavers following the meeting.** **JM**

13. ANY OTHER BUSINESS

13.1 There being no other business, the Chairman closed the meeting.

....

Chairman **Date**

POL00401626

POL Risk and Compliance Committee
Action List

Status Report as at: 06/03/2018

Meeting Date	AP ref	ACTION	Action Owner	Due Date	STATUS	Open/ Closed
18/01/2018	**3.3**	**Financial Crime Risk** - The importance of ensuring Product Information Packs were complete to demonstrate a full risk assessment was highlighted. OW agreed to follow up with the PMs in question.	Owen Woodley	13/03/2018		Open
18/01/2018	**4**	**GDPR Programme Update -** (a) A clear articulation of the Programme's "known unknowns" to be prepared, including details of the key stakeholders, and where prioritisation calls may be required. (b) The Programme team to consider how they could drive understanding of the issues raised by GDPR across	Clare D'Netto	13/03/2018		Open
18/01/2018	**8.1**	**Internal Audit Report** - Owen Woodley to provide his view on the Banking Framework Report from a Post Office Money perspective.	Owen Woodley	13/03/2018		Open
18/01/2018	**9.1**	**Annual Legal Risk Review** - the actions being taken to mitigate any risk arising from the remaining cases (of material arrangements in which services were being provided without a written contract in place) to be clearly spelled out in the Review.	Ben Foat	13/03/2018		Open
08/11/2017	**1801**	**Business continuity testing** - Test Bolton before the implementation of SuccessFactors and Chesterfield by the financial year end	Tim Armit	02/05/2018	Bolton to be tested by end of April 2018.	To close
08/11/2017	**1800(b)**	**IT DR plans** - Provide an update on IT Disaster Recovery plans	Mick Mitchell	02/05/2018	Included in March agenda.	To close
13/09/2017	**1789**	**Compliance requirements -**Discuss impact of likely enhanced AML & fit & proper requirements with the relevant stakeholders in Government	Jane MacLeod/ Patrick Bourke/ Mark Davies	13/03/2018 (next update)	In light of the new challenges from HMRC regarding retention of customer ID, together with Patrick Bourke we are looking to set up stakeholder meetings with HMRC shortly.	To close
20/07/2017	**1781**	**Insurance Distribution Directive -** Provide a briefing on the potential training requirements of the IDD in order to consider the future compliance burden against capacity in the branch network	Jonathan Hill	18/01/2017	Update at November RCC: Network and Learning team currently looking at this. Will have a year to implement. Update on progress due at January RCC.	Open
09/03/2017	**1773**	**RCC Terms of Reference** - to be reviewed and updated based on changes in PO structure	Jane MacLeod	13/03/2017	Verbal discussion at March meeeting.	To close

POL00401626

Actions Update

Author: Company Secretariat Meeting date: 13 March 2018

Executive Summary

Context

Further to the actions list published with the Risk and Compliance Committee agenda on 7 March 2018 supplementary information has been supplied. Accordingly an updated actions list is provided for the committee's reference.

Input Sought

1. The committee is asked to review the revised actions list and comment on the updates contained therein.

Appendices

1. Risk and Compliance Committee Actions List Updated 12 March 2018
2. GDPR Programme Update in Response to Action 4

POL00401626

1. Risk and Compliance Committee Actions List Updated 12 March 2018

Meeting Date	AP ref	ACTION	Action Owner	Due Date	STATUS	Open/ Closed
18/01/2018	**3.3**	**Financial Crime Risk** - The importance of ensuring Product Information Packs were complete to demonstrate a full risk assessment was highlighted. OW agreed to follow up with the PMs in question.	Owen Woodley	13/03/2018	Packs have been completed.	To close
18/01/2018	**4**	**GDPR Programme Update** (a) A clear articulation of the Programme's "known unknowns" to be prepared, including details of the key stakeholders, and where prioritisation calls may be required. (b) The Programme team to consider how they could drive understanding of the issues raised by GDPR across the business.	Clare D'Netto	13/03/2018	The GDPR Programme Manager has provided an overview of the known unknowns and actions to drive understanding which is annexed to this actions tracker.	To close
18/01/2018	**8.1**	**Internal Audit Report** - Owen Woodley to provide his view on the Banking Framework Report from a Post Office Money perspective**.**	Owen Woodley	13/03/2018	Owen had a look at the report and did not have anything further to add.	To close
18/01/2018	**9.1**	**Annual Legal Risk Review** - The actions being taken to mitigate any risk arising from the remaining cases (of material arrangements in which services were being provided without a written contract in place) to be clearly spelled out in the Review.	Ben Foat	13/03/2018		Open
08/11/2017	**1801**	**Business Continuity Testing** - Test Bolton before the implementation of SuccessFactors and Chesterfield by the financial year end.	Tim Armit	02/05/2018	Bolton to be tested by end of April 2018.	To close
08/11/2017	**1800(b)**	**IT DR plans** - Provide an update on IT Disaster Recovery plans.	Mick Mitchell	02/05/2018	Included in March agenda.	To close
13/09/2017	**1789**	**Compliance requirements -** Discuss impact of likely enhanced AML & fit & proper requirements with the relevant stakeholders in Government.	Jane MacLeod/ Patrick Bourke/ Mark Davies	13/03/2018 (next update)	In light of the new challenges from HMRC regarding retention of customer ID, together with Patrick Bourke we are looking to set up stakeholder meetings with HMRC shortly.	To close
20/07/2017	**1781**	**Insurance Distribution Directive -** Provide a briefing on the potential training requirements of the IDD in order to consider the future compliance burden against capacity in the branch network.	Jonathan Hill	18/01/2017	Update at November RCC: Network and Learning team currently looking at this. Will have a year to implement. Update on progress due at January RCC.	Open
09/03/2017	**1773**	**RCC Terms of Reference** - to be reviewed and updated based on changes in PO structure.	Jane MacLeod	13/03/2017	Verbal discussion at March meeting.	To close

POL00401626

2. GDPR Programme Update in Response to Action 4

Known/Unknowns	Impact & decision	Stakeholders	Actions to drive understanding
IT Remediation costs for suppliers to comply with the updated DP clauses and security standards	Cost – potential impact on agreed budget for 2018/19	CIO / Systems Owners	1. Requires an accurate/documented view of the personal data processes and relevant controls, including the ability /processes to delete data. ○ *The Programme is experiencing blockers to getting this from IT suppliers. This has been well documented via the programme governance. The remediation is that the Programme Director and Systems PM are going to focus on a couple of key suppliers to understand how we can remove these.* 2. Contracts updated with the DP clauses and schedules including the Schedule of Processing and Security Schedule (by May 2018). ○ *A process for Assurance will be established by May 2018 which will result in gaps for remediation being identified which will continue beyond May 2018.*
Costs of data deletion to complete with retention schedules	Cost – as above	CIO / Systems owners	1. PO's Document Retention policy and retention schedules is currently outside scope of the GDPR Programme and is a key dependency. Therefore a business case will be raised via the GDPR programme to address this. • *The programme is currently assessing the existing processes and capability for suppliers to delete data when this comes into force.*
Unstructured data We don't know where all the unstructured data is on POL, POMS and suppliers systems	Scope & cost	CIO / Business Owners	1. Work with suppliers to identify the location of the data on their systems. We have asked this via the original questionnaire but information received is incomplete. IT help required to push this forward and this may incur a cost – see above. 2. The Business Functions work stream is assessing where this is on PO systems – for high risk areas. 3. POL could invest in a tool to search for data and delete based on a POL retention policy (see above re: dependency), but cost is dependent on the size of the data if unknown. 4. Education will be key, so data will be on One Drive and Share-point otherwise we can't scan and delete.
Suppliers Information on Bravo is out of date and incomplete so we know we don't know all the contracts, including non-IT suppliers, software licences and this will impact on our ability to remediate contracts and but also puts us at risk as a result of our failure to maintain an up to date inventory and / or if there is a data breach for an unidentified vendor.	Scope	Contract Owners	1. Email going out to GE/GE-1 on 12/3 to identify a single point of contact to help us pick up some of the smaller contracts, not currently held on Bravo or visible to the Team. 2. The Programme is also working with IT and Procurement on this, however there will be a requirement for tighter controls for new IT vendors and software in BAU. 3. We have engaged a Contract PM who will drive this forward.

POL00401626

Financial Reporting Controls

Author: Danielle Goddard Sponsors: Micheal Passmore, Al Cameron Date: 13 March 2018

Executive Summary

Context

The purpose of this paper is to update the RCC on the status of the Financial Reporting Controls Framework (the FRC), the most recent control self-assessment results (January 2018), current areas of focus, and the progress made on the second phase of the project.

Questions addressed in this report

1. What is the current status of the FRC?
2. What testing is being performed over the FRC?
3. What is the status of the additional scope of the FRC?
4. What other controls changes are being implemented?
5. What actions are being taken in response to the control points raised in EY's FY16/17 audit report?
6. What additional work is planned for FY17/18 year end?

Conclusions

Current status of the FRC
The number of controls has increased from 303 at end December 2017, to 326 at end January 2018. Most of the increase relates to 18 new controls over Success Factors (after the January go live). The framework continues to be self-assessed on a monthly basis within the TrAction online self-assessment tool and results are monitored.

Of the 326 controls at end January 2018, 255 (78%) were issued for self-assessment. 250 (98% of those issued for self-assessment) were operating effectively. Of the remaining 5 controls, 2 related to new controls where work is required to formalise the evidence of the control for the next self-assessment, 1 relates to a monthly process and risk review which will be completed for the next self-assessment due to a change in ownership, and the remaining 2 are under review with the control owners.

Of the 71 controls not issued for self-assessment at the end of November, 59 were not due to be operated in the period. The remaining 12 controls were in remediation, with workaround controls in place or remediation in progress.

PwC's comments over spreadsheet controls have been fully implemented.

Strictly Confidential

POL00401626

Testing performed
Internal sample testing is now being performed by the FRC team; 186 controls have been tested to date, the results are detailed within section 2.2 of this paper. Of the 186 controls tested, 148 were operating effectively, 18 had insufficient evidence, 13 were not operating effectively, and 7 were in remediation. All 13 ineffective controls have since been remediated, and 15 of the 18 with insufficient evidence have been resolved (with the remaining 3 in progress). In addition to this, communications have been issued to remind control owners how to appropriately evidence controls in line with best practice.

PwC began further independent testing in February and are currently finalising the results of the 74 controls they selected for testing.

EY selected 33 controls to walkthrough, and are in the process of testing those which they can rely on for audit purposes.

Additional scope of the FRC
5 Masterdata processes are complete, the 9 remaining Masterdata processes are expected to be complete by end June 2018 (extended from May 2018 due to recent work over Success Factors, ART and CWC Masterdata).

FSC Transaction Correction controls are now being self-assessed on a monthly basis; further work commenced in March to analyse the balance sheet accounts relevant to FSC, and to ensure that the appropriate in-depth reconciliations and controls are in place.

Other controls changes and improvements
18 new controls have been added to the self-assessment process in relation to Success Factors. There are still some control recommendations being closed in relation to Success Factors; these will be complete by the year end or workaround controls in place where necessary.

Interim controls continue to operate over POLSAP journals. Work is being performed as part of Back Office Transformation ('BOT') to ensure that strong automated controls are in place once POLSAP processes migrate into CFS.

A full cash count is planned for Belfast cash centre at transition from POLSAP to CWC. There was a full cash count performed at all cash centres in February; the Glasgow and London counts are required to be re-performed, this is planned for March 2018 and Finance will attend both locations.

Closure of the FY16/17 control points raised by EY is in progress. Progress against each item is detailed in Appendix 2 of this paper.

Input Sought

The RCC is asked to note the progress made and comment on the priorities.

POL00401626

The Report

1. What is the current status of the FRC?

1.1 The FRC is self-assessed by control owners on a monthly basis, with results monitored by the FRC Manager. The table below summarises compliance in January 2018.

January 2018 - Total controls	**326**	
Less: Controls in remediation	(12)	
Controls not due to be operated due to frequency	(59)	
Total population for self-assessment	**255**	**78%**
Self-assessed and operated effectively	250	98%
Self-assessed but not operated effectively	5	2%
No self-assessment submitted	0	0%

1.2 The total number of controls continues to expand for changes and improvements in processes, and the additional scope of the project. 29 incremental controls have been added, and 6 controls removed since the last update to RCC; the new controls relate to 18 controls over Success Factors (after the January go live), and 11 other new controls.

1.3 Of the 326 controls at end January 2018, 255 (78%) were issued for self-assessment. 250 (98% of those issued for self-assessment) were operating effectively. Of the remaining 5 controls, 2 related to new controls where work is required to formalise the control or control evidence for the next self-assessment, 1 relates to a monthly process and risk review which will be completed for the next self-assessment due to a change in ownership, and the remaining 2 are under review with control owners.

1.4 Of the 71 controls not issued for self-assessment at the end of January, 59 were not due to be operated in the period. The remaining 12 controls were in remediation; remediation is expected to be complete by year end except where reliant on BOT implementation (although workaround controls are in place where this is the case).

1.5 The implementation of PwC's recommendations over spreadsheet controls is now fully complete and a sample review control will be performed going forwards. The recommendations related to the implementation of a summary control sheet, separation of inputs and outputs, and password protection; these have been applied across the full population of critical spreadsheets.

POL00401626

2. What testing is being performed over the FRC?

2.1 Internal sample testing of controls is being performed by the FRC team. 186 controls have been tested to date. Of these 186, 148 (80%) were 'green' (control operating effectively), 18 (10%) were 'amber' (deemed to be operating effectively but not appropriately evidenced), 13 (7%) were 'red' (not operating effectively), and 7 (4%) were in remediation. The testing results by process are summarised below.

2.2 All 13 red controls have since been remediated and now deemed as operating effectively. Of the 18 amber controls, 15 are now deemed as being evidenced appropriately and the remaining 3 are being followed up. In addition to this, communications have been issued to remind control owners how to appropriately evidence controls with examples of best practice.

Process	Controls tested	Control in remediation	Controls operating effectively	Controls with insufficient evidence for audit purposes	Controls not operating effectively
Bank & Cash Management	27	0	23	4	0
Bill To Cash	13	0	13	0	0
Client Settlement	1	1	0	0	0
Fixed Assets	17	2	7	6	2
Payroll	44	0	39	3	2
Procure To Pay	16	0	14	2	0
Project Accounting	5	0	2	0	3
Record To Report	33	0	27	2	4
Settlement Process	10	1	9	0	0
Stock	2	0	2	0	0
Tax	12	3	6	1	2
Treasury	6	0	6	0	0
Total	**186**	**7**	**148**	**18**	**13**

2.3 PwC are performing further independent testing of the controls framework and have selected a sample of 74 controls for testing. The sample selected includes controls from each process; some of the controls selected have been internally tested by the FRC team. PwC are currently completing their testing and will report their results in due course.

2.4 As part of the external audit, EY were provided with a list of key controls from the framework. EY selected 33 controls to walkthrough and are in the process of testing those which they can rely on for audit purposes.

POL00401626

3. What is the status of the additional scope of the FRC?

3.1 The scope of the FRC was extended to cover; Masterdata, Finance Service Centre ('FSC') processes, Agents' Debt, Agents' Remuneration, Cash Management and Forecasting, and POMS.

3.2 5 Masterdata processes have now been completed. Vendor, Customer, GL, Payroll and Employee Masterdata controls are in TrAction being self-assessed on a monthly basis. The remaining 9 Masterdata processes are expected to be complete by end June 2018 (extended from May 2018 due to recent work over Success Factors, ART and CWC Masterdata).

3.3 Key controls over the FSC Transaction Correction process are now part of the monthly self-assessment process. An additional piece of work commenced in March to analyse the FSC balance sheet accounts; this will include mapping the balance sheet accounts back to the relevant FSC process and ensuring that risks and controls have been documented for each of these processes, and alongside this reviewing the balance sheet reconciliations in place to ensure completeness and robustness.

3.4 Mapping of risks and controls over the Agents' Debt process has also commenced in March.

4. What other controls changes are being implemented?

4.1 Interim authorisation controls continue to operate over POLSAP journals. A monthly 10% sample check is performed; one exception was noted for January 2018 and retrospective authorisation is being obtained. Work is being performed to develop automated controls as part of BOT (refer to section 4.5.5 of this paper).

4.2 A bi-annual full cash count (at all cash centres) control has been added to the framework. Cash count instructions and templates have been issued by Finance to the cash centre managers.

4.3 Full cash counts took place at all cash centres in February 2018; with Finance attendance at Birmingham and external audit attendance at London and Glasgow. It has been deemed necessary for London and Glasgow to re-perform their counts, as counts were completed prior to the time that external audit were advised to arrive on site. The counts have been rescheduled for 16 and 17 March 2018 and for both sites a Finance representative and external audit representative will attend.

4.4 Work is in progress over Fixed Asset controls, including a review of all AUCs >£500k to ensure that no material live projects remain in AUC. This is substantially complete and will be fully complete for end March 2018. A quarterly review will be implemented going forwards. Further work is being performed to ensure appropriate controls over additions, disposals and physical verification prior to year end.

POL00401626

4.5 There are a number of projects which the FRC team have engaged with to ensure existing controls are adapted or new controls are documented:

4.5.1 New controls have been documented over the new HR system Success Factors which went live in January 2018; 18 new controls were live for the January self-assessment, and 8 existing controls were adapted. A number of IT General Controls have also been documented in respect of Success Factors, which have been reviewed by the IT Controls team for inclusion within the IT Controls Framework.

4.5.2 31 new controls have also been documented in respect of Agent Remuneration Transformation ('ART'); these have been loaded into TrAction to be performed for the February self-assessment (performed in March).

4.5.3 Review of CWC controls is still in progress; there are a number of outstanding controls actions which are expected to be completed during March 2018. Some lower risk outstanding actions will remain for completion by June 2018 go live.

4.5.4 The Back Office Transformation team continue to work closely with the FRC team to ensure an appropriate control environment is in place over all process changes and migrated processes. Business process documents and control matrices are being reviewed and signed off by the relevant business owners, the FRC team and the Finance Director, POL.

4.5.5 The FRC team are engaged in the building of automated user access controls in CFS; this will minimise the user access risk when POLSAP processes are migrated to CFS. The BOT team are performing the analysis required to design these user access controls so that they can be formally signed off and built prior to go live in June 2018. The controls will ensure that all manual journals are centrally processed where possible, and there is a closed environment for any manual transactions which cannot be centralised (e.g. transaction corrections, file uploads, settlements, and other high volume processes which are transitioning from POLSAP to CFS).

5. What actions are being taken in response to the control points raised in EY's FY16/17 audit report?

5.1 Actions and deadlines are being tracked for each Management Letter Point raised by EY (refer to Appendix 2). A detailed status update is included in Appendix 2.

5.2 All items are expected to be completed prior to end March 2018 with the exception of item 2.18 which cannot be resolved until Back Office Transformation go live.

5.3 There are three items which are behind target but are expected to be completed by year end:

5.3.1 Item 2.8 Bill payments revenue; the required analysis has been performed to determine the correct income accrual required. A paper was provided to EY at

POL00401626

the prior year end and this is currently being updated to reflect the current position. This is expected to be resolved by end March.

5.3.2 Item 2.19 Management of SAP privilege accounts; EY recommended changes to two specific SAP privilege accounts. The DDIC account has been locked by Accenture as recommended, however the TMSADM account password has not been changed as Accenture have advised against this; this will be discussed with EY prior to end March.

5.3.3 Item 2.20 Changes approval; the IT team have discussed with Atos the evidence retained for changes that require CAB approval, and we believe this is sufficient evidence of approval. A discussion will be held with the EY IT audit team before end March 2018.

6. What additional work is planned for FY17/18 year end?

6.6 The following work is in progress or planned to be performed for FY17/18 year end:

6.6.1 Finance Directors have been notified that their Balance Sheet review files for P11 and P12 should include auditable evidence to accompany the reconciliations for any line item >£250k; the evidence will be reviewed centrally and questioned appropriately P11 and P12 Balance Sheet review meetings.

6.6.2 Annual controls are being performed prior to year end where they are not specific to P12, in order to identify any potential issues and allow internal testing of annual controls prior to year end.

6.6.3 Cut-off reminders have been issued to Finance prior to year end, and teams will be reminded of this in the Balance Sheet review meetings. Unrecorded liabilities review will be performed in the weeks prior to and after the year end date.

POL00401626

Appendix 1 – January 2018 CSA results by process

Controls		Control Gaps				Control Owners		January 2018 CSA Results (submitted February 2018)				
Process	Total controls	Control gaps	H/M/L risk gaps			Owner Assigned	No owner assigned	Controls operated effectively	No self assessment submitted	Not operated due to agreed frequency	Self-assessment submitted but control not operated	Controls to be set to live
			H	M	L							
Bank & Cash Management	31	0	0	0	0	31	0	31	0	0	0	0
Bill To Cash	41	0	0	0	0	41	0	34	0	5	2	0
Control Environment	38	2	0	1	1	38	0	30	0	4	2	0
Fixed Assets	22	2	0	0	2	22	0	17	0	3	0	0
Payroll	64	0	0	0	0	64	0	57	0	7	0	0
Procure To Pay	27	0	0	0	0	27	0	18	0	9	0	0
Project Accounting	10	1	0	1	0	10	0	5	0	4	0	0
Record To Report	44	5	0	4	1	44	0	24	0	14	1	0
Settlement Process	16	1	0	0	1	16	0	10	0	5	0	0
Stock	5	1	0	1	0	5	0	4	0	0	0	0
Tax	20	0	0	0	0	20	0	12	0	8	0	0
Treasury	8	0	0	0	0	8	0	8	0	0	0	0
	326	**12**	0	7	5	**326**	**0**	**250**	**0**	**59**	**5**	**0**

POL00401626

Appendix 2 – Status of EY control findings from FY16/17 audit

Observation		Control issue	Business efficiency	Priority	POL Owner(s)	POL deadline	Status	Comments
2.1.	Assets under construction project monitoring	✓	✓	High	Tom Woodhouse	25-Mar-18	In progress	An AUC review is substantially complete, and is expected to be fully complete by end March 2018.
2.2.	Asset under construction additions	✓	✓	High	Tom Woodhouse	25-Mar-18	In progress	The AUC review will be performed quarterly from end March 2018.
2.3.	Fixed asset disposals	✓	✓	Medium	Tom Woodhouse	25-Mar-18	In progress	The business case template has been updated to identify disposals. A review of the masterplan report is in progress in order to identify branch closures and assess completeness of disposals; this will be complete by end March 2018.
2.4.	Ongoing management of the FAR		✓	Medium	Tom Woodhouse	25-Mar-18	In progress	Accenture have been engaged to assist with processing bulk changes through the SAP asset register. There has been delay due to system restraints but this is expected to be complete for year end.
2.5.	Branch postcodes		✓	High	Tom Woodhouse	25-Mar-18	In progress	A review of the different sources of data is in progress.
2.6.	Revenue commission rates	✓	✓	High	Danielle Goddard	31-Jan-18	Complete	Product manager review of all billing rates has been co-ordinated by Finance and is complete; this exercise will be performed quarterly from end March 2018.
2.7.	Revenue third party information		✓	High	Danielle Goddard	25-Mar-18	Complete	A third party audit control is now live; three third party audit visits have been performed to date and a plan for FY18/19 is currently being drafted.
2.8.	Bill payments revenue	✓		High	Danielle Goddard	28-Feb-18	In progress	Calculations have been completed and a paper is currently being drafted for external audit.
2.9.	Network cash internal audit	✓		High	Russell Hancock, Danielle Goddard	31-Jan-18	Complete	Cash counts were held in February 2018 at all cash centres with instructions and templates issued by Finance, and Finance attendance at one site. Reperformance of counts for Glasgow and London will take place in March 2018 with Finance attendance at both. A plan is in place for future bi-annual counts; Finance oversight and attendance will continue.
2.10.	Network cash counts	✓		High	Russell Hancock, Danielle Goddard	31-Jan-18	Complete	See comments above regarding Finance attendance at cash counts. A policy regarding sealed cages has been included in the count instructions.
2.11.	Pension discount rate		✓	Medium	Micheal Passmore	25-Mar-18	In progress	Pension assumptions will be discussed in March 2018; planning meetings have been held with external advisors in line with normal year end procedures.
2.12.	Financial statements preparation		✓	Low	Danielle Goddard	25-Mar-18	Complete	A new Sharepoint site (with restricted access) has been set up and all FY16/17 and FY17/18 support to date has been saved here.
2.13.	New accounting standards		✓	High	Briony Tristram	25-Mar-18	Complete	Initial report has been submitted to the ARC and discussions will be held with external audit as part of their audit requests. Project is in progress.
2.14.	Timely deactivation of leavers' accounts	✓		High	Matthew Warren, Tracy Wilkes	31-Jan-18	Complete	Weekly leavers control is now being evidenced.
2.15.	Approval of third party created user accounts	✓		High	Matthew Warren, Tracy Wilkes	25-Mar-18	Complete	Steria have been instructed not to create new user accounts without POL approval; a sample check has been performed with no issues noted.
2.16.	Improvement in the periodic user access review process	✓		Medium	Matthew Warren, Tracy Wilkes	25-Mar-18	In progress	Two bi-annual user reviews will have been completed by end March 2018.
2.17.	Segregation of incompatible duties within the manage change process	✓		Medium	Rebecca Barker	25-Mar-18	In progress	This is under review as part of the IT Controls Framework.
2.18.	Direct access to make changes to SAP - SCC4 security settings	✓		Medium	Max Jacobi	30-Jun-18	In progress	This is expected to be resolved after BOT implementation.
2.19.	Management of SAP privilege accounts	✓		Medium	Matthew Warren	31-Jan-18	In progress	EY's recommendations have been discussed with Accenture; the DDIC account has been locked as advised. Accenture have advised that changing the TMSADM password is not advised as it could affect service; this will be discussed with EY in March 2018.
2.20.	Changes approval		✓	Medium	Rebecca Barker, Max Jacobi	28-Feb-18	In progress	Evidence of change approval is being maintained through the CAB process; this process will be discussed with EY prior to year end.
2.21.	Audit of third party providers		✓	Low	Rebecca Barker	28-Feb-18	Complete	EY's recommendation has been noted for any future contract negotiations.

POL00401626

Financial Services Conduct Risk Update

Author: Jonathan Hill

Meeting date: 13 March 2018

Executive Summary

Context

1. This paper updates the Committee on current risks and actions in respect of conduct risk. One of the key risks on the FS Risk register (also reflected in the Post Office and POMS risk registers) relate to conduct risk. Conduct risk in the regulated financial services context refers to risks to customers from poor product design, distribution and selling processes as well as those risks relating to poor product fulfilment.

Questions this paper addresses

2. This paper provides an update on the key conduct risks and how they are being managed.

Conclusions

3. Conduct risk is within risk appetite. The February BoI risk dashboard highlights 17 green, 4 amber and 1 red rating on its dashboard. For POMS the data reported in February was 16 green, 0 amber and 3 red.
4. The common red rating theme from POMS and BoI identified through mystery shops is that colleagues are not following the approved introductory processes. Separately POMS had a red metric for a higher incidence of upheld complaints because of issues surrounding delivering the free £50 gift card for Over 50s Life cover but this is outside of Post Office's control.

Input Sought

5. The Committee is asked to note these developments.

POL00401626

The Report

Key risks, governance and management information

6. Conduct risks are measured and reviewed by FS&T Risk together with our Principals on an on-going basis and management information is provided on the key risk areas. These are reviewed at the BoI-Post Office Customer and Conduct Risk Committee (CCRC) and POMS-Post Office Joint Compliance Committee (JCC), which meet monthly.
7. In the new financial year Post Office FS&T Risk will be working with BoI, POMS and the LRG team to take on and further develop the dashboards as the first line for Conduct Risk.

Current risks and issues

Mystery Shops

8. FS&T Risk has undertaken counter mystery shops of FS products. This has highlighted a failure in branches to follow the introductory sales processes.
9. Encouragingly, close to 100% of our shopping results confirmed that the mystery shopper was not pressurised to take out a product 'there and then'. The shopper was given time to read the product literature.
10. We are taking the product managers and training team through our findings so they can understand which areas need improving so that the introduction/sales process is as easy as possible to follow, whether this be via a Post Office counter or a tablet.
11. A key conformance weakness in the sales process is the provision of the 'summary box leaflet' with each savings application. We are deploying series of activities to help improve this performance. This includes reducing the number of different savings packs (with improved designs), improving the ordering processes for branch savings materials, monthly communications and working with the BoI Business Controls Team to help support conformance.

Out of date product literature in branch

12. We have identified that there is a high frequency of 'out of date' product literature out in branch or behind the counter available to give to customers.
13. FS&T Risk have been working with Network and Supply Chain (including the branch user forum) on solutions. The key actions taken include updated communications through a new branch focus article supported by an updated monthly checklist to enable branches to understand all the FS literature that is current. This has received good feedback from the network.
14. We are also piloting a new branch checklist to be deployed by the end of March for Branch Managers/Postmasters to use, working with the Network Gateway team.

Vulnerable Customers

15. The Post Office ARC approved the updated Vulnerable Customers policy in September 2018, with both Kevin Gilliland and Nick Kennett sponsoring and Tom

POL00401626

Wechsler and Jonathan Hill as policy owners. The policy recognises that Post Office already does a large amount to support vulnerable customers (and there are many examples in the 'One' communications). Nevertheless we have challenged ourselves to identify gaps and possible solutions.

16. A key area of our work has been to listen to key stakeholders and, in liaison with the Public Affairs team, we have linked up with Mind, Age UK, Sense and the Alzheimer's Society. We have also liaised with BoI and UK Finance (including joining two of their working groups on vulnerability) and reviewed FCA/Ofcom guidance as vulnerability is a key focus area for the regulators.

17. To date we have not identified any large gaps in our approach but there are always potential areas of improvement we can consider. For example:

- POMS is developing dementia training for its Glasgow contact centre, working with the Alzheimer's Society.
- We have asked the Alzheimer's Society to review Post Office Vulnerable Customers training that we include in various training courses to give feedback on how this could be improved
- We are looking at how we as an organisation/individuals might be able to become a Alzheimer's Society "Dementia Friend" and also what support we can give to our own people impacted by dementia.
- We need to improve our website to better organise the current vulnerability information, strengthen information on how to avoid scams and publish our vulnerability approach to meet Ofcom vulnerability requirements
- Sense has offered a resource to 'road-test' new propositions such as the customer hub
- Operational improvements have been identified to the provision of alternative forms of product information e.g., type talk, large print information

18. We will conclude the full report for the May RCC and ARC.

Regulatory agenda items previously highlighted.

Insurance Distribution Directive

19. This key piece of legislation will come into force on 1st October 2018. This covers a number of key requirements including:

- New disclosure wording requirements,
- A customer's best interest rule and
- A requirement to demonstrate that those involved or overseeing insurance mediation can demonstrate competence and are trained with 15 hours of CPD.
- POMS is driving the project on this which will require wide FS&T Risk and Network engagement.

Further FCA Consultation Papers on Senior Manager and Certification Regime (SM&CR).

20. The FCA released three Consultation Papers (CPs) in December covering this topic with the implementation timetable still unclear for intermediaries such as POMS. In previous papers the FCA had acknowledged that SM&CR did not apply to ARs, but said it would bring out a further CP covering ARs. However, in these CPs the FCA states that the regime will not apply to ARs. This is because the FCA has acknowledged the Financial Services Act 2016 does not give it the powers to do this.

POL00401626

21. Therefore, the responsibility rests with the Principal firm to ensure the activities of the AR remain compliant. POMS is driving a project to implement these requirements, supported by Post Office HR and FS&T Risk.

FCA Mission Our Future Approach to Consumers Paper (issued November 2017)

22. The FCA outlines its mission in respect of consumers, recognising the changes in technology and the characteristics and changing demographics of consumers. In all markets the FCA wants to see consumers being able to access the products they need, for the market to deliver high quality good value products and services and for there to be financial inclusion. But the FCA recognises that it does not have the mandate to ensure access to financial services for all but it will intervene under its public sector equality duty if it sees discrimination against vulnerable customers.

23. It aims for partnership working with the industry and others to achieve its objectives recognising that in some areas (such as vulnerable customers) it has been able to make good progress with industry engagement rather than rules and regulation.

FCA Financial Lives Study 2017-issued October 2017

24. Based on nearly 13,000 face-to-face and online interviews, Financial Lives is the regulator's tracking survey on consumers and finance. The paper can provide some useful data on our key markets and the challenges that might be raised by the FCA in the future. This paper has been shared with the Post Office Money team

FCA published findings from the Ageing Population Project-Occasional Paper no 31 issued September 2017

25. A report was provide at the previous committee

FCA focus on culture and performance management guidance.

26. This is an ongoing theme in the FCA's business plan and regulatory approach to ensure an appropriate customer centric culture is embedded in firms.

General Data Protection Regulation

27. The General Data Protection Regulation (GDPR) ushers in an enhanced legal regime for the collection, processing and storage of personal data from 25th May 2018. A comprehensive risk review and programme is underway in Post Office, with appropriate training being provided to personnel. The Post Office and BoI GDPR teams are working together.

FCA Strategic Review of Retail Banking

28. Further to the FCA's review, it is now seeking to improve its understanding of the state of competition and conduct in retail banking markets at a pivotal time of change. We await first publication of the information in mid-August 2018.

Jonathan Hill
Head of FS&T Risk & Regulation

POL00401626

BOI Post Office Money branch distribution - February 2018

Risk ratings

January risk ratings and how they compared to December

Red rated MS shops	▲
Red rated CRM shops	◀▶
Red rated counter shops	◀▶
Black rated MS shops	◀▶
MS mutiple red/black shops	◀▶
A or B rated mortgage cases	◀▶
D rated mortgage cases	◀▶
MS meeting QAT benchmark	◀▶
Distribution complaints	◀▶
Mis-selling complaints	◀▶
Conduct survey results	▼
Mystery shopper experience	◀▶
NPS survey results	
Branch product knowledge	◀▶
Branch regulatory knowledge	◀▶
Specialist/CRM knowledge	◀▶
Branch advertising reviews	▲
Advertising compliance issues	▲
Social media compliance issues	◀▶
Savings cancellations	◀▶
Competent specialists	◀▶
Supervisor spans of control	◀▶
BOI supervisor reviews	◀▶

Performance measured in January

Risk ring and overall performance rating



Based on the weighted cumulative outcome of the KRIs we measured in January, the overall risk rating is Amber.

Green rated KRIs



Amber rated KRIs



Red rated KRIs



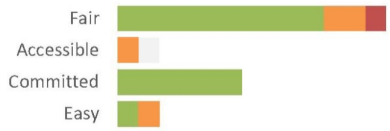
This month we were within tolerance for 21 out of the 22 KRIs we measured. 17 of our KRIs were rated green and 4 of our KRIs were rated amber. One of our KRIs was rated red. In comparison, in December we exceeded tolerance in 2 of our KRIs and in November we exceeded 3 of our tolerances. On average, in each month between August and January, we were within tolerance in 20 of the KRIs we measured and exceeded tolerance in 2.

January v December ratings

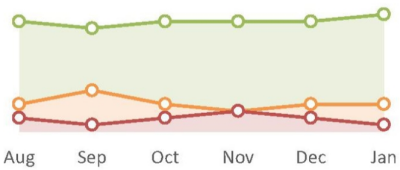
◀▶	15
◀▶	2
◀▶	1
▲	2
▲▼	2
▼	0

One KRI remained red, one KRI moved out of red and no KRIs fell to red.

Performance against our FACE commitments



Distribution of KRI risk ratings between August 2017 and January 2018



Exceptions and key trends

CRM mystery shops - Savings shops are still resulting in red ratings, with 9 out of 52 (17.3%) being red rated in the 3 months to the end of January 2018. This rate has remained steady over the previous 3 months. A detailed action plan was submitted to C&CRC at the January 2018 meeting and will continue to be monitored.

Counter shops - The Red rated KRI relates to counter-staff savings mystery shops completed across the DMB, agency and multiple networks by both BOI and Aba during the three months ending January 2018. 26 of the 59 shops completed (44.1%) were rated red. The shops related to introductory conversations and the red ratings were caused by staff making comments or taking actions which could have been deemed as suggesting the suitability of a particular course of action and/or failing to provide a summary box leaflet.POL have prepared a detailed breakdown of the MI which is due to be presented to C&CRC in February with recommended actions included. A targeted campaign of counter mystery shops has since been planned for early 2018.

Branch Advertising Reviews - Whilst only one BOI branch review was rated 'red' in January 2018 for displaying out-of-date marketing literature and/or not following display instructions, POL continue to investigate what process and control improvements could be made to ensure out-of-date literature is less likely to remain in the public domain across the network. There was one material financial promotion issue recorded in January in relation to the online Summary Box Leaflet which was published with an old approval number displayed. There was one in-branch social media breach, where a branch uploaded details of a credit card offer without the corresponding link to T&Cs.

Conduct Survey Calls - Due to the low volume of calls made in Jnauary (5), the data has been skewed. No new issues were identified.

Mystery Shopper Experience - Whilst the results have remained steady over recent months, a full review of the question set completed by the mystery shopper is to be reviewed to ensure the questions fully reflect an introductory conversation.

◀▶ Remained green ◀▶ Remained amber ◀▶ Remained red ▲ Improved to green ▲ Improved to amber ▼ Fell to amber ▼ Fell to red

BOI Group classification : **Red** (Confidential) - distribute only with sender's permission

POL00401626

Joint Conduct Committee (JCC) - Network Distribution Scorecard

Jan-18

Risk ratings

January risk rating and how they compared to December		
●	Branch net sales vs complaints	◀▶
●	% of branch complaints upheld	◀▶
●	FOS cases upheld	◀▶
●	Red rated MS VMS shops	▼
●	Red rated CRM VMS shops	▼
●	Black rated MS/VMS shops	◀▶
●	Non VMS observations	◀▶
●	Branch monitoring red ratings	◀▶
●	Home cancellations	◀▶
●	Travel cancellations	◀▶
●	Life cancellations	◀▶
●	Over 50s cancellations	◀▶
●	Branch sales - errors	◀▶
●	MS mandatory training	◀▶
●	CRM mandatory training	◀▶
●	T&D record checks	◀▶
●	On the job observations	◀▶
●	NPS results	◀▶
●	CES results	◀▶
●	Reportable incidents	◀▶

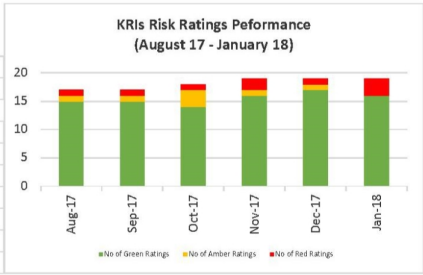
Key	
●	green
●	amber
●	red
●	not measured this month
◀▶	remained green
◀▶	remained amber
◀▶	remained red
▲	improved to green
▲	improved to amber
▼	fell to amber
▼	fell to red

Performance measured in January

Overall performance rating	Green rated KRIs	Amber rated KRIs	Red rated KRIs	KRIs not measured
AMBER	16	0	3	1

Based on the weighted culmative outcome of the KRIs we measured in September, the overall risk rating is AMBER.

This month we were within tolerance for 18 out of the 19 KRIs we measured. 16 of our KRIs were rated green, 0 of our KRIs was rated amber and 3 of our KRIs were rated red. In comparison with December there were no changes in the number of KPIs measured and achieved. In the last six months (August - January) we have averaged an achievement rate of 85.4% of the total KRIs measured within this period which results in an amber rating.



This month we were within tolerance for 11 out of the 13 KRIs we measured. 11 of our KRIs were rated green, 1 of our KRIs were rated amber and 1 of our KRIs were rated red. In comparison with August there was no change in the number of KPIs measured and achieved. In the last six months (April - September) we have averaged an achievement rate of 84.4% of the total KRIs measured within this period which results in an amber rating.

Key headlines and trends

Summary - January saw a deterioration in our key risk metrics. Of particular concern is the VMS scores. Whilst this relates to low volume, the failure rate is worrying and we should be seeing a higher level of monitoring given the volumes of transactions performed. The introduction of non-VMS observations should be key to providing this additional level of assurance.

POL00401626

Change Risk Update

Author: Jenny Ellwood Sponsor: Tim White Meeting date: 13 March 2018 (RCC)

Executive Summary

Context

This report provides an update on the delivery status of the Change Portfolio, the key risk themes under management and the risks we think RCC and ARC should have visibility of.

Questions addressed in this report

- What is the current change portfolio delivery status and key delivery challenges?
- What are the current top portfolio risks?
- What are the types of portfolio risks and how has this mix changed?

Conclusion

1. The project delivery and risk status (which is an amalgam of the status of individual programmes) remains 'Red' due to a number of contributing factors. In particular dDelivery challenges still remain in a number of Programmes these include Customer Hub, GDPR, Transaction Simplification, Mercury (HNGT lite) and Back Office Transformation.

2. The current portfolio risks which we consider should be given visibility at RCC and ARC are: i) GDPR: Contracts, ii) Late delivery of Change leading to increased costs and reduced benefits and iii) EUM effectiveness. There are currently **28** risks within the Portfolio. MI is shown as an Appendix.

3. The late delivery of change risk is also one of the group reported risks and work on this continues to be led by the newly formed Strategic Portfolio Office. The inaugural Investment Committee was held at the end of February. This is one of the first steps in improving the change process ensuring that where funding is allocated to change it is aligned to the Post Office Strategy and is given to the Programme in stages on proof of delivery of key milestones/agreed value.

4. At the moment the Portfolio holds a mix of portfolio-wide risks and some key Programme risks. The number of portfolio risks have seen a net increase of **+4** from November 2017. This is reflected in the current aggregated risk severity score of **260**. This score has been incrementally increasing since September.

Input Sought

The Committee is asked to note the slight deterioration of the portfolio risk position since the last ARC, the top risks being faced, how they are being managed and mitigated and to advise on any additional areas/topics that should also be taken forward.

POL00401626

The Report

What is the current delivery status of the Change Portfolio and key delivery challenges?

1. At the end of February 2018, the overall Post Office change portfolio status was 'Red'. There were 3 key programmes which reported Red from a risk dimension:
   - Customer Hub: as it continues negotiations with FRES around the development of APIs, the new Customer App and migrating existing customers on to this.
   - GDPR: as it continues to work towards reaching 'effective compliance' by end of May 2018' see paragraphs 4-7.
   - Transaction Simplification: there is a risk the programme continues its development work in the absence of an agreed negotiating position with RMG on receipt printer quality.

2. Discussions continue around our appetite to further reduce agents' pay and we are monitoring the following programmes:
   - Project Mercury: The proposition is being reviewed with Spar and there are a number of 'show stopping' restrictions which will require negotiation with RMG. In addition, the development of the APIs is taking longer and is more expensive than first thought. For this reason HNGT lite proposition is being reconsidered. The development work will not be wasted as it is core for HNGT.
   - Back Office Transformation: The programme is facing a number of delivery risks with both POLSAP migration and the Cash Processing work streams. Both of which were due to go live in June 2018 and under a full replan. Further details on the risk and the delay that POLSAP migration creates on DR Testing is provided in the IT risk update paper.
   - IT Networks: This programme is continuing to roll out the new networks and is targeted to reach 6,500 branches by the end of March. Despite the difficult weather conditions there hasn't been any major impact on the Network Migration/Branch Counter refresh schedule this week.

What are the top risks currently being managed within the Portfolio and what is the performance of risk management based on the mitigation plans?

3. There are currently **28** open risks being managed at a Portfolio level, a net increase of **+4** from the last time this was reported to ARC in November 2017. The current portfolio risks which we consider RCC and ARC should be given visibility of are: i) GDPR: Contracts, ii) Late delivery of Change leading to increased costs and reduced benefits and iii) EUM effectiveness:

General Data Protection Regulations (GDPR)

4. The GDPR comes in to force in May 2018. The Programme has from inception flagged that it was unlikely to achieve full compliance by May 2018. Instead the programme has taken a risk based approach to achieve 'effective compliance' which is defined as all new activity and remediation for existing high risk/priority activities will be completed. However, there is still much to do to reach 'effective compliance' by the commencement date of the legislation.

POL00401626

5. A number of our 3rd party suppliers, in their role as 'data processors', are now subject to increased accountabilities. Controllers need to understand who has access to their personal data and ensure appropriate due diligence is undertaken on suppliers, vendors and processors. This is a significant risk for Post Office owing to historic issues with contract management. Contracts with many suppliers do not contain appropriate governance provisions, even for existing data protection obligations. There is therefore a lack of shared understanding of processing responsibilities. In many cases documentation is not sufficient to comply with GDPR.

6. The GDPR Programme is addressing this using a risk based approach. A high level assessment has been done and an external legal firm has been appointed to work with business stakeholders and relevant 3rd parties to deliver compliance, based upon a graded and suitable risk based approach.

7. This approach is in line with the guidance the Programme has received from the Department of Culture, Media & Sport (DCMS) which sponsors the Information Commissioner's Office (ICO). The latter have also made a number of public statements stating that securing full regulatory compliance will be a long haul and preparations will be ongoing beyond May 2018. The ICO have emphasised that they will adopt a proportionate approach subject to organisations' self-reporting potential breaches, being able to demonstrate effective accountability arrangements are in place and, finally, proactively engaging with them to resolve issues. A recent survey from Deloitte indicated that overall, only 15% of organisations surveyed expect to be fully compliant by May 2018, with the majority instead targeting a risk-based, defensible position.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
GDPR Contract Risk	Risk that the GDPR programme cannot deliver what is defined as "Effective Compliance" by 5/2018 because of difficulties: • in establishing what the universe of 'material' and 'non material' contracts is, and to obtain all current versions, • that current controller to processor contracts do not provide sufficient governance of suppliers obligations • with a lack of up to date core documentation on the personal data suppliers process and lack of clarity of their processing responsibilities.	**16** **I/L: 4:4**	• Validation of the 'material' contracts via GE • Validation of 'non-material' value contracts list via GE • P-Suite to include GDPR compliant clauses for new commercial agreements • Renegotiation of Existing contracts	Complete 15 March Complete Ongoing	**12** **I/L: 4:3**

Late Delivery of the Change Plan

8. This update follows on from the update provided in January, where the root causes were highlighted. PA Consulting are continuing with their review of the way the Post Office manages change and is seeking to make, by the end of March 2018, recommendations for improvement. This includes developing mitigations to tackle these key root causes. Additionally, this work currently involves validating the design of the high-level target Change Operating Model (including the Strategic Portfolio Office), building a phased transition plan and identifying implementing and delivering Quick Wins.

POL00401626

9. A key component of the new approach is the creation of a Post Office Investment Committee (IC). This commenced in February and is chaired by Rob Houghton. Its purpose is to review and make investment decisions on both the in-flight and pipeline change initiatives. It will also have a role in making strategic interventions to in-flight work, as required.

10. PA have already made some suggestions around some low effort, high impact improvements, which include development of:
    - criteria to assess all new projects against, to determine the level of control that should be applied, depending upon size and complexity
    - a revised delivery framework application which is flexed for less complex programmes
    - clear and robust mandatory gate requirements,
    - improved / creation of best practice templates aligned to the delivery framework and gate requirements
    - a Delivery RACI and clarification of role requirements for key personnel, ensuring there is a common understanding of who does what, and when

11. The above recommendations are all key mitigations and will help reduce the late delivery risk. PA are also looking at providing Agile insight into the Target Operating Model deliverables. Change Risk and Assurance will develop an Agile assurance approach and plan which will be agreed with Internal Audit.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
Late Delivery of Change	Our change is delivered late, risking costs and benefits or has unintended consequence	15 I/L: 3:5	• Transfer the executive sponsor of change to Rob Houghton / Tim White • Implementation of a Strategic Portfolio Office (SPO) and recommend the Target Operating Model which should be in place. • Create a new Investment Committee – develop TOR, attendees, roles and responsibilities. • Develop a project prioritisation methodology, which prioritises those initiatives that contribute the most to the PO's strategy and financial objectives • Build a phased transition plan to implement the new strategic portfolio office and processes (including the introduction of an agile delivery and governance process).	Complete End Mar 18 Complete End-March 18 End-March 18	6 I/L: 2:3

Enhanced User Management (EUM)

12. To date the Programme have rolled out the new identity solution to 1700 branches, within current gating approval to go to 4000 branches. The current planning assumption is that the design enhancements approved at POL Board in January will be implemented in June, although the Fujitsu release date has not yet been confirmed. If Fujitsu and the programme do not hit the June slot, this will impact our ability to deploy the training controls in July as we need the system functionality to allow branches to regain access to Horizon in near real time once they have completed their training to avoid significant operational issues including unexpected branch closures. This risk is being carefully managed and we expect confirmation of the release date in March.

POL00401626

13. The main outstanding risk is the efficacy of data capture from branches as this is a manual process involving branch by branch data verification. Through close working with the Common Services programme, steps have been taken to improve the communication to branches, using memoview rather than letters as this is a more certain way to ensure the message is seen and read.

14. Additionally, a simpler data collection process using Horizon will be implemented in late March. The current mitigating action of collecting data from 500 branches per week to achieve 300 branches per week of clean data will continue. If the improvements lead to better response rates, this will inform our ability to achieve an improved beat rate, but this won't be known until April 2018 at the earliest. An independent assurance review is planned in March/April 2018 to test the confidence in this new data collection process as well as the progress made by Fujitsu ahead of a confirmed release slot.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
EUM	There is a risk that EUM does not perform as expected due to • being unable to collate accurate data from agents • POL staff/agents not having an individual email address which can be used to communicate logins and training information **(resolved)** • Agents not being able to access SuccessFactors via the internet/browser solution **(resolved in new design)** This all leads to our inability to address the key business goal, which is for POL to prove to its client that persons transacting on its behalf are suitably qualified and vetted.	**12** **I/L: 4:3**	• Liaise with Common Services programme regarding data capture. Agreed ramp up request of data to 500 branches and improvements in data capture process and alternative communication process. • Build Horizon/SF learning interface in EUM to enable both systems to be available for agents to complete their training. • Uplift Branch standards resources to support branch migration to using the new Smart IDs and securing training compliance.	Mar-May 18 Ongoing Ongoing	**9** **I/L: 3:3**

15. ARC also requested an update on the SuccessFactors Programme. Payroll went live in January 2018, and this has gone well, with no material over or under payments. The project is currently undertaking post go-live support, preparing for transition to BAU later in March 2018 and agreeing contractual 3rd line support with Accenture, who want unlimited liability in respect of TUPE cases. Hyper care arrangements are still in place and will remain until the knowledge transfer is completed.

16. The SuccessFactors project is now moving towards formal closure. However, there will remain some activities outstanding from the approved Risk Exception Notice, in relation to single sign-on and 'bring your own device'. A corporate solution to resolve these is targeting delivery in June 2018. Design documents have been produced and a supporting business case updated. The action owner confirms that although there will be significant progress made by this date, if not fully successful then access to SuccessFactors must be limited to Post Office corporate devices. This would mean that front line employees, for example, having to book annual leave/access payslips through their depot/branch manager's PC. There will also be multiple employees accessing their personal and sensitive data from a shared computer, which could give rise to additional risk of data leakage.

POL00401626

17. A full list of the **28** active portfolio risks is shown as an Appendix.

What are the types of portfolio risks and how has this mix changed?

18. In November 2017, there were **24** portfolio level risks (October 2017 data). This was the last time we formally reported on this data to ARC. The current total is **28** which has been subject to churn in that (since October 2017) **5** risks have been opened (GDPR contracts, DPO Bandwidth, HR SAP decommissioning, HNGx & New Receipt Printer and Late Delivery of Change) and **1** risk closed (Operational Impact of Generic Training Expiry Dates).

19. An illustration on how the mix of risks at portfolio level continues to flex and shows the open portfolio risks by severity is shown on the following page.

RAG Impact/Likelihood	Minor (1)	Moderate (2-4)	Major (5-11)	Significant (12-19)	Critical (20-25)	Total
February 18	0	4	14	10	0	28
January 18	0	4	13	10	0	27
December 17	0	4	13	10	0	27
November 17	0	4	12	8	0	24
% of total (current period)	0%	14%	50%	36%	0%	100%
Number of New Risks in last period						5
Number of Emerging Risks in last period						1
Number of Closed Risks in last period						1

Figure 1: Please note the minor/moderate risks are managed at a local level and not escalated to the Portfolio view.

POL00401626

Appendix: Change Portfolio risks, supporting metrics and mitigation plan dynamics

The Portfolio

	Risk Title	Nov ARC	Mar ARC	Grid Ranking CURRENT	Grid Ranking TARGET
1	GDPR Contracts		✓	16	12
2	Complex Portfolio Planning & IT Management	✓		16	8
3	HNGx & New Receipt Printer	✓		16	2
4	ISDN removal from Branch estate[1]			15	8
5	Late Delivery of Change		✓	15	6
6	DPO Bandwidth Risk			12	4
7	Delivery of elements of the Change Plan	✓	✓	12	9
8	EUM Effectiveness	✓	✓	12	9
9	IT Change Operating Model			12	8
10	Data Risk			12	8
11	GDPR			12	8
12	ITBNA Incumbent Supplier Proactive Engagement - BT			9	4
13	IT Vendor Renegotiations			9	9
14	IT Delivery Capability			9	6

[1] To be closed in the next reporting cycle

POL00401626

	Risk Title	Nov ARC	Mar ARC	Grid Ranking CURRENT	Grid Ranking TARGET
15	Unintended consequences on Operational Performance - Process			9	6
16	Adverse Impact of Change/ Organisational Change on Agents			9	6
17	Accounting & Reconciliation			8	8
18	Financial risk - Benefits/Revenue Realisation			8	6
19	Availability of Key Skills and Knowledge			6	6
20	Responsible use of public funds			6	1
21	Strategy & Design: Conflict between current BaU and Transformation activities			6	3
22	Reputational Damage - Media risk			6	4
23	Reputational Damage - Political stakeholder risk (local government)			6	4
24	Decommission of HR SAP			5	1
25	Deployment of Non-Compliant Solutions/Systems - (Breach of LRC reqts)			4	4
26	Reputational Damage - Political stakeholder risk (national government)			4	4
27	Poor coordination of change communications with stakeholders and employees			4	4
28	Model Office Testing Capacity/ Resilience			3	2

Strictly Confidential

POL00401626

The Churn

The table below details the number of risks open and closed over the last rolling 12 months.



Figure 2: A comparison of open/closed risks (by month)

Risk Weighting

Each portfolio risk has a weighting score calculated by multiplying their impact/probability scores. When added together this provides a cumulative portfolio score which currently stands at **260**.

The overall risk severity has oscillated since February 2017 when it was **18**% than it is now albeit it has been incrementally increasing since September 2017. The risks continue to be monitored in line with the change portfolio risk review process.

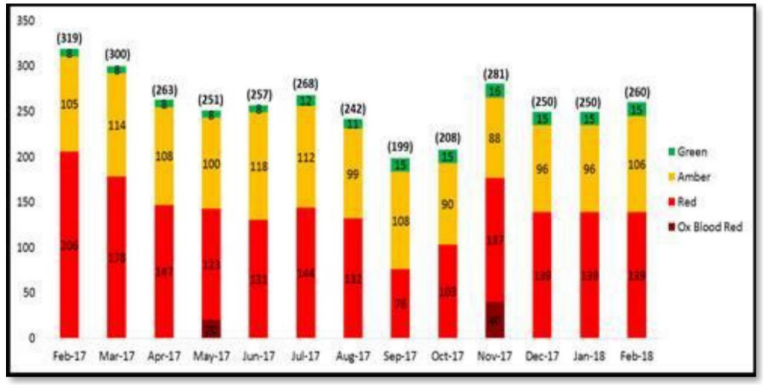


Figure 3: Current cumulative portfolio risk weighting score by month

Figures 4 and 5 illustrate the anticipated impact of a reduction in the number of active risks over the next 6 months will have on the residual risk weighting.

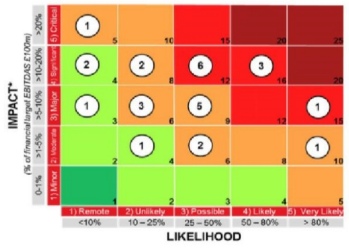


Figure 4: Current portfolio risk weighing (Feb 2018)

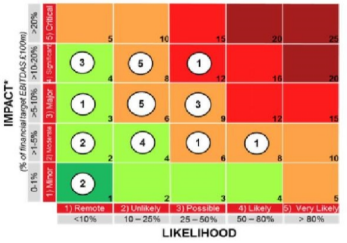


Figure 5: Target portfolio risk weighting (Feb 2018)

POL00401626

Financial Crime Risk Update

Author: Sally Smith | Sponsor: Jane MacLeod | Meeting Date: 13th March 2018

Executive Summary

Context

This paper updates the Risk and Compliance Committee on financial crime risks relating to Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) and Anti-Bribery and Corruption and compliance with The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 and The Terrorism Act 2000.

Questions this paper addresses

- What are the key AML and CTF risks within Post Office Ltd and are there any significant gaps or weaknesses in the Post Office's compliance with its regulatory obligations under the Money Laundering Regulations (MLRs)?
- What is the current position with the post HMRC Audit Bureau de Change remediation project
- What is the current position with financial crime risk assessments.
- Are the minimum control standards in the Post Office's Anti-Bribery and Corruption and Whistleblowing Policies being effectively applied?

Conclusion

1. The project team are progressing with the work needed to comply with the new Fit & Proper requirements, but there is still significant work to meet the June 2018 deadline and to ensure that the ongoing framework is robust.
2. There have been further delays with the Bureau de Change remediation projects with implementation of the data warehouse solution pushed back to the beginning of March, meaning that the new reports have not yet been built and tested. The eKYC, PEPs and Sanctions solution is progressing for April implementation, however, HMRC have now verbally advised that our interim solution for cash transactions over £2k is not acceptable, and we are due to meet with them on 12th March to discuss.
3. Risk assessment work continues, although there are a number of new or updated Product Information Packs that remain outstanding, and these are being chased.
4. There have been no issues with Gifts & Hospitality reporting since the communication in January. The volume of Whistleblowing reports received via various channels has increased, although further communication and awareness activities are planned throughout 2018.

POL00401626

Input Sought

The R&CC is asked to review this report and consider whether further actions should be undertaken.

The Report

Compliance with MLRs

5. The pre-penalty notice in respect of Regulations 19 and 20 relating to the Bureau de Change product was received on the 8th January 2018 for the sum of £344,766 and this has been paid.

6. Annual training content for Network and back office staff is being drafted and is due to be delivered 4th – 30th May 2018. There are still 4 branches that have not completed their training from last year and second remedy letters have been sent to them. If they still remain non-compliant, the contracts team will need to escalate.

7. We continue to liaise with HMRC on the new Fit & Proper tests, and have sent them an initial data set split out by Multiples, Sole Trader Agents, Limited Company Agents, and direct employees who are now captured. There is significant work still to do to complete the gaps in data, especially the identification of Directors and Beneficial owners. Other activity that needs to be completed includes documenting the policy and processes to cover on-boarding and periodic vetting/self-declarations, training and defining events that would require fit and proper status to be reviewed.

8. HMRC have written to all Large Traders at the end of February to emphasise that the deadline for responses with the information they require is the 25th June 2018 (i.e. one year after the new regulations came into force). Whilst Post Office will have identified all individuals that are subject to the Fit & Proper regime, there will still be gaps in some of the data fields as these are obtained from agents, directors and beneficial owners. Our HMRC supervisor has indicated that this is acceptable, but we will raise again with them when we meet in March.

9. Non-conformance issues in the Network in January and February 2018 included 38 incidents identified at 38 branches.
    - 17 branches identified were Directly Managed Branches and/or WH Smith Multiples and these have been addressed by the Financial Crime Team and escalated to Network as appropriate. A number of these instances relate to breaches that we deem 'unavoidable' – i.e. not the same clerk, day or time that the customer is transacting.
    - 15 branches remain on the non-conformance watchlist following the new ID thresholds and are manually monitored monthly.
    - 1 new branch was added, and none were removed.

10. The volumes of suspicious activity reports (SARs) have increased slightly in January and February 2018. The increase volume on internal SARs submitted by the AML team has contributed to this rise in overall SARs, these predominantly are in relation to Bureau de Change.

POL00401626

11. The Financial Crime Team were previously concerned that SARs in relation to MoneyGram and potential vulnerable customers had decreased since the introduction of MoneyGram's new ID capture portal, and this was resulting in branches assuming transactions were genuine because the customer was still willing to complete the transaction. In January and February we have seen a steady increase in SARs relating to this issue and the Financial Crime Team have planned communications to increase the networks awareness.

Bureau de Change remediation project status

12. HMRC have responded verbally to the letter sent in January setting out our approach for transactions over £2000. Whilst they accept that for transactions paid by card the proposal is sufficient, they have stated that our proposal for cash transactions, whereby the clerk will need to confirm on Horizon that the photo ID and the customer are the same individual, is in breach of regulation 40, which requires us to retain a copy of the ID.

13. They have requested a meeting with us to discuss, which is scheduled for the 12th March. We are taking further legal advice on the regulations and looking at what options may be available to avoid the need to retain copy documentation.

14. The eKYC, PEPs and Sanctions capability has progressed to testing and should be live in April, but the exact date is yet to be determined. Post Office have been advised that the Government Document Checking Service cannot be used for one-off transactions, only where re-usable credentials are established, so this element cannot be applied until the new Customer Hub and Identity service is achieved later in 2018.

15. The new data warehouse delivery has slipped but is due to go live week commencing 5th March. The new reports can then be built and tested, and HMRC are due to review these in Chesterfield on 21st March. The reports cannot be finalised until the PEPs and Sanctions checking goes live. Once the new reports have been built, the operational team in Chesterfield will need to parallel run against the current report to ensure they are working.

Financial Crime Risk Assessment

16. Work on risk assessment continues as BAU, and Appendix A gives full updates on the status of Product Information Pack completion and re-assessment work. Completion of the Banking Framework Services Product Information Packs is critical if the risk assessment work is to meet the end of March deadline from the recent Internal Audit report.

17. We have identified managers within Retail and Financial Services & Telecoms that require financial crime risk assessment training, and will be looking to roll out sessions in the new financial year.

18. As part of the work the Risk team are doing on the Risk and Controls Matrix, we are piloting a methodology to ensure that there is appropriate oversight of financial crime as a principal business risk.

Anti-Bribery and Corruption (ABC) update

13. Following further communications sent out in January after the Oct-Dec quarterly report, there have not been any significant issues identified in Gifts & Hospitality reporting. However, an issue was identified with the new

POL00401626

expenses tool relating to the 'external entertainment' category, and this now references that any external entertainment claimed must have been reported and approved via the Gifts & Hospitality Tool. A quarterly review of entertainment expenses data is going to be compared against the central Gifts & hospitality register from the end of the current quarter.

Whistleblowing update

14. The volume of Whistleblowing reports is improving, and further regular communications are planned for 2018.

15. 13 reports were received between January and February, and 11 of these named a Post Office branch. 6 were classified as fraud and 1 as money laundering. The majority of Fraud reports were submitted via Grapevine or the Speak Up line and were in relation to theft carried out by a Postmaster, Agent Assistant or an employee. 2 reports alleged thefts from vulnerable customers. All reports are investigated with recommendations made and followed up

Regulatory updates

16. The update relating to the Fifth Money Laundering Directive in the January report remains current.

17. The new Sanctions and Anti-Money Laundering Bill introduced on 18th October 2017 has been reviewed. There are two key areas it is designed to address:

    - enable the UK to continue to implement United Nations (UN) sanctions regimes and to use sanctions to meet national security and foreign policy objectives; and
    - enable anti-money laundering and counter-terrorist financing measures to be kept up to date, helping to protect the security and prosperity of the UK and continue to align the UK with international standards

    There are no significant impacts for Post Office.

18. Following the National Risk Assessment that was published at the end of October 2017, HMRC has published a review of anti-money laundering compliance in money service businesses (MSBs). This is mostly aimed at money transmitters operating via an agency model, but covers some generic areas. The review identified good practices to assist with a risk-based approach and reduce vulnerability. The document has been reviewed and there are no significant areas that impact Post Office business.

External threats

19. There have been no new issues since the January 2018 report.

POL00401626

Appendix A

Risk Assessment and Product Information Pack update

Due for reassessment in the next two months

Product/Service	PIP initially received	PIP due for review and update	Month FCT will re-assess risk	RAG status	Comments
Gift Cards	July 17	July	September	RED	Following an incident in October 2017 the PIP needs to be updated
Bill Payments	October 17	October	December	RED	Following an incident in October 2017 the PIP needs to be updated
Postal Orders	April 17	April	June	Not yet due	
Travel Insurance	May 17	May	July	Not yet due	
Business Insurance	May 17	May	July	Not yet due	
Home Insurance	May 17	May	July	Not yet due	
Car Insurance	May 17	May	July	Not yet due	
Motorcycle Insurance	May 17	May	July	Not yet due	
Van Insurance	May 17	May	July	Not yet due	
Pet Insurance	May 17	May	July	Not yet due	
Drop & Go	May 17	May	July	Not yet due	

Due from November 2017 Product Manager Workshop

Product/Service	Month PIP Due	Completed PIP received?	Month FCT scheduled to re-assess residual risk	RAG status	Comments
Partner Banking Framework	February	No	March	RED	PIP has not been received to date. This will cause the audit action risk assessment to be delayed
Identity Services	March	No	May	Due March	Draft has been received and reviewed. Awaiting amendments.
Savings Products	March	No	May	Due March	Draft has been received. Awaiting review
Credit Card Products	March	No	May	Due March	
Pre-Paid Cards	March	No	May	Due March	
Mortgages	March	No	May	Due March	

POL00401626

Supplementary Documents

Product/Service	Month PIP Due	Completed PIP received?	Month FCT scheduled to re-assess residual risk	RAG status	Comments
Loans	March	No	May	Due March	
Life Insurance Products	March	No	May	Due March	Draft has been received and reviewed. Awaiting amendments.
Telecommunications products	March	No	May	Due March	
National Lottery	March	No	May	Due March	

Post Office Limited Risk and Compliance Committee-13/03/18

POL00401626

Identification and Management of Risk :Gift Card

Keith Maple

March 2018

POL00401626

Situation at the end of 2016 indicated high risk and lack of control

Initial Financial Crime Risk assessment completed in September 2016 concluded high residual risk (10.24) and a control rating of only 14%

WHY?

- No evidence to show the product was effectively managed
- No immediate evidence of a signed contract
- No evidenced or demonstrable understanding of contract obligations or evidence that POL were complying with financial crime policies and applicable legislation OR if POL needed to be registered with the FCA
- Nothing that provided an overview of the risks to which POL could be exposed
- No framework for enabling the effective management of Gift Card
- No evidence of branch training being required or executed
- No evidence of monitoring of possible fraud

POL00401626

Gift Cards do have inherent risks

- The product is Anonymous
- The product can be bought with cash which increases the anonymity
- They can be sold to commercial customers

BUT

Something needed to be done to reduce the risks that could be addressed

The conduit for the solution was the completion of a **Product Information Pack** to;

- outline Gift Card's risks, processes, obligations and procedures
- provide an overview of the risks to which Post Office Ltd might be exposed
- provide the framework to enable the effective management of Gift Card

POL00401626

June 2017 risk has been reduced from high to moderate with control of risk at 75%

Financial Crime Risk Reassessment completed in June 2017 produced a reduction in residual risk from 10.24 to 3.04 **moving from high to moderate risk**

WHY?

- Thistle worked with Legal, Risk and Governance and the POL Gift Card Product Manager to ensure the necessary controls are in place to mitigate the risk of financial crime. The framework for this is the Completed Product Information pack
- Contractual obligations and POLS contractual position were clarified and understood and confirmation that POL, as a distributor for GVS, are not required to be registered with the FCA
- Recognition that Postmasters are required to follow the overarching POL polices to report suspicious behaviour, AML etc. Training uses Gift Card examples including purchases of multiple cards.
- Confirmation that GVS have procedures in place to detect fraud including being able to block cards. This is supplemented by POL Financial Crime analysing reports of sales by branch and acting on "suspicious" behaviour

POL00401626

June 2017 until now

- The Financial Crime Team have honed their analysis to pinpoint possible irregular behaviours in branches and have investigated, actioned and in some circumstances helped to re-educate staff in branches
- There is a greater understanding of the features of the product, its flows and the contextual and contractual arrangements and obligations within the Product Team. There is also a closer relationship with GVS after going through the Product Information Pack process
- It has been highlighted by GVS that, that in some circumstances, the cards can be reloaded. Early investigations indicate that though this should not happen at all the incidence is very low. GVS and POL are currently working on a remediation plan
- One lesson learned from this is that if the Product Information Pack had been developed at the inception of the product over 10 years ago then any subsequent 'Memory loss' may have been avoided as the product ownership changed hands .

POL00401626

IT Risk Update

Author: Rebecca Barker Sponsor: Rob Houghton Meeting date: 13th March 2018

Executive Summary

Context

This report provides updates on the IT Risk landscape within Post Office; the key projects within the IT risk area; and details on the remediation activities for the risks identified as outside our risk tolerance.

Questions addressed in this report

1) What is the current IT Risk Landscape?
2) What is the existing progress of the remediation activities planned for the risks outside of the Risk Tolerance?
3) What is the progress against the key activities in Risk Management?

Conclusion

We remain outside our risk appetite in key operational areas, especially the Fujitsu supported infrastructure estate. However infrastructure related change programmes intended to reduce these risks over time are in progress.

The Branch Network refresh project, which will address the risk to replace ageing kit and move from Fujitsu to Verizon is on schedule to complete by the 31st March 2018. Despite the difficult weather conditions there hasn't been any major impact on the Network Migration/Branch Counter refresh schedule.

Following delays within the Cash Management Processing project, POLSAP Migration is now planned for 1st September 2018. This revised date impacts our DR programme, and our Fujitsu failover test needs re-planning (originally planned for August), as the risk is too high to perform the failover whilst POLSAP remains in operation on the existing Fujitsu infrastructure. We need to assess when the Failover test can be planned with minimal impact to service.

We continue to reduce and mitigate the risk of cyber-attacks and security breaches with the Security Operations Centre (SOC) programme. DDoS protection is live, protecting our website service. Firewall assurance is live, improving our understanding of our security perimeter and allowing us to reduce the risk of attacks. Certificate management is in progress, and once fully operational, this SOC component will remediate Certificate Management risks.

An improvement plan is in progress to reduce the risk of loss of service to Swindon stores: the activities over the next four weeks will focus on improving Disaster Recovery plans and increasing the support wrap provided by our Suppliers.

Input Sought

The RCC is requested to note the progress made, and provide feedback on the report.

Strictly Confidential

POL00401626

The Report

What is the current IT Risk Landscape?

1. At the end of February 2018 there are currently 52 open risks being managed within IT, this has increased slightly from January, this is as a result of improved risk insight with our suppliers. No known risks have materialised to issues. Six risks remain outside our risk tolerance and are detailed in section 3 (see also Appendix 1 for the high level tube map).
2. The number of risks outside tolerance is reducing over time, and IT are running key programmes which will mitigate our overall risk and bring us within risk appetite, these include;
    - Horizon Data Centre Refresh (HDCR): The HDCR Programme is moving applications off very old infrastructure onto new. We are currently testing all Banking and Payment services interfaces for the Banking and Payment services migration in Q1 2018. All business critical migrations will be completed by Q1 2018. The programme will complete in Q2.
    - Branch Network Refresh: 9,393 branches have migrated. Work continues with Verizon to improve the Verizon secondary service, ensuring that the strongest secondary connection is prioritised. Migration is still on course to complete by end March 2018.
    - SOC (Security Operations Centre): Firewall Assurance Service is live, covering the four major tower providers which represents over 85% of the current estate. The Security Incident & Event Monitoring (SIEM) service will be in place for the four major towers, starting from end April 2018. Improved Certificate Management is currently being introduced, increasing secure trusted connections to be electronically established. Risk and controls functionality will be provided via the Archer platform scheduled to be in place by end March 2018. SOC is on plan to be fully commissioned from July 2018 when Verizon will take on operational management.
    - DDoS (Distributed Denial of Service attacks): There have been no DDoS attacks since end November. For increased protection, a proof of concept of a DDoS protection product, Distil, has been initiated and is protecting the live website today. The output and level of protection afforded will be reviewed throughout March to determine ongoing requirements.
    - BYOD (Bring Your Own Device): BYOD will be materially rolled out by the end of March. All obsolete Windows mobiles phones need to be replaced and this will occur by end April, enabling the protected service to be fully adopted. The closure of exposure of non-corporate devices requires a multi-layered approach and as such requires significant communications to colleagues to ensure they understand differences in business behaviours. Office 365 lockdown will be end April once we have replaced the windows phone estate.
    - Horizon Counter Refresh: Branch counter transition stretch target for exit of HNGX is Aug-18 (commercial deadline is 31/3/19). Working with Computacenter (and other partners) to agree plan to accelerate delivery to meet this target. The programme is now rolling out the new Epsom 7200 slip and receipt printer, which we expect will reduce the volume of calls regarding printer failures and improve service availability.

POL00401626

- IT Disaster Recovery: The DR Framework and IT DR policy target sign date is 13/03/2018, planning for 2018 DR testing is well progressed. Monthly IT Service Continuity Meetings are in place. Recovery Time (RTO) and Recovery Point Objectives (RPO) have been documented for Computacenter, Verizon and Accenture. We expect to complete documentation of RTO and RPO's for all Tier 1 suppliers by 23rd March. This will allow us to meet our commitment in closing the actions with the PWC Banking Framework Audit by the 31/03/2018.
- Cyber Security Vulnerability: A new zero day chip vulnerability known as Spectre or Meltdown exists affecting all chips in computer systems. We review our position against these vulnerabilities regularly and have applied protective patching where available. There are no known publicly exploits of this vulnerability that require remediation, however we continue to be vigilant and to patch all our environments to the latest security levels to ensure we are protected. There have been no major IT Security incidents since December 2017 on our estate.

How are the remediation activities progressing for the risks outside tolerance?

3. The risks below are currently sitting outside risk tolerance; with the potential to significantly impact service availability, compliance, regulatory requirements.

- POLSAP
- Horizon Datacentre Failover
- GDPR
- PCI
- Stock Services
- Accenture Resilience

4. POLSAP: POLSAP Services will be migrated by September, this date has moved from June due to delays in the migration of Cash Processing. Additional hardware blades have been purchased to mitigate risks. The revised date of September will probably result in the Fujitsu Failover Test being postponed from the August bank holiday. (See point 5 for additional information).

Risk Title	Risk	Curr. RAG	Mitigation Plan	Due date	Target RAG
POLSAP Legacy Systems	Failure to ensure all components are fully supported by the appropriate levels of adequate technology, hardware, whilst programme activities are in progress, may lead to a loss of service within Supply Chain and Finance Teams, resulting in service unavailability, financial loss, reputational damage and Security Vulnerabilities.	20 I/L 5:4	1. POLSAP Processes migrated to core finance. 2. Cash Processes migration to Belfast. 3. POLSAP Hosting Contract Extension – period April 1st to December 31st 2018. 4. IPSEC Tunnel Failover – Exploring MSEG options with Verizon. – REN has been raised. 5. Network Upgrade to core final planning stages. Fujitsu have confirmed that Tests plans are underway. The Live dates are being planned. Data Centre work	1.01/09/2018 2 19/03/2018 3.31/03/2018 4.Ongoing 5.In progress	9 I/L 3:3

POL00401626

Risk Title	Risk	Curr. RAG	Mitigation Plan	Due date	Target RAG
			and the network is in progress. 6. SAP Application Support 7. Reviewing the purchase of 2 additional blades for additional contingency.	 6.Complete 7.Complete	

5. Horizon Datacentre Failover Test: As a result of the new migration date of September for POLSAP, the Fujitsu failover test needs re-planning (originally planned for August), as the risk is too high to perform the failover whilst POLSAP remains in operation on the existing Fujitsu infrastructure. We need to assess when the Failover test can be rescheduled with minimal impact to service.

Risk Title	Risk	Curr. RAG	Mitigation Plan	Due date	Target RAG
Horizon Datacentre Failover Test	Failure by Post Office IT to ensure that a full Disaster recovery test is carried out on a regular basis in line with contractual agreements, may lead to being unable to restore primary servers and services not being restored in a real outage. Resulting in financial losses, reputational damage, and prolonged service interruption.	20 I/L 5:4	1. Ensure that component testing that does not impact the delivery of POLSAP or Horizon Datacentre refresh continues to as planned, this is supported by the DR Framework. 2. Planning in place to support the Full Datacentre refresh takes place in August. First session complete 3. March Planning session – assess when the revised Fujitsu failover can take place.	1.Ongoing 2.In progress 3.w/c 26/03/2018	9 I/L 3:3

6. GDPR: A GDPR programme is in flight, supported by the IT Team. The programme team will provide a comprehensive GDPR update to RCC.

Risk Title	Risk	Curr. RAG	Mitigation Plan	Due date	Target RAG
GDPR	Failure by POL IT to communicate the expectations of GDPR to projects and programmes may lead to products and services being prevented or being delayed from launching, Resulting in delays to operational activity, financial loss and reputational damage.	16 I/L 4:4	To be updated by GDPR team in a separate paper to RCC		8 I/L 4:2

7. PCI Compliance: Engagement is ongoing between the IT Security Team, IPA, IT Risk Management and Vendor Management. We are working closely with Computacentre and Fujitsu to mitigate risks to PCI compliance.

POL00401626

Risk Title	Risk	Curr. RAG	Mitigation Plan	Due date	Target RAG
PCI Compliance	Failure by Post Office to ensure operational activities, IT infrastructure/security and related services are PCIDSS compliant may cause challenges during external audit, require significant remediation activities and attract unbudgeted costs. This may result in a failure to obtain the required certification, breach our agreed banking framework and may lead to a legal/regulatory breach, financial loss and reputational damage	16 I/L 4:4	To be updated by IPA and Payments team in a separate paper to RCC		8 I/L 4:2

8. Stock Services: Swindon Stores are running on an obsolete platform that has limited levels of support in place. Furthermore, robust Disaster recovery processes are not in place and the restoration of any service incidents heavily relies on a single individual within Swindon stores to resolve. The impact of an outage to Swindon Stores not only impacts our estate but the service provided to Royal Mint, DVLA and Royal Mail.

Risk Title	Risk	Curr. RAG	Mitigation Plan	Due date	Target RAG
Stock Services	Failure to ensure all components are fully supported by the appropriate levels of adequate technology, hardware, whilst programme activities are in progress, may lead to a loss of service within Supply Chain and Finance Teams, resulting in service unavailability, financial loss, reputational damage and Security Vulnerabilities.	16 I/L 4:4	1. Business paper submitted to suppliers to request a cost effective proposal for support of: • Infrastructure, Operating systems and Oracle Databases. • Remediation plan to be delivered within 4 weeks of service take over and covering - weak areas of support, reduction in risk, improved, ITSCM/DR , Virtualisation and hosting of the FTP/Reporting Server (Business Objects) and hosting, Alternative solutions for support of the primary service 2. Data Cabling – assessment of site and bring up to standard. 3. Proposal from ATOS to ensure the services and suppliers are integrated with ATOS Incident Management and Change Management processes. 4. Swindon Staff to ensure all issues with PC's and printers	1. 12th March 2.19th March 3.19/03/2018 4.w/c 05/03/2018	8 I/L 4:2

POL00401626

			are reported to the service desk to clear the backlog 5. Review on supporting applications: Galaxy, WCS, Mercia and Capricorn 6. Strategic decision on direction for Swindon Stock Centre	5.w/c 26/03/2018 6.In-progress	

9. Accenture Datacentre Resilience: Verizon are now delivering network services to the Post Office. Verizon provide a pair of resilient connections connecting Accenture Datacentres, Hoff and Kronberg. The last mile into the Datacentres is connected via a single fibre connection. In the event of a disaster, the recovery process is manual and the downtime is unknown. The impact of such an event has increased following the migration of Credence and MDM. Further Services will also be migrated to Accenture over the next 6 months thus increasing the impact.

Risk Title	Risk	Curr. RAG	Mitigation Plan	Due date	Target RAG
Accenture Datacentre Resilience	Failure to ensure adequate infrastructure to support failover of the Core finance systems. Resulting in financial losses, loss of services and reputational damage.	16 I/L 4:4	1. Change request has been submitted to Verizon. 2. Review Verizon Response. 3. Solution to be implemented.	1. w/c 05/03/18 2. date to be confirmed. 3. date to be confirmed	8 I/L 4:2

What is the progress against key activities in IT Risk Management?

10. IT Controls Framework (ITCF): Positive engagement with Control Owners with a high response rate to their self-assessments of the controls due for the month of Jan and Feb 2018 respectively. Control testing is in progress and will be complete on the agreed date 16 March 2018. A number of controls are due for assessment in April and will be tested upon submission. IT will complete 100% test of controls for Tranche 1 by the 1st May. The project team are engaged with the Internal Audit team who are supporting the ITCF programme by carrying out a sense check of several complete controls and will provide informal feedback.
11. IT Risk Transformation: An IT Risk Transformation programme has been established to improve our capability maturity. This includes improvements in risk awareness, IT Risk reporting, and supplier risk management. The IT Controls' Framework implementation to improve control across the IT landscape is in self-assessment phase and on target to finish by end of F17/18.

POL00401626

Next Steps

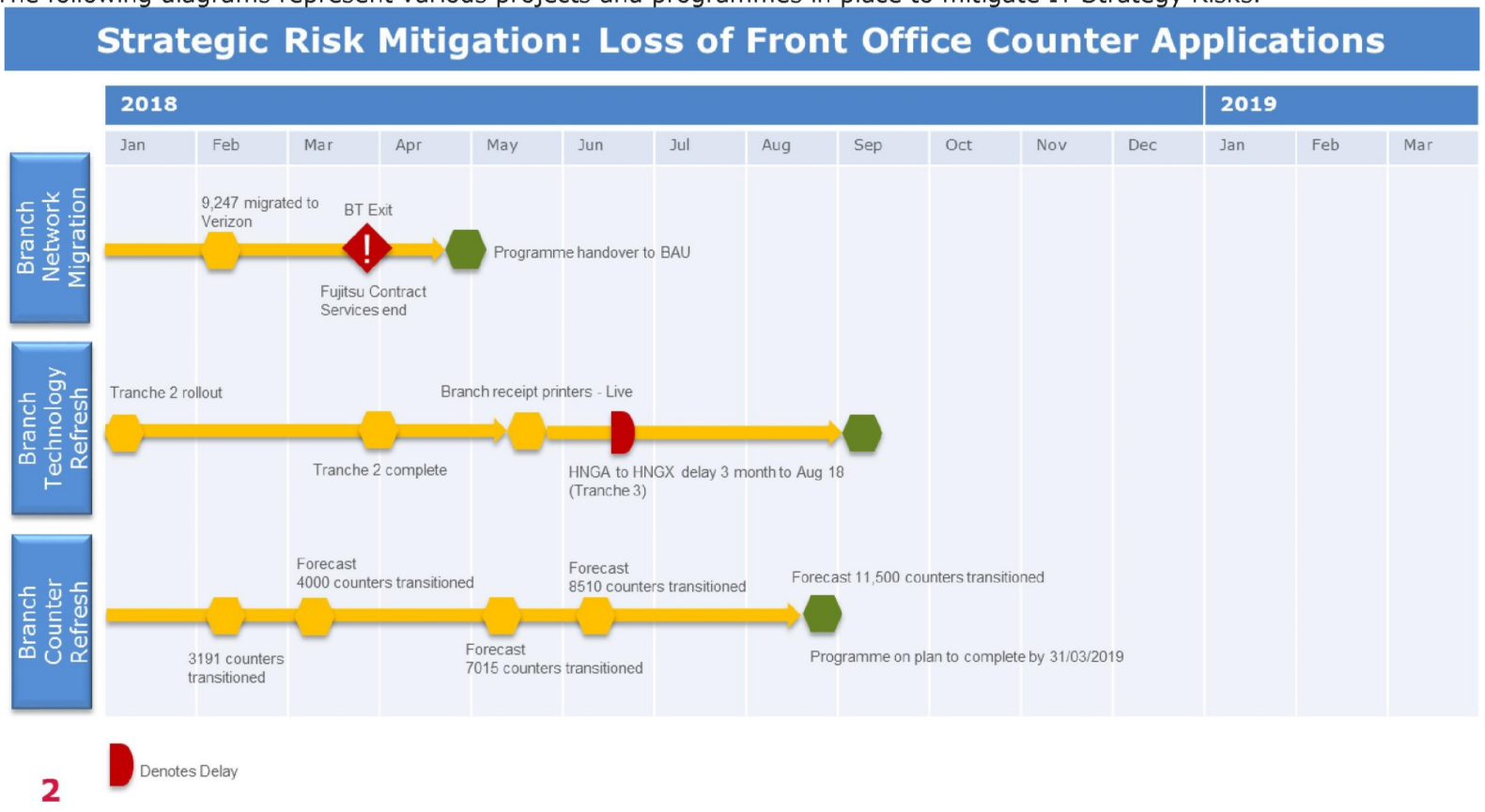
- Informal testing of 6-10 controls from the ITCF to be carried out in March/April to align with the next RCC update in May.
- High level plan to be submitted to ITLB (IT Leadership Board) w/c 12th March for Tranche 2 of the IT Controls Framework.
- Planning session to be held w/c 26th March with Fujitsu to assess a rescheduled date for Fujitsu Failover.
- Workshop to be held with Change Portfolio Programme to formalise process on risks being transferred to live w/c 19th March 2018.

POL00401626

Appendix 1: Risk Tube Map

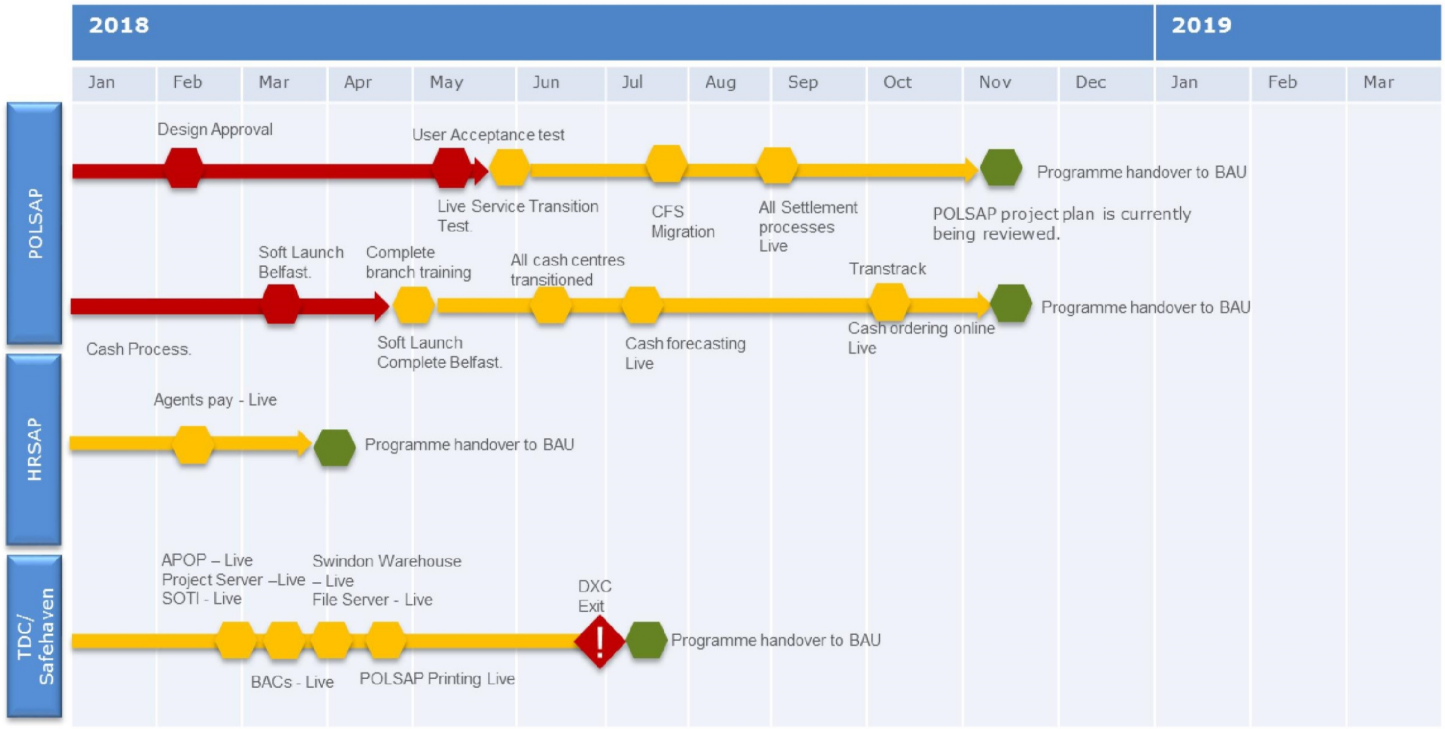
** updated 20th February 2018*

The following diagrams represent various projects and programmes in place to mitigate IT Strategy Risks.



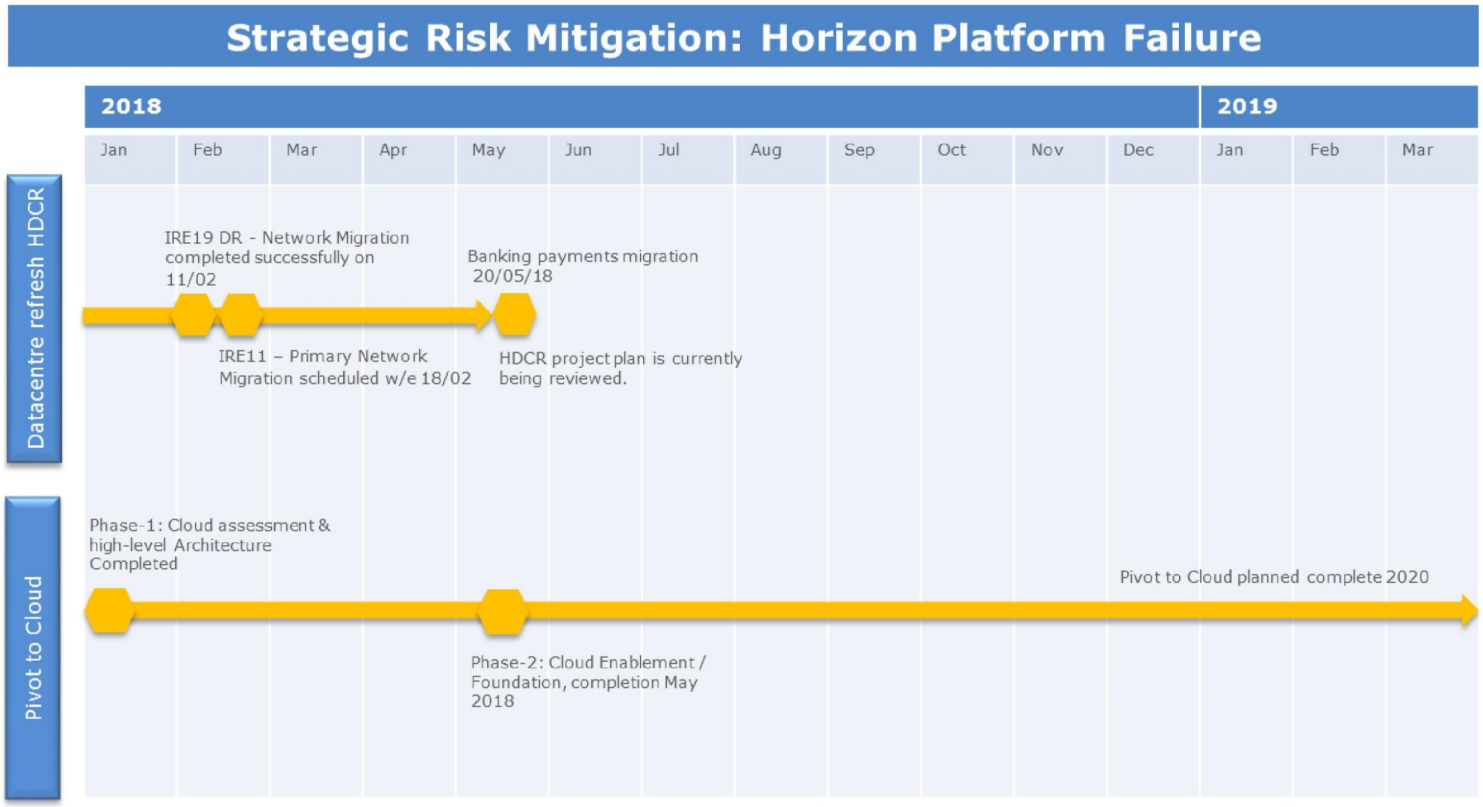
POL00401626

Strategic Risk Mitigation: Back Office Platform Failure



3 NB Credence/MDM Live – Programme Handover 31/03/2018
Swindon Risk Assessment is in progress and will be visible on the Risk Tube map in March

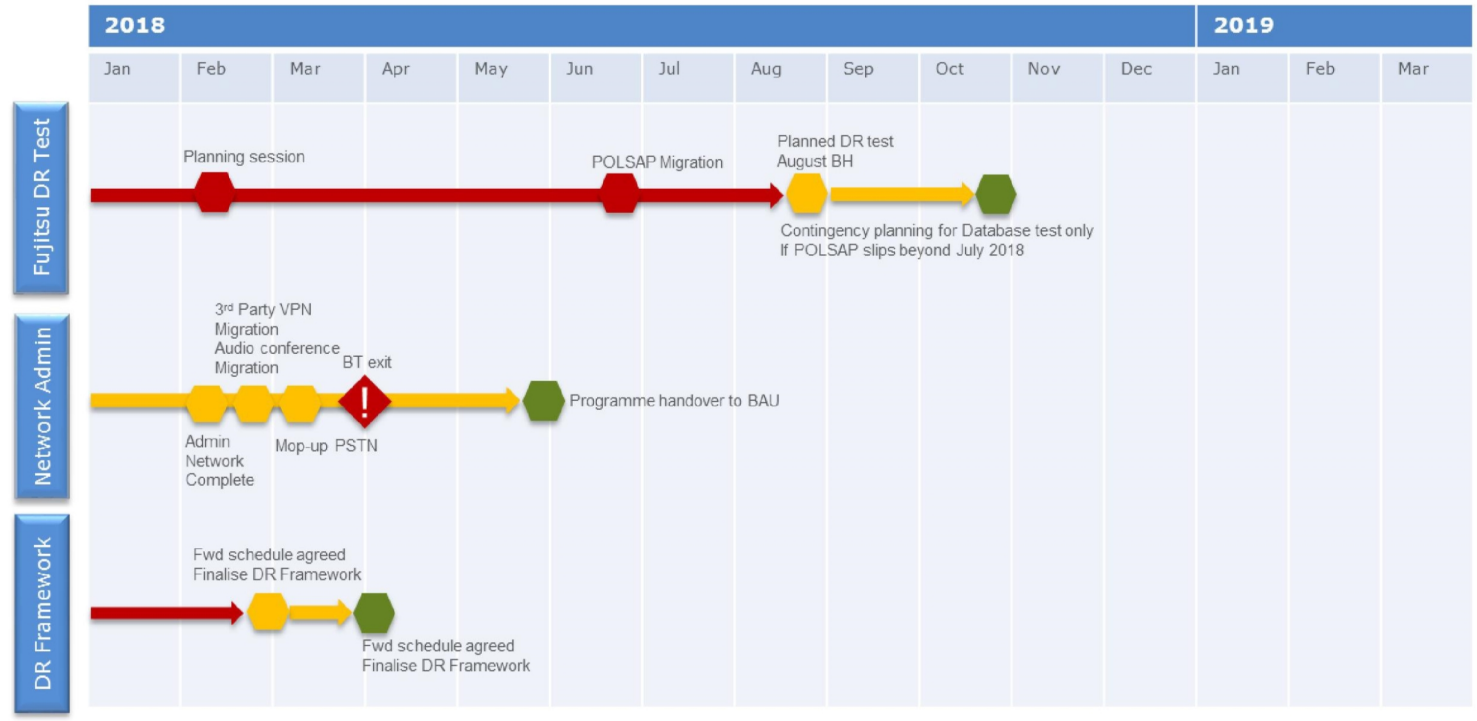
POL00401626



4

POL00401626

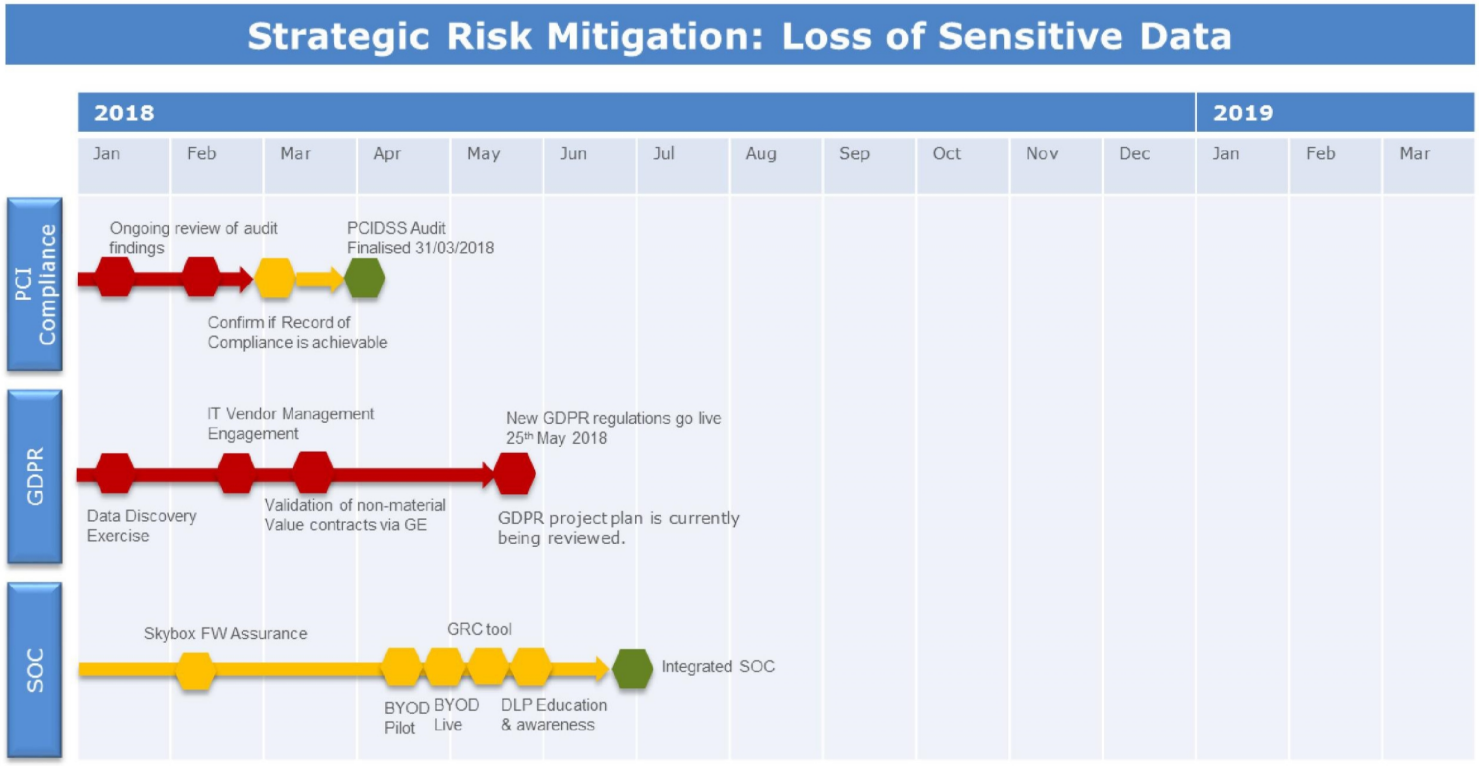
Strategic Risk Mitigation: IT Availability/Ability to Trade



5

Strictly Confidential

POL00401626



Strictly Confidential

Post Office Limited Risk and Compliance Committee-13/03/18

POL00401626

Cyber Security and Information Assurance Update Paper

Authors: Mick Ebsworth/Jules Harris Sponsor: Rob Houghton/Jane Macleod Meeting date: 13 March 2018

Executive Summary

Context

In order to discharge its duties, the Board and Audit and Risk Committee (ARC) request regular updates on cyber and data security risk.

This report is to provide an update on CSIA to Risk and Compliance Committee (RCC) and for onward communication to Audit and Risk Committee (ARC).

Questions this paper addresses

- What are the current top risks to Post Office (PO) from an Information Security and Cyber-perspective?
- How would we know if the risk has materialised?
- What is the current status of the remediation against those top risks?
- What steps are taken to keep abreast of the risk threat horizon?
- What will our risk profile look like once all the current plans have been completed?

Conclusion

PO continue to make significant headway with its Information Security Transformation journey, building on Information Security Governance and the Security Transformation Programme.

The initiation of the '24x7x365' Security Operations Centre (SOC) has been awarded to Verizon for implementation. Service augmentation has commenced with the introduction Firewall Assurance, addressing a concern previously raised in the Deloitte report of 2016. The SIEM will consuming system logs in May 2018 and the full service augmentation will complete in July 2018.

Lock down of Office 365 is progressing, BYOD for mobiles is being rolled out, this includes a replacement handset for Corporate users. This will complete in April 2018 enabling unfettered mobile access to the environment to be disabled.

Additionally, technology to protect against phishing attacks and provide awareness training has been procured and is in the process of implementation (Ironscales), as well as technology to manage our digital Certificates, used to enable secure trusted connections to be established (Entrust). Entrust will identify all certificates in use and determine any issues that the certificates may pose to our live service.

POL00401626

IPA is working on improving the ability of people to recognise and react appropriately to cyber threats through increased awareness activities and have recently launched security characters to assist in getting the improving cyber security training to colleagues.

In conclusion, progress is being made and we have defined key next-steps and have realistic plans to deliver enhancements to our security posture throughout 2018. PO still remain below the level of maturity in cyber and information security for a company in a digital age, but our current provision is appropriate for where Post Office are on their digital journey.

Input Sought

The Committee is requested to note this paper.

POL00401626

Report

What are the current top risks to Post Office (PO) from an Information Security and Cyber Perspective?

The risks to our systems and information assets, as with many other organisations, are as follows:

Risk Number	Risk Description
1	External malicious attack
2	Loss of corporate and personal data through leakage across our perimeter
3	Insider threat (which includes accidental events i.e. phishing attacks)
4	IT Availability

How would we know if the risk has materialised?

PO would be aware if a cyber or information security related risk has materialised by:

- System outages or performance outside of accepted operational parameters (E.g. Denial of Service attacks);
- Identification of a breach through our SOC team;
- Ransomware demands;
- Internal incident reporting; or
- 3rd Party Alerts and Reporting.

What is the current status of the remediation against those top risks?

Risk Number	Remediation	Progress Update	Deadline
1, 3	Implementation of 24x7x365 Security Operations Centre (SOC)	Verizon contract has been signed (Jan 18). Service augmentation commenced, and FW Assurance went live 06/02/2018. Full SOC services implementation on track for July 2018.	Complete July 18

POL00401626

Risk Number	Remediation	Progress Update	Deadline
1, 3	Implementation of IronScales	Testing of Ironscales (phishing protection and awareness training) is now complete with full rollout by March 2018	Q4 17/18
2, 3	Data Leakage Prevention	Bring your Own Device – implementation of Microsoft InTune to control some aspects of data leakage. Completed rollout to GE.	Complete.
2, 3		InTune rollout of mobile devices remains in progress. The project has been re-planned to ensure all obsolete (windows) mobiles phones are replaced by end April, enabling the protected service to be fully adopted. Office 365 lockdown has moved to end April.	~~Q4 17/18~~. Q1 18/19
2, 3		Non Post Office owned laptops and access to Post Office E-Mail protection is due to be available from End Feb 18. Rollout to users will be over the following months.	Q1 18/19.
3	IPA Improving Security Awareness Culture	The images have been created and IPA have started their campaign. The questionnaire to determine the current status has also completed.	Complete
4	Data Owners Programme	GE will have been trained in Data Owner responsibilities during March	Complete

POL00401626

What actions remain to be performed?

Risk Number	Remediation	Progress Update
1	Updating of Legacy Systems	Our ageing systems continue to be a challenge to IPA's ability to maintain our certifications, especially to the Payment Card Industry – Data Security Standard (PCI-DSS). IPA, working with our Payments and Banking Services colleagues, are closely monitoring the situation. IT have a number of programmes already inflight to aid in the remediation of this risk.
2, 4	Data Leakage Prevention (DLP)	DLP paper has been submitted with progress being made on email controls to protect against data leakage. Project initiation to commence for other boundary solutions. The paper and plan to be presented at March ISC for approval.
2, 4	Data Classification	PO has had a classification scheme for a long time but colleagues do not habitually adhere to it. In order to implement any data leakage product successfully a sister programme is required to enforce better usage of our classification scheme. The DLP paper mentioned above also covers options for enforcement of data classification.
3	Security Culture	Campaign is underway. Information Security and GDPR awareness days scheduled for March in all support offices.
2,3	2 Factor Authentication	Passwords are recognised as not being secure enough to protect critical assets. Post Office need to better protect our remote access and should therefore implement a second level of protection. IT Security are assessing the impact to the business and a proposal for implementation will be delivered during Q1 18/19.
2, 3	Single Sign-on	IT Security in conjunction with Enterprise Architecture will be assessing the impact to the business during Q1 18/19.
3	Information Security Technical Standards	IT Security are fully committed with operational priorities. This will be revisited Q1 18/19.
1	Protection of postoffice.co.uk domain.	IT Security have identified a need to better protect our domain name to stop abuse of both the website and e-mails we send out to our

POL00401626

Risk Number	Remediation	Progress Update
		customers. Papers will be prepared and socialised Q1 18/19.

What steps are taken to keep abreast of the risk threat horizon?

IPA, IT and IT Security hold monthly risk meetings to:

- Identify new and emerging risks, allocate accountable leads and set milestones/deadlines;
- Review internal and 3rd Party Supplier Information Security Reports against our current risk appetite;
- Update on progress with existing risks and agree future activities;
- Test the validity and performance of existing controls, setting new actions where necessary; and
- Developing KRI to act as early warning systems to generate interventions.

The meetings are chaired by Heads of Department, where a strict governance process is followed to ensure risks are managed in-line with appetite, reviewed cohesively and only tolerated when there is sufficient evidence to suggest that the risk is mitigated.

All activity is recorded on the respective Risk Registers to ensure we have a transparent and auditable process.

The levels of confidence IPA and IT Security have over the levels of protection that our 3rd party suppliers is improving from its previous low position, this is due to the work being carried out through the SOC implementation and the visibility this affords Post Office over technical controls such as Firewalls. Work has been progressing during 2017/18 to set expectations within our critical supplier

What will our risk profile look like once all the current plans have been completed?

Without doubt, the completion of actions to a time and quality that we agree will lower the likelihood of risks materialising and in some cases, lower the impact. The implementation of the Advanced SOC and the fine tuning of alerting as a result of that, will be a significant step forward in protecting PO.

However, it is important to note that addressing impact is more complex due to the ever-changing risk landscape. As an example, having a complete and effective firewall estate may reduce the 'likelihood' of our defences being breached however, if breached, the impact would still remain 'high'.

To address the constant changing risk landscape it is vital that even once actions have been completed, there is a process of 'control re-assessment' to ensure that our defences are relevant and current. IPA, IT and IT Risk fully accept this and periodically reassess controls whether those controls are owned by ourselves of 3rd Party Suppliers.

Monitoring of our performance and the effectiveness of controls in now managed through new Risk Reporting Dashboards.

POL00401626

Risk Placemat, including an update on Risk Exceptions

Author: Richard Williams/Deana Herley Sponsor: Jane MacLeod Meeting date: 13 March 2018

Executive Summary

Context

The purpose of this paper is to provide the RCC with the latest version of the Placemat, which now includes the results from Financial Services & Telecoms (FS&T), POMS and Retail. The Q4 reassessment of risks has been performed with Finance and Operations (F&O) and Legal, Risk & Governance (LRG), with Government and Payment Services (G&PS) and Telecoms also reflected on the Placemat. The paper will also update the RCC on the the final 20% phase of the Placemat approach and a current status of Risk Exceptions.

Questions this paper addresses

- What are the results of rolling out the placemat in FS&T, POMS and Retail?
- What does the Q4 reassessment of risks tell us?
- What are the next steps in rolling out the placemat approach?
- What is the current status of Risk Exceptions?

Conclusion

1. FS&T has identified 155 risks overall, which includes Banking Services, with 8 top FS&T risks (8 red). POMS has identified 82 risks overall with 6 top risks (4 red, 2 amber). To date, as a start Retail has identified 132 risks within each team. Debbie Smith will present the top down view at the next RCC in May.
2. Since the Q3 reassessment, out of 32 top risks, 41% of the F&O risk profile has changed, with better processes and controls leading to reductions in 5 risks, most notably to cash management, client settlement and the appointment of agents. 7 risks have increased in the period and 1 new risk has been identified relating to instability of the NBSC telephony system. For LRG, out of 10 top risks, there has been a slight change in the risk profile, as mitigating actions continue to be progressed. The GDPR risk score has increased due to delay in getting additional team resource due to the very high demand for such technical expertise.
3. The final phase of the Placemat approach will be rolled out in April/May to the teams in IT, HR, Comms, Strategy and Identity Services.
4. There are 3 current Risk Exceptions for noting.

Input Sought

5. The Committee is asked to review and comment on the report.

POL00401626

The Report

What are the results of rolling out the placemat in FS&T, POMS and Retail?

FS&T

6. FS&T has provided a consolidated top down view of their respective risk and controls. A total of 155 risks have been identified, which includes Banking Services, with 8 top FS&T risks (8 red). The highest scoring risks in the profile are as follows:
   - PCI DSS non Compliance for Post Office (5x4 same risk as Banking Services): This risk is scored highly because of the contractual requirements of the Banking Framework. Following a PCI Audit in December, the planned remediation requirements to certification are scheduled to be in place by the end of March 2018, working with the Information Protection and Assurance Team.
   - GDPR Compliance for Telecoms (4x4): Post Office is the data controller for customer data but we are largely reliant on Fujitsu to ensure compliance with GDPR. There is a risk that we will not meet GDPR requirements because of the lack of capacity at Fujitsu to make the changes. The Telecoms Team, FS&T Risk and Post Office's GDPR team are working together on the remediation plan.
   - Customer Hub (4x4): Whilst the Customer Hub establishes itself, there are a series of programme and wider stakeholder engagement risks to be managed, mitigated and controls to be put in place. These include operational functionality and aligning them to business requirements, contractual risks, relationships with third parties and managing compliance, including regulatory requirements and data security standards.
   - Travel Money AML (4x4): The HMRC audit (Jan 17) identified that Post Office is not collecting nor can it evidence the required information in respect of our bureau transactions. A plan of improving controls was agreed with the regulator. There remains a risk we will not meet the timescales or required solution to HMRC audit requirements for Travel Money. The risk has increased as HMRC appears to be changing its position in relation to KYC record requirements. There is a remedial plan in place overseen by the Financial Crime team, which includes regular engagement meetings with HMRC.
   - Business Continuity Planning (5x3): Whilst the outsourced business centres, such as BoI, Fujitsu and FRES, have BCP plans it is unclear to the management of FS&T what the overall arrangements are, how we gain comfort that these are adequate and what the local arrangements are for staff members and how these are tested.
   - Regulation (3x4): There is a risk that the on-going growth in regulation in FS&T increases the risk of non-compliance and/or making various business activities unprofitable. Regulatory initiatives such as price caps on BT for home

POL00401626

phone-only contracts and automatic compensation risk significant impact on our costs and margin.

- Senior Manager and Certification Regime (4x3): Whilst POMS will be subject to this regime (timetabling yet to be determined by the FCA) there could be significant impacts on FS&T (and Post Office) as an Appointed Representative (AR) and supplier. This includes the need to ensure that responsibilities for all activities caught by the regime (vetting, conduct rules for a wide set of employees, systems and controls) can meet the SMCR requirements of POMS. POMS has an SMCR action plan in place.
- Key Person Risk (4x3 same risk as Banking Services): A significant amount of business knowledge and experience is covered by a few key individuals in FS&T, which, if they left the business, could have a significant detrimental impact on the ability of FS&T to complete its objectives. Following the recent changes to the management structure the team will be reviewing succession planning and retention measures.

POMS

7. POMS has provided a consolidated top down view of their respective risk and controls and has built on an existing risk management framework. POMS has identified 82 risks overall with 6 top risks (4 red, 2 amber). The highest scoring in the profile are as follows:
   - Marketing capacity and capability (4x3): POMS is currently recruiting approximately 12 staff to ensure its marketing needs can be met. The lack of sufficient and capable resource within the central marketing team with the required skill sets to deliver the POMS marketing plan may result in an under performance against the stated plan.
   - GDPR Compliance (3x4): Whilst progress is being made within the GDPR project, with both privacy notices and our approach to permissions nearing completion at the time of writing. Benchmarking with other insurers and via our new ABI membership has proven useful in moving the project forward. Uncertainty remains over readiness to comply with or understand the impact and costs associated with GDPR and DPA.
   - AR compliance (4X3): POMS has regulatory responsibility for the regulated activity of it's AR. There is a risk relating to PO's inability to provide assurance to POMS that its activities are is compliant. This includes: training, vetting, oversight, reporting and performance management/incentives. A separate list of PO risks has been created. A number of actions need to be undertaken if POMS is to be able to demonstrate it has a fully effective AR control framework. These include:
     - Conduct MI for use by POMS is being restructured and the revised MI set is on track for delivery by the end of March.

POL00401626

  - The branch review process is being restructured, and consideration is being given as to the overall approach to mystery shopping and how this might be better coordinated with our branch reviews.
  - EUM will create an ability to ensure all staff have been subject to proper fit and proper checks and have undertaken adequate training. Without the completion of adequate training or fit and proper checks, staff will not be able to access the system for these products. The EUM project is on track for material delivery by the end of July 2018. POMS management are obtaining regular updates regarding the EUM project which are also being reviewed by the Non-Executive Directors (NEDs).
- POMS strategy (4x3): The POMS strategy has been produced and is currently awaiting POL approval, which is expected by the end of March 2018. The strategy will highlight the key targets that POMS will be expected to achieve going forward.
- Senior Management Regime (SMR) readiness (3x3): The SMR will need to be introduced by late 2018.
- IDD readiness (3x3): EIOPA introduced the Insurance Distribution Directive to replace the Insurance Mediation Directive and is due to be enacted into local regulation by February 2018.

Retail

8. To date, Retail has identified 132 risks within each team. Debbie Smith will present the top down view at the May RCC. The risks cover the teams led by Mark Siviter (Mails and Retail), Roger Gale (Network and Sales), Tom Moran (Network Development), Tom Wechsler (G&PS) and Martin Kearsley (Banking Services). Debbie Smith will present the "top down" view at the May RCC. The rollout of the placemat to Mails, Network Sales and Network Development has built on the existing risk management framework. The Q4 reassessment in Government and Payment Services (G&PS) has further enhanced risk awareness. The highest scoring risks in the profile are as follows:

   Mails and Retail
   - RM renegotiation (4x2): A significant amount of work has gone into Mails renegotiation readiness, but uncertainties continue to exist over our current agreement with Royal Mail beyond 2020, until an outcome is reached. The existing MDA will require better alignment to today's market challenges.
   - Product Risk: 30% of net risks in Mails relate to Product Risk resulting in a loss of revenue and footfall, with customers likely to migrate from RM to competitors as well as, general market declines in lottery, retail and stamp sales.

POL00401626

Network Development

- Retail Proposition and Network Sustainability (5x3): There have been significant developments in almost all areas relevant to the Retail business area and this is reflected in the risks being managed by Network Development. The most significant relates to the attractiveness of the Post Office proposition to Retailers, which is being addressed through a fundamental reassessment of our Retail Network Strategy.
- HNGT (4x3): There is a risk that HNGT cannot deliver the new simpler operating model for agents and POL due to operational and financial constraints.
- Employment Status (5x2): The employment status of Postmasters remains under ongoing review, a risk which carries a significant impact but low likelihood.

Banking Services

The rollout of the placemat in Banking Services was conducted by FS&T Risk (now part of LRG) in collaboration with the Central Risk team and who continue to support Banking Services going forward. The highest scoring risks in the profile are:

- PCI DSS non Compliance for Post Office (5x4 same risk as FS&T): This risk is scored highly because of the contractual requirements of the Banking Framework. Following a PCI Audit in December, the planned remediation requirements to certification are scheduled to be in place by the end of March 2018, working with the Information Protection and Assurance Team.
- Cheque Clearing (3x5): Provider, Barclays Bank, is to change cheque clearing sub-contractor (from iPSL in Northampton to Parseq in Rotherham) which will negatively impact SLAs and cause disruption for the Banking Framework. The Banking Services team is working on mitigating disruption together with Royal Mail.
- Key Person Risk (4x3 same risk as FS&T): A significant amount of business knowledge and experience is covered by a few key individuals, which, if they left the business, could have a significant detrimental impact on the ability to complete objectives. Following the recent changes to management structure the team will be reviewing succession planning and retention measures.

G&PS

There are 15 existing top risks. Since the Q3 reassessment, 8 new risks have been identified and 5 closed or transferred. The highest scoring Q3 risk relating to the POca procurement has been closed, while the majority of the risk relating to AEI infrastructure has been transferred to the new Identity Services team:

- ATM industry (4x4): Wider changes in the ATM industry and market may lead to BOI invoking a renegotiation of the ATM agreement.
- PCI DSS noncompliance for Post Office (4x4): There is a risk that the business will not complete the remediation activities needed to meet PCI DSS within

POL00401626

the extended timeframe of 31st March, which would jeopardise current and prospective G&PS client business.

- TLS upgrade (5x3): The Transport Layer Security (TLS) upgrade may not meet the deadline of 20th May 2018. If we do not meet the deadline, there is a risk we will not be able to process card payments for G&PS clients (e.g. BT, DVLA)
- POca contract (4x3): The contract becomes loss making towards the end of the main term with a corresponding loss of branch footfall from POca customers. A 'Future of POca' programme has been established to develop future products for this customer group.
- ATM operational availability (3x4): ATM operational availability continues to be a concern. The Post Office Service Team is now in place and improvements taken and underway are starting to be reflected in performance improvements.

Network and Sales

- Failure of IT infrastructure (5x3): The most significant risk for Network and Sales continues to be the reliability and recoverability of IT infrastructure. The size of the overall branch network makes it resilient to most operational issues other than complete system failure, but if whole sub-networks of branches with specialised equipment such AEI kit are affected, customer disruption could be severe.
- Reduction in agent remuneration (5x3): Reduction in agents' remuneration makes branches less sustainable and this could lead to a reduction in staff numbers with a negative impact on customer experience.
- Proposed changes to Directly Managed Branches (4x3): On-going changes to the DMB network continue to carry a reputational risk.
- Managing change (3x4): In common with other business areas, Network and Sales is vulnerable to changes to products, processes or systems which have a negative impact on customer experience in branch. On-going changes to the Directly Managed Branch network continue to carry a reputational risk.
- Retail supply of Postpak (3x4): Current challenges with the supply of Postpak retail items pose a risk to sales and customer experience, but work is underway with the Mails team and WH Smith to resolve the supply issues.

What does the Q4 reassessment of risks tell us?

9. Since the Q3 reassessment in November 2017, risk registers covering 22 teams have been formally reviewed with senior management. The most notable changes to the "top risks" for F&O and LRG are as follows:

F&O

There are 32 existing top risks. Since the Q3 reassessment, 41% of the F&O risk profile has changed, with better processes and controls leading to reductions in 6 risks, most notably to cash management, client settlement and the appointment of agents. 7 risks have increased in the period and 1 new risk has been identified

POL00401626

relating to instability of the NBSC telephony system (3x2). Key elements of the F&O risk profile are as follows:

- Legacy Systems (4x2 from 4x3): Good progress has been made towards reducing the risks posed by aged IT systems with the successful transfer from HRSAP of staff payroll to SuccessFactors and agents' remuneration to CFS. POLSAP and legacy systems at Swindon remain vulnerable and the overall risk is unchanged.
- Health and Safety (5x3 from 5x2): An increase in small accidents in Supply Chain has resulted in an increased score. A proactive approach to health and safety management is being rolled out across Supply Chain, including training Safety Champions in each business unit and setting up a Safety Forum to provide support and guidance.
- Agent Theft and Fraud (3x5 from 2x5): A significant increase in agent debt compared to last year means this is now one of the highest scoring risks in the F&O risk profile. Improvements in detection of fraud and better control of cash are helping to limit the consequences of fraud, but the key driver continues to be the inability to prosecute.
- Management information (3x5 from 2x5): This risk has been scored higher to reflect the importance of management information in driving business improvements. The Data Governance project (Arrow) has been initiated and a Data Strategy will be presented in March 2018.
- Business Continuity (4x3 from 3x3): Business continuity is an increasing risk because of the aged systems and untested plans. Plans are in place to test Chesterfield in March and Bolton in April 2018.

<u>LRG</u>

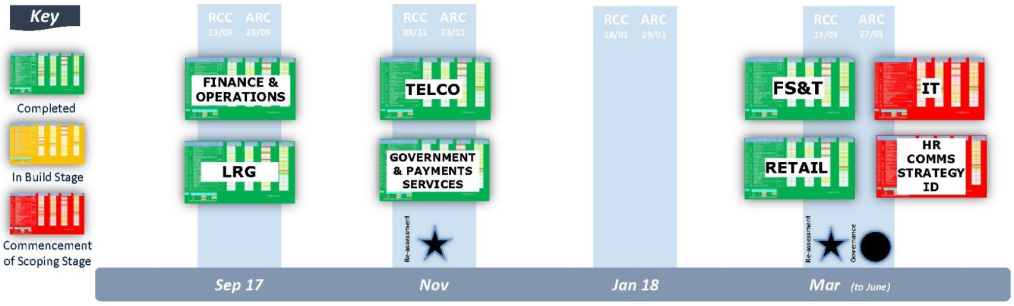
There are 10 existing top risks. Since the Q3 reassessment, 20% of the LRG risk profile has changed, most notably to GDPR (4x4 from 3x3). Key elements of the LRG risk profile are as follows:

- PCI accreditation (5x4 no change): Progress is being made towards reducing the risk with actions plans in place to remediate the shortcomings identified in the audit. Fujitsu and Computacentre are also involved in the remediation and audits continue across the network. There is a dependence on Computacentre to deliver remediation activities, confidence in which is currently low.
- GDPR (4x4 from 3x3): A lack of documentation, scale and complexity and capacity in the BAU DP Team has increased the likelihood. Recruitment is underway for interim Data Protection SMEs which are scarce due to demand in other GDPR programmes.
- Insider threat (4x3 no change): Progress to date include the signing of the Verizon contract to establish a Security Operations Centre, which will provide oversight of all security controls from each provider, centralise and aggregate events and incidents to enable POL to react against security issues efficiently and effectively, thereby reducing our risk exposure.

POL00401626

What are the next steps in enhancing the roll out?

10. The final phase of the Placemat approach will be rolled out to teams in IT, HR, Comms, Strategy and Identity Services; an update will be provided for May RCC.



What is the current status of Risk Exceptions?

11. The current approved Risk Exceptions are as follows:

Title	Risk	Category	GE Owner	Accountable owner	Date Raised	Closure Date	Actions	Due Date	Status/ Update
Robotic Process Automation (RPA) Live Operation - Finance Service Centre	There is a risk of loss of data /service as the RPA software is running on stand-alone desktop machines, which are not backed-up, have no UPS and have no provision for real time resilience.	Policy	Al Cameron	Angela Van-Den-Bogerd	29-Nov-16	31-Dec-17	Migrate to a permanent infrastructure.	31-Dec-17	**On-going.** Risk Exception is being renewed with detailed actions and timelines. Business was pursuing a hosted solution. Accenture have returned with a reduced cost proposal which looks like it will factor in to the existing budget. Detailed time frame will be assessed and included in the revised Exception.
SalesForce – Procurement	Contract has been renewed /extended non-compliantly for a period of 12 months.	Regulatory	Owen Woodley	Chrysanthy Pispinis	21-Apr-17	29-Apr-18	POL should seek to run a full compliant procurement as soon as possible to reduce the risk of a challenge.	29-Apr-18	**On-going.** The business requirements for Salesforce have been included in the scope of the CDP Procurement, which has recently been awarded to Accenture. A Change Request has been submitted into Accenture and is under review by both legal teams. On-track to deliver by end of April 2018
Success Factors	Implementation of Success Factors without addressing certain data protection and information security risks could result in breach of data protection regulation and Post Office policy requirements as line managers can download, copy, export and distribute, personal data of their team members, via non-corporate devices.	Regulatory	Martin Kirke	Martyn Lewis	02-Jan-18	30-Jun-18	Directive from the Group HR Director for a declaration to be signed by the staff in HR Service Centre	08-Jan-18	**Closed -** HRSC team have all signed the declaration.
							Weekly report to monitor access via IP addresses of non-corporate devices	w/c 08-Jan-2018	**Closed–** No longer required due to action 3.
							Installation of a password manager	26-Jan-18	**Closed -** Password Manager App has now been deployed to the HRSC team, meaning a technical restriction is now in place for this population. This will remain until the corporate solution is identified.
							Suitable training and information during the roll out of SuccessFactors to all line managers and new joiners.	08-Jan-18	Measures to be put in place : - **Closed.** Data Protection statement screen when logging on. - **On-going, to be included in the 18/19 compliance test.** Compliance training Info Sec/DP, updated module content to reflect. - **Closed.** Further training and comms have been issued to the HRSC team to strengthen operational controls.
							A corporate solution (combination of SSO/BYOD)	30-Jun-18	**On-going** - The JML project has run a design on SSO/Provisioning that we believe will solve this issue. design documents are now with The CTO for review. - The business case is being updated to include this work and is expected to be submitted this week (w/e - 3/3/18). - Technical work can begin once design is complete and funding is agreed. - At this stage we believe significant progress will have been made by June, reducing this wider risk for our business.

POL00401626

Appendices

1: Placemat
2: Financial Services and Telecoms results
3: POMS results
4a: Mails and Retail
4b: Network Development
4c: Banking Services
4d: G&PS
4e: Network and Sales
5: Finance and Operations Q4 refresh
6: Legal, Risk and Governance Q4 refresh

POL00401626

Appendix 1

Placemat - RCC 12/3/2018

Ref		Principal Risks	GE Owner	Retail: Mails and Retail Q4 18	Retail: Mails and Retail Influencing Factor	Retail: Network Development Q4 18	Retail: Network Development Influencing Factor	Retail: Banking Services Q4 18	Retail: Banking Services Influencing Factor	Retail: Government and Payment Services Q4 18	Retail: Government and Payment Services Influencing Factor	Retail: Network Sales Q4 18	Retail: Network Sales Influencing Factor	Financial Services and Telecoms Q4 17	Financial Services and Telecoms Influencing Factor	POMS Q4 17	POMS Influencing Factor	Finance & Operations Q3 17	Finance & Operations Q4 17	Finance & Operations Influencing Factor	Legal, Risk and Governance Q3 17	Legal, Risk and Governance Q4 17	Legal, Risk and Governance Influencing Factor	Principal Risks	Ref	Risk Appetite - Mar 2015: Averse	Neutral	Tolerant	Seeking
1		Manage process and deliver services	TBC	2	Transition of retail to WHSmiths	2	Employment status	1	Knowledge risk on key man dependency / Demand for Banking Services	2	Transport Layer Security upgrade / ATM availability	2	Customer experience	1	Knowledge risk on key man dependency			2	2	Supporting agents				Manage process and deliver services	1				
2		Product risk	OW / DS	2	Decline in revenue - stamps, lottery and retail																			Product risk	2				
3		Make payments	AC															2	3	Client settlement				Make payments	3				
4		Records management	TBC																					Records management	4				
5	OPERATIONAL	Procure	AC							2	Replacement of Paystation							2	2	Procure badly				Procure	5				
6	OPERATIONAL	Contract Management	All	2	MDA			2	Barclays IPSL relationship	2	Non-compliance in Branch	2	Gaps in Postfish								2	2	Contract non-compliance	Contract Management	6				
7	OPERATIONAL	Managing change	AC			2	HNGT programme and volume of change	2	HDRC upgrade / Atos capacity			2	Potential industrial action	2	Horizon development			1	2	POLSAP / Legacy Systems				Managing change	7				
8	OPERATIONAL	Keep our people, customers & 3rd parties safe	AC									2	Security guidelines in branches					2	2	Increase in small accidents (SIC)				Keep our people, customers & 3rd parties safe	8				
9	OPERATIONAL	Physically secure	AC															3	3	Cash centre security				Physically secure	9				
10	OPERATIONAL	BCP (excel ITDR)	JMaC							2	No contracts for some clients			1	Infrastructure Failure (Lack of BCP)			2	2	BCP Plans / Swindon	2	2	BCP arrangements	BCP (excel ITDR)	10				
11	TECH	Technology Ops	RH									2	Branch technology refresh											Technology Ops	11				
12	TECH	Business Interruption (ITDR)	RH									2	Disruption to Network					2	2	POLSAP/Telephony system				Business Interruption (ITDR)	12				
13	TECH	IT Security	RH																		2	2	Cyber Threat	IT Security	13				
14	TECH	Dependence on IT 3rd Parties	RH																					Dependence on IT 3rd Parties	14				
15	LEGAL & REGULATORY	Managing losses and Fraud	AC					3	Splitting transactions					2	Vulnerable customers			2	2	Agent fraud				Managing losses and Fraud	15				
16	LEGAL & REGULATORY	Financial Crime	JMaC	2	Gift cards for money laundering			2	SYSC 6					2	HMRC Audit						2	2		Financial Crime	16				
17	LEGAL & REGULATORY	Information Protection	JMaC					1	PCI compliance	2	PCI compliance			1	PCI / GDPR compliance	2	GDPR	2	2		2	2	PCIDSS / GDPR	Information Protection	17				
18	LEGAL & REGULATORY	Brand	MD																					Brand	18				
19	LEGAL & REGULATORY	Record and pay taxes	AC															2	2	Resource changes				Record and pay taxes	19				
20	LEGAL & REGULATORY	Litigation	JMaC																		3	3	Incessing : Postmaster Litigation	Litigation	20				
21	LEGAL & REGULATORY	Governance	JMaC					3	Banking Reform							2	AR				2	2	Risk mgt & policies	Governance	21				
22	LEGAL & REGULATORY	Compliance with laws and regulations	JMaC	2	MDA change request					2	ATM exemption	2	Mis-selling of easy life product	2	SMR / Telco Reg Regime	2	SMR and IDD	2	2	EUM roll-out not yet complete	2	2	Increased visibility to Regulators	Compliance with laws and regulations	22				
23	FINANCIAL	Reporting results and providing data accurately	AC	1	Credence reporting													2	2	MI / Forecasting				Reporting results and providing data accurately	23				
24	FINANCIAL	Sufficient cash / headroom	AC															2	2	Cash data / Mgt of cash				Sufficient cash / headroom	24				
25	FINANCIAL	Ensuring sustainable profit	AC			3	NFSP relationship / Model profitability and consentration			2	ATM industry changes / ATM Availability / POCA	2	Reduction in agent remuneration					2	2	Insurance Coverage				Ensuring sustainable profit	25				
26	FINANCIAL	Control activities	AC															2	2	Informal controls in FSC				Control activities	26				
27	STRATEGY	Competitiveness	OW/DS	2	RM customer acquisition strategy	2	Retail proposition and Network Sustainability			2	Bill payments market / contract exchange / CMA conditions	2	Customer feedback methodology	2	Wholesale fibre customer retention									Competitiveness	27				
28	STRATEGY	Strategic Risk	OW/DS	2	RM renegotiation									2	Failure of Customer Hub	2	POMS strategy sign off							Strategic Risk	28				
29	STRATEGY	Market	OW/DS																					Market	29				
30	STRATEGY	Customer Relevance	OW/DS																					Customer Relevance	30				
31	PEOPLE	Communicate, inspire and align	TBC	2	Employee engagement	3	Capacity, capability and engagement					2	Uncertain future and lack of development opportunities			2	Marketing resource	2	2	Supply Chain / SecOp comms on front line				Communicate, inspire and align	31				

Key	Risk & Control Status	Harm Tarsie (U/L) Minimum Score	RAG	Control Effectiveness Score	RAG
	Low	1	G	1	R
	Medium	6	A	2	A
	High	11	R	3	G
	Risk n/a				

Colour indicates net risk score / Number equals control effectiveness

POL00401626

Appendix 2

FS&T Dashboard

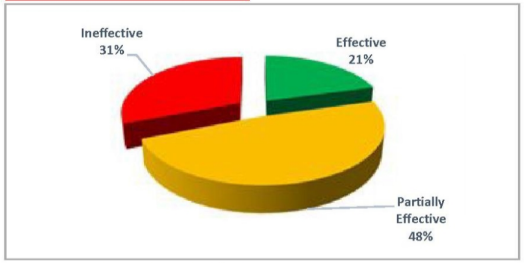
Top Risks by Risk Score

#	Sub-Risk Title	Risk description	CSA	Residual Risk Score	Commentary
1	Information Protection	PCI auditors identified remediation activities that will go beyond the date (28th December 2017) that our Report of Compliance (RoC) should be completed .The outcome of the audit , PO has failed to obtain the required PCI -DSS certification. This is a breach of our agreed banking framework and may lead to a legal/regulatory breach, financial loss and reputational damage. If Post Office fails to ensure operational activities, IT infrastructure/security and related services are PCI-DSS compliant it cause challenges during external audit, and require significant remediation actions, attracting unbudgeted costs.	1	20	PCI certification is critical to the Post Office. PCI audit remediation activities will go beyond the date (28th December 2017) that our Report of Compliance (RoC) should be completed .The outcome of the audit , PO has failed to obtain the required PCI -DSS certification. This is a breach of our agreed banking framework and may lead to a legal/regulatory breach, financial loss and reputational damage. If Post Office fails to ensure operational activities, IT infrastructure/security and related services are PCI-DSS compliant it cause challenges during external audit, and require significant remediation actions, attracting unbudgeted costs. We have formed a steering committee to oversee remediation activities. RCC is receiving regular updates and we are aiming to achieve PCI certification by or before 31 March 2018.
2	Information Protection	Failure of Fujitsu to have the correct controls and processes in place to meet the new requirements of General Data Protection Regulation in 2018 (GDPR) . Failure to do so will result in loss of global turnover of between 2%-4%.	2	16	Post Office needs to be compliant with GDPR by May 2018. Post Office is the data controller for customer data but we are largely reliant on Fujitsu to ensure compliance with GDPR. There is a risk that we will not meet GDPR requirements because of the lack of capacity at Fujitsu to make the changes. The Telecoms Team, FS&T Risk and Post Office's GDPR team are working together on the remediation plan.
3	Strategic Risk	Failure to operationalise the hub to meet business requirements due to inadequate alignment to business, lack of governance and controls or third party and contractual risks	2	16	The hub is an innovative digital programme (Post Office in your pocket) to support customers and help move Post Office further up the value chain. Whilst it establishes itself there are a series of programme and wider risks to be managed. These include operational functionality and aligning them to business requirements, contractual risks, relationships with third parties and managing compliance, including regulatory requirements and data security standards. The FS&T Risk team is working with the Hub business and programme teams to ensure controls are put in place to mitigate this risks, whilst supporting an agile approach. This includes ensuring that the programme engages with stakeholders across the Post Office.
4	Financial Crime	(A) The HMRC audit (Jan 17) identified we are not collecting or can evidence the required information in respect of our bureau transactions. FRES13(B) Risk we may not delivery the required changes within the deadlines outlined in the plan . HMRC have made is clear that there is zero tolerance in respect of missing these deadlines.	2	16	The HMRC audit (Jan 17) identified that Post Office is not collecting nor can evidence the required information in respect of our bureau transactions. A plan of improving controls was agreed with the regulator. There remains a risk we will not meet the timescales or required solution to HMRC audit requirements for Travel Money. This risk has increased as HMRC appears to be changing its position in relation to KYC record requirements. There is a remedial plan in place overseen by the Financial Crime team, which includes regular engagement meetings with HMRC.
5	BCP (excl ITDR)	Significant infrastructure failure-no effective Business Continuity programme for FS & T.	1	15	Business continuity planning is not only important for Post Office to continue its operations, it is also a contractual requirement across a number of contracts. Whilst the outsourced business centres, such as BoI, Fujitsu and FRES, have BCP plans it is unclear to the management of FS&T what the overall arrangements are, how we gain comfort that these are adequate and what the local arrangements are for staff members and how these are tested.
6	Compliance with laws and regulations	There is a risk that the on-going increase in regulation in FS (and Telecoms businesses) increases the risk of non-compliance and/or making various business activities unprofitable (e.g., Insurance Distribution Directive requirements). Regulatory risk from Ofcom activity e.g. review of general conditions, complaints, automatic compensation could lead to a drain on resources, increased costs to the business and impact on the change schedule.	2	12	There is a risk that the on-going growth in regulation in FS&T increases the risk of non-compliance and/or making various business activities unprofitable. Regulatory initiatives such as price caps on BT for home phone-only contracts and automatic compensation risk significant impact on our costs and margin. We undertake regulatory horizon scanning to anticipate future requirements and work with each business area to undertake appropriate solutions. We also have a planned budget for regulatory change, relationship with OFCOM. We have also recently recruited a Senior Risk & Compliance Manager for Telecoms.
7	Compliance with laws and regulations	Senior Managers and Certification Regime, PO are unprepared or can not deliver the extension of these requirements due in 2017 and 2018.	2	12	POMS will be subject to the Senior Manager and Certification Regime, there could be significant impacts on FS&T (and Post Office) as an Appointed Representative and supplier. This includes the need to ensure that responsibilities for all activities caught by the regime (vetting, conduct rules for a wide set of employees, systems and controls) can meet the SMCR requirements of POMS. Post Office and POMS are working together to ensure that Post Office is in a position to support POMS.
8	Manage process and deliver services	A significant amount of business knowledge and experience is covered by a few key individuals who if they left the business suddenly could impact significantly on the ability to complete our objectives.	1	12	A significant amount of business knowledge and experience is covered by a few key individuals in FS&T, which, if they left the business, could have a significant detrimental impact on the ability of FS&T to complete its objectives. Following the recent changes to management structure the team will be reviewing succession planning and retention measures.

Heatmap



Control Self Assessment



Risk Headline

No of Risks (Open or New)	155
No of Red Risks	21
No of Amber Risks	69
No of Green Risks	65
No of Red risks with ineffective controls	14
No of New Risks	49
No of Closed Risks	38

POL00401626

Appendix 3

POMS Dashboard

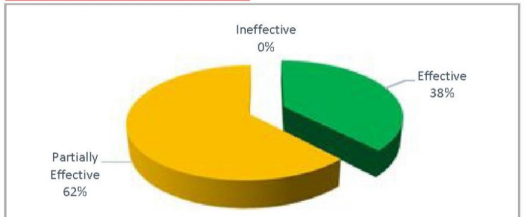
Top Risks by Risk Score

#	Sub-Risk Title	Risk description	CSA	Residual Risk Score	Commentary
1	Communicate, inspire and align	Lack of sufficient and capable resource within central marketing with the required skill sets to deliver the POMS marketing plan results in an under performance against our stated plan.	2	12	In 2017, there was a restructuring in the Post Office Marketing team and POMS is currently recruiting approximately 12 staff to ensure its marketing needs can be met.
2	Information Protection	Failure for readiness to comply with or understanding the impact and costs associated with GDPR and DPA - this could lead to financial penalties by our regulators and loss of reputation/confidence by customers affecting market share.	2	12	Progress is being made within the GDPR project, with both privacy notices and our approach to permissions nearing completion at the time of writing. Benchmarking with other insurers and via our new ABI membership has provided useful in moving the project forward.
3	Governance	POMS has regulatory responsibility for the regulated activity of it's AR. Given that there are over 11,000 agency branches, there is a risk that POL is unable to provide assurance to POMS that activity is compliant. This includes: training, vetting, oversight, reporting and performance management/incentives. N.B. A separate list of POL risks has been created.	2	12	It has been identified that a number of actions need to take place if POMS is to be able to demonstrate it has a fully effective AR control framework. These include: • Conduct MI for use by POMS is being restructured and the revised MI set is on track for delivery by the end of March. • The branch review process is in the process of being restructured, and consideration is being given as to the overall approach to mystery shopping and how this might be better coordinated with our branch reviews. • EUM will create an ability to ensure all staff have been subject to proper fit and proper checks and have undertaken adequate training. Without the completion of adequate training or fit and proper checks, staff will not be able to access the system for these products. The EUM project is on track for material delivery by the end of July 2018. POMS management are obtaining regular updates regarding the EUM project which are also being reviewed by the Non-Executive Directors (NEDs).
4	Strategic Risk	Risk that POMS Strategy/Business Plans (including Annual Operating Plan target) are not implemented completely and/or as per agreed deadlines.	2	12	The POMS strategy has been produced and is currently awaiting POL approval, which is expected by the end of March 2018. The strategy will highlight the key targets that POMS will be expected to achieve going forward.
5	Compliance with laws and regulations	The SMR will need to be introduced by late 2018 - there is a risk that POMS are not able to meet the requirements of SMR, leading to financial penalties.	3	9	HM Treasury announced that the SM&CR will apply to insurers from 10 December 2018. It is likely that insurance intermediaries (including POMS), will follow shortly after. There is therefore a need to ensure that we have a clear plan and timeline for SMCR deliverables, and that appropriate resources are applied to this work.
6	Compliance with laws and regulations	EIOPA introduced the Insurance Distribution Directive to replace the Insurance Mediation Directive and is due to be enacted into local regulation by February 2018. There is a risk that POM's are not able to meet the requirements of the IDD, leading to financial penalties.	2	9	Following the revision of the IDD delivery date to 1 October 2018 POMS has spent time re-planning the deliverables required to ensure Compliance. At this stage the project is green and on track. Work is also ongoing to ensure that the web based process is optimised within the requirements of IDD.

Heatmap



Control Self Assessment



Risk Headline

No of Risks (Open or New)	82
No of Red Risks	6
No of Amber Risks	61
No of Green Risks	15
No of Red risks with ineffective controls	0
No of New Risks	0
No of Closed Risks	0

POL00401626

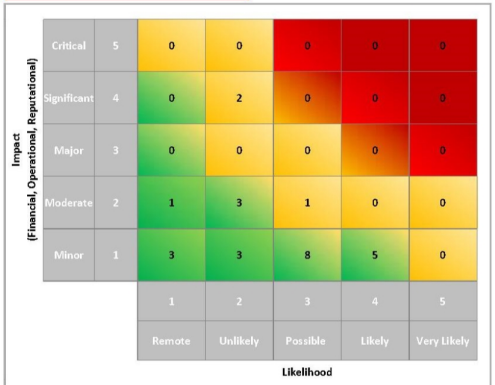
Appendix 4a

Retail – Mails and Retail Dashboard (1/5)

Top Risks by Risk Score

#	Principal Risk Title	Risk description	CSA	Residual Risk Score
1	Strategic Risk	New - Misalignment of objectives and unsuccessful renegotiation of MDA or negotiation of disadvantageous terms.	2	8
2	Strategic Risk	New - RMG give notice of termination of contract in 2020 which would involve us ceasing all existing mail services and seek a replacement possibly at a lower income rate.	2	8
3	Product risk	In branch fraud e.g. false accounting of stock resulting in financial loss to agent or PO.	2	6
4	Ensuring sustainable profit	Mail work negotiations leave Post Office less value in the proposition - c. £1-2m p.a. income below forecast.	2	4
5	Competitiveness	A competitor launches a Letter/Large Letter format product to compete with RMG resulting in a loss of revenue and income from the transaction as customers migrate.	3	4
6	Manage process and deliver services	Transitional arrangements for the handover to a new retail supplier lead to either no stock available for sale, or too much stock left over in branch.	2	4
7	Financial Crime	New - Customers purchase gift cards for the purpose of money laundering or financing terrorism.	2	4
8	Product risk	On-line Postage takes off faster as a result of increased differential channel pricing - projected impact of £1.8m	3	4
9	Contract Management	Product Team breach compliance requirements within the MDA (Change Request timelines not met) resulting in RMG reputational damage.	2	4
10	Product risk	Drop & Go - Errors in systems allow customers to go into a negative balance and can then be blocked.	2	4
11	Communicate, inspire and align	New - Poor employee engagement leads to low productivity and/or higher propensity to churn.	2	4
12	Manage process and deliver services	Customers defraud POL through misuse of the Cheque Authority Card processes resulting in losses due to funds being unrecoverable.	3	3
13	Product risk	RM's new 'confirmation of delivery' option will cannibalise SF and SD further than budgeted. Expected to be £1.3m (on top of £1.3m in budget).	3	3
14	Communicate, inspire and align	Projects may not deliver to time or quality as a result of reduced resourcing and potential conflicting time scales.	2	3
15	Competitiveness	RMG 'poach' customers through offering doing significant volume - POL earn £1.5m p.a. from customers who post 50+ items per week.	2	3

Heatmap



Risk Headline

No of Risks (Open or New)	26
No of Red Risks	0
No of Amber Risks	3
No of Green Risks	23
No of Red risks with ineffective controls	0
No of New Risks	4
No of Closed Risks	2

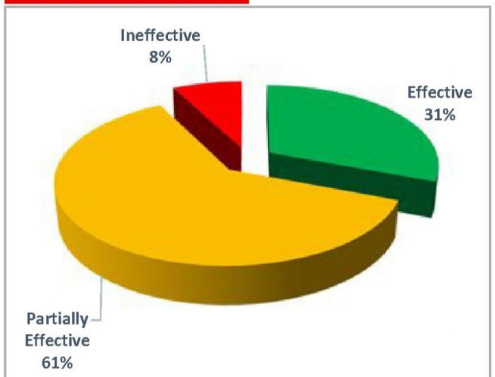
Control Headline

No of Risks assessed as effectively controlled	8
No of Risks Self assessed as partially controlled	16
No of Risks assessed as ineffectively controlled	2

Top Risks by Principal Title



Control Self Assessment



POL00401626

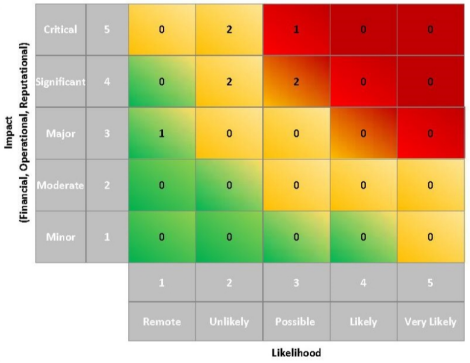
Appendix 4b

Retail – Network Development Dashboard (2/5)

Top Risks by Risk Score

#	Principal Risk Title	Risk description	CSA	Residual Risk Score
1	Competitiveness	New - Post Office's retail value proposition becomes insufficiently attractive to retailers result in shrinkage to our branch network and breach government commitments.	2	15
2	Managing change	New. HNGT does not deliver the new simpler operating model for agents and POL due to operational and financial constraints.	2	12
3	Managing change	New – The extensive change currently underway and planned within Post Office negatively impacts Postmasters and their business.	3	12
4	Manage process and deliver services	A successful challenge is made with regard to the employment status of postmasters such that they are categorised as employees or workers and Post Office becomes liable for additional cost.	2	10
5	Ensuring sustainable profit	New - One of our large multiple partners McColl's, Spar, One Stop, Co-Op resigns their Post Offices, damaging our reputation, proposition and may breach government commitment on network numbers.	3	10
6	Ensuring sustainable profit	The relationship with the NFSP becomes unworkable, resulting in an inadequate return on investment and need to cease funding.	3	8
7	Communicate, inspire and align	New - Poor employee engagement, lack of capacity or capacity leads to ineffectiveness low productivity and/or higher propensity to churn.	3	8
8	Ensuring sustainable profit	New - CWU Postmaster branches increases to 50% (plus) in membership, giving them a strong case for recognition, meaning PO would have to negotiate with another party.	3	3

Heatmap



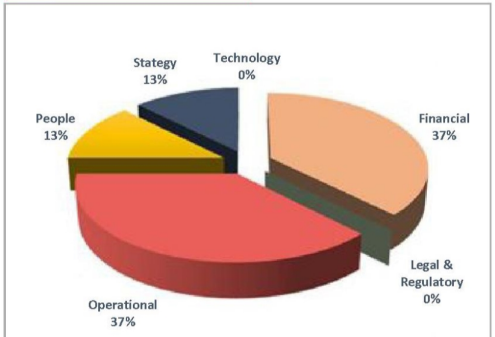
Risk Headline

No of Risks (Open or New)	8
No of Red Risks	3
No of Amber Risks	4
No of Green Risks	1
No of Red risks with ineffective controls	0
No of New Risks	6
No of Closed Risks	0

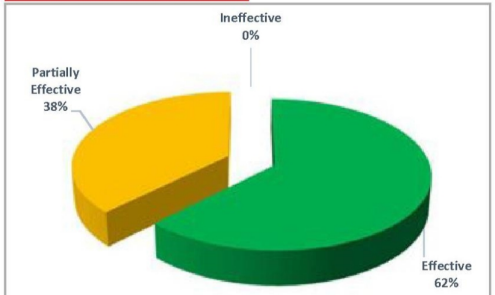
Control Headline

No of Risks assessed as effectively controlled	5
No of Risks Self assessed as partially controlled	3
No of Risks assessed as ineffectively controlled	0

Top Risks by Principal Title



Control Self Assessment



CONFIDENTIAL

POL00401626

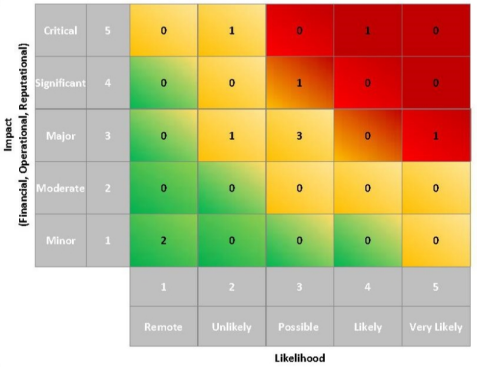
Appendix 4c

Retail - Banking Services Dashboard (3/5)

Top Risks by Risk Score

#	Sub-Risk Title	Risk description	CSA	Residual Risk Score
1	Information Protection	This is a breach of our agreed banking framework and may lead to a legal/regulatory breach, financial loss and reputational damage. If Post Office fails to ensure operational activities, IT infrastructure/security and related services are PCI-DSS compliant it cause challenges during external audit, and require significant remediation actions, attracting unbudgeted costs.	1	20
2	Contract Management	There is a risk that Barclays change of cheque clearing sub-contractor (from iPSL in Northampton to Parseq in Rotherham), due to the industry transition from paper to image clearing, will negatively impact our partner banks.	2	15
3	Manage process and deliver services	New - A significant amount of business knowledge and experience is covered by a few key individuals who if they left the business suddenly could impact significantly on the ability to complete our objectives.	1	12
4	Managing change	HDCR Programme Upgrade to PODG in March 2018. There is a risk that the testing to be undertaken fails to identify defects that could result in a loss of connectivity between POL and the client banks. A loss of connectivity would result in no client files being sent to circa 15 Banks, resulting in them being unable to reconcile customer accounts with deposits or charge them for using services such as Change Giving.	1	10
5	Financial Crime	SYSC 8 - Banking Framework has made a POL Board approved commitment to SYSC 8 (material outsource partners to banks). SYSC 8 requires auditable evidence of HR vetting for all counter based staff. This could be audited anytime from Jan 17 onwards, Current systems and processes offer limited scope for successfully achieving the required standard.	2	9
6	Managing change	ATOS Capacity and Capability to Deliver the Volume of Banking Services Projects with a high number of projects forecast to be delivered, there is a risk that anticipated timescales will not be achieved by ATOS and a further risk that where the team are stretched errors could occur which impact live services.	3	9
7	Contract Management	Link Members Council has discussed and agreed two candidate changes to the Link regulations. They are 1) Contactless ATM and 2) Settlement Disaggregation. The second of these could be significant for POL regarding how we clear and settle daily sums via Vocalink into the BOE RTGS system to banks. The main reason would seem to be a desire to ensure all scheme companies (LINK, FPS, BPSL etc.) remain totally arms-length from the Infrastructure companies . If this threat materialises for PO, it will have a major impact on our Banking and POCa transactions.	2	9
8	Manage process and deliver services	Increase in Banking Services demand through POL Network. Whilst this is great news for the business, there are risks that the increase in demand could adversely impact areas of the business, inclusive of: - An increased queuing time for services within POL Branches - Insufficient cash storage space within POL Branches - An increase in transactions being processed by the FSC that require intervention	3	6

Heatmap



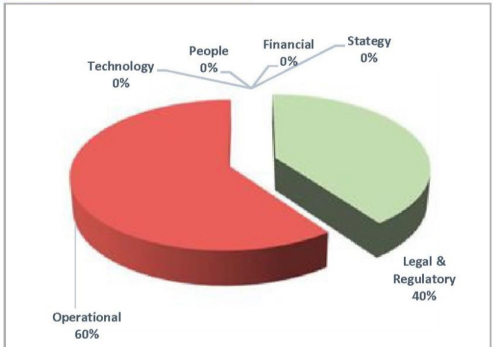
Risk Headline

No of Risks (Open or New)	10
No of Red Risks	3
No of Amber Risks	5
No of Green Risks	2
No of Red risks with ineffective controls	2
No of New Risks	1
No of Closed Risks	20

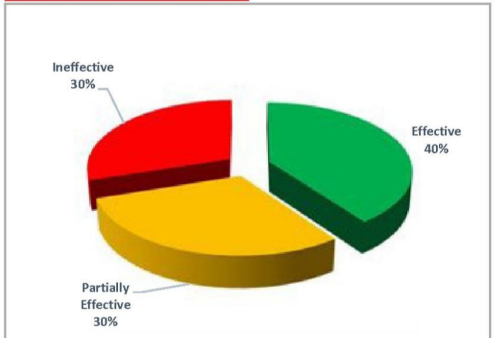
Control Headline

No of Risks assessed as effectively controlled	4
No of Risks assessed as partially controlled	3
No of Risks assessed as ineffectively controlled	3

Top Risks by Principal Title



Control Self Assessment



POL00401626

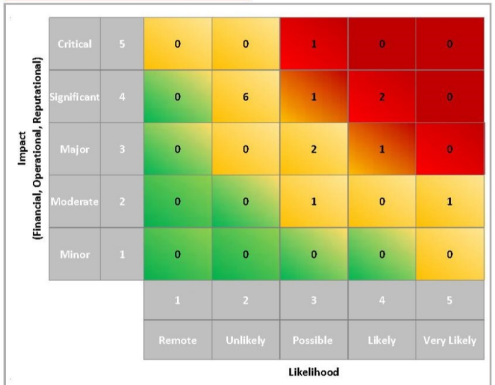
Appendix 4d

Retail - Government & Payment Services Dashboard (4/5)

Top Risks by Risk Score

#	Sub-Risk Title	Risk description	CSA	Residual Risk Score
1	Ensuring sustainable profit	New - Wider changes in the ATM industry and market will cause BOI to renegotiate the ATM Agreement to review the ATM model beyond 2022. They may also try to include as part of the wider changes/ business discussions with POL.	2	16
2	Information Protection	New - There is a risk that the business will not complete the remediation activities to meet PCI DSS (Payment Card Industry Data Security Standard) compliance within the extended timeframe (31st March 2018) which will jeopardise current and prospective G&PS client business.	2	16
3	Manage process and deliver services	New – There is a risk the Transport Layer Security (TLS) upgrade will not meet the deadline (20th May 2018). If we do not meet the deadline, there is a risk we will not be able to process card payments for G&PS clients (e.g. BT, DVLA).	2	15
4	Ensuring sustainable profit	New - There is a risk of the POca contract becoming a loss making contract towards the end of the main term (to November 2021) with a corresponding loss of branch footfall from POca customers.	2	12
5	Manage process and deliver services	ATM operational availability is less than 96% resulting in lost revenue.	2	12
6	Contract Management	Non-compliance in branch leads to breach of contract and financial penalties.	2	10
7	Compliance with laws and regulations	VOA reconsiders their operational decision to exclude Bank of Ireland ATMs in Post Office branches from separate assessment and agents become unwilling to host BoI ATMs.	2	9
8	Ensuring sustainable profit	There is a risk that non-cash payments costs are increasing due to unpredictable scheme fee changes and regulatory changes.	2	9
9	Manage process and deliver services	New - There is a risk that DVLA cease credit card as a payment method at Post Office branches due to an inability of POL to add the legislative charge for commercial cards.	2	8
10	Procure	Procurement exercise to replace PayStation by end May 2018 is unsuccessful and Ingenico ceases to service or support the current model, adversely impacting our ability to deliver bill payment services.	2	8
11	BCP (excl ITDR)	No known contracts in force for 45 client and supplier business relationships.	2	8
12	Competitiveness	We are unable to compete effectively in the bill payments marketplace and are unable to gain market share.	2	8
13	Competitiveness	New - Prior to contract exchange, market is informed of the deal before going public.	2	8

Heatmap



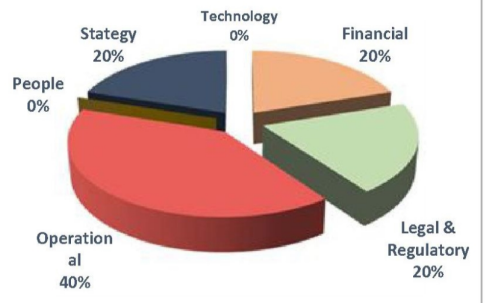
Risk Headline

No of Risks (Open or New)	15
No of Red Risks	5
No of Amber Risks	10
No of Green Risks	0
No of Red risks with ineffective controls	0
No of New Risks	8
No of Closed Risks	5

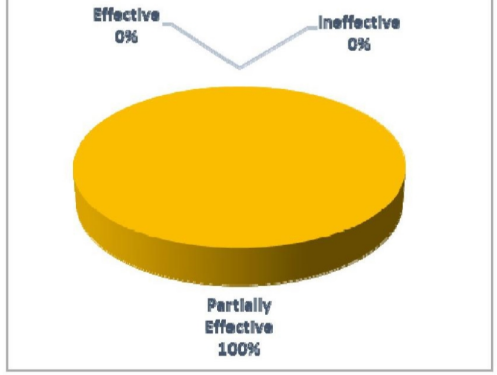
Control Headline

No of Risks assessed as effectively controlled	0
No of Risks Self assessed as partially controlled	15
No of Risks assessed as ineffectively controlled	0

Top Risks by Principal Title



Control Self Assessment



POL00401626

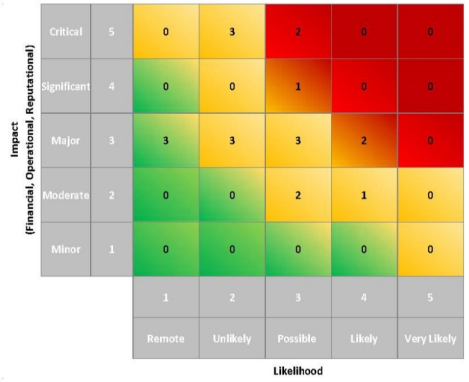
Appendix 4e

Retail – Network & Sales Dashboard (5/5)

Top Risks by Risk Score

#	Principal Risk Title	Risk description	CSA	Residual Risk Score
1	Business Interruption (ITDR)	Failure of IT infrastructure disrupts branch network leading to operational disruption and poor customer experience.	2	15
2	Ensuring sustainable profit	Reduction in agents' remuneration makes branches less sustainable and leads to reduction in staff numbers with negative impact on customer experience.	2	15
3	Managing change	Proposed changes to the Directly Managed Branch network and other business issues create stakeholder noise, which leads to reputational damage.	3	12
4	Contract Management	New - The transition of our retail offer now being provided by WHS has led to some initial gaps in our Postpak range with the risk to sales levels, commission and customer experience.	2	12
5	Managing change	New- Changes to products, processes or systems agreed in other parts of the business have a negative impact on customer experience in branch.	2	12
6	Compliance with laws and regulations	Failure to comply with legal or regulatory requirements, including mis-selling, non-compliant marketing and misuse of customer data, leading to poor customer experience and reputational damage.	3	10
7	Keep our people, customers and third parties safe	Risk of harm or breach of regulatory requirements caused by failure to follow Health and Safety procedures.	2	10
8	Compliance with laws and regulations	New-Serious regulatory breach involving customer detriment due to mis-selling of EasyLife product (term life assurance).	2	10
9	Technology Ops	New - Branch technology refresh causes unplanned operational disruption in DMBs.	2	9
10	Competitiveness	New - Changes in the methodology of gathering customer feedback result, could show a decline in feedback received and feedback becomes unrepresentative.	2	9
11	Communicate, inspire and align	New - Unable to influence whole network effectively to ensure consistent customer experience.	2	9
12	Managing change	Proposed changes to the Directly Managed Branch network lead to industrial action which causes operational disruption and reputational damage.	2	8
13	Communicate, inspire and align	Uncertainty around branch futures and a lack of suitable development opportunities lead to loss of key staff to other areas of the business or externally.	3	6
14	Keep our people, customers and third parties safe	New - Security risk due to inability to follow security guidelines at hosted branches because of difference in opening hours between PO and WHS host.	3	6

Heatmap



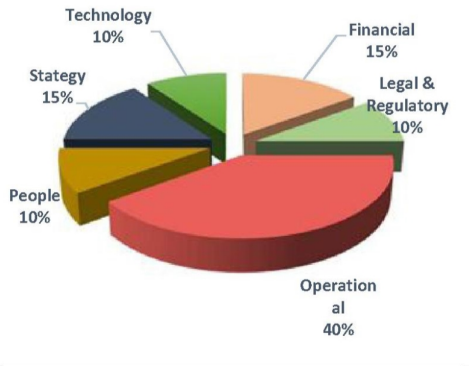
Risk Headline

No of Risks (Open or New)	20
No of Red Risks	5
No of Amber Risks	12
No of Green Risks	3
No of Red risks with ineffective controls	0
No of New Risks (8 top risks)	12
No of Closed Risks	0

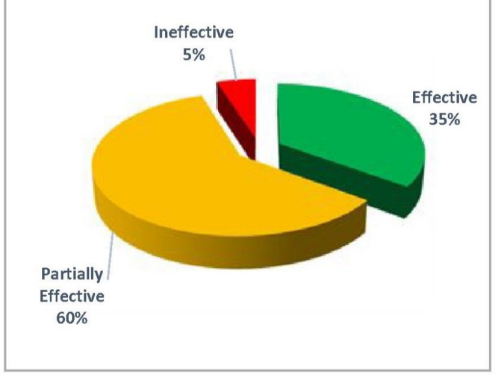
Control Headline

No of Risks assessed as effectively controlled	7
No of Risks Self assessed as partially controlled	12
No of Risks assessed as ineffectively controlled	1

Top Risks by Principal Title



Control Self Assessment



POL00401626

Appendix 5

F&O Dashboard

Top Risks by Risk Score

F&O Top Risks by Score						Q3			Q4				
#	Risk Description	Business Area	Principal Risk	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Impact	Likelihood	Risk Score	Q4 Commentary	Movement
1	High levels of change may cause fragile legacy systems to fail during the migration period.	Finance and Operations	Managing change	Ben Cooke	Tim White	4	4	16	4	4	16	HR SAP, which is out of extended support, is on track to be decommissioned following the deployment of SuccessFactors and expected migration of Agent Remuneration in February (see Risks 4 & 5). Our small apps (SQL & CRM) have been migrated into a secure data centre and consolidated. However areas of concern remain – the highest risks being POLSAP and legacy systems at Swindon. POLSAP is closely monitored and reported on with a number of remedial activities taking place and additional spares being procured. Plans to improve Swindon until a strategic solution is in place are progressing.	◁▷
2	Failure of POLSAP legacy system, results in severe operational disruption.	Finance and Operations	Business Interruption (ITDR)	Michael Passmore	Ben Cooke	5	3	15	5	3	15	The Back Office programme will migrate POLSAP to CFS. The programme scope covers a number of processes which drive our financials (e.g. client settlements, branch transaction corrections). Significant testing will take place and each area will be subject to a "go / no-go" decision by the programme team and Exec sponsors, where all risks will be discussed and 'go live' only approved if any remaining risks are extremely low. A controls specialist joined the programme team in November 2017 and has been overseeing the production of Business Process douments and documenting controls for each process impacted by the programme; the BPDs and controls matrices will all be reviewed and signed off by the Financial Accounting & Governance Manager and the Finance Director, POL. User access controls are also being developed with oversight from the controls specialist on the programme and the Financial Accounting & Governance Manager.	◁▷
3	Safety outcomes are not world class and where they are not in line with required legal and regulatory standards, may lead to serious injury.	Finance and Operations	Keep our people, customers and third parties safe	Angela Van-Den-Bogerd	Martin Hopcroft	5	2	10	5	3	15	Likelihood increased due to an increase in minor accidents in Supply Chain since the last refresh. Proactive approach to health and safety management being rolled out across Supply Chain, including training Safety Champions in each business unit and setting up a Safety Forum to provide support and guidance. A Road Risk Forum is already operating and providing guidance on road safety issues.The scope of agent activities and opportunity for Post Office to provide guidance is under review in Q4. To assess the robustness of the Safety Management System and to identify improvement opportunities to meet World Class level, an independent 3rd party audit is being undertaken by HSL / HSE with interviews held across the business, including front line, line managers, senior leaders and GE. A report has been shared with GE and PO Board.	△
4	Unable to deter agent theft or fraud and unable to recover agent debt effectively due to failure to prosecute.	Finance and Operations	Managing losses and Fraud	Stuart Nesbit / Mark Ellis	Sally Smith	2	5	10	3	5	15	Impact increased due to an increase in identified agent fraud and debt. Faster debt path processes approved and implemented in FSC. Increased levels of agent debt identified IRRELEVANT Effective recovery prevented by inability to prosecute. The Fraud Analysis team have completed implementation of EXL Analytics tool. Use of tool in pilot exercise identified branches which had not been flagged by existing detection methods. Increased number of audits performed in the quarter and further increase in capacity to carry out audits in Network Operations from April 2018. Period 9 YTD 17/18 / YTD16/17 IRRELEVANT	△

POL00401626

Appendix 5 (cont)

F&O Dashboard

Top Risks by Risk Score

F&O Top Risks by Score						Q3			Q4				
#	Risk Description	Business Area	Principal Risk	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Impact	Likelihood	Risk Score	Q4 Commentary	Movement
5	We make poor decisions because our MI is limited.	Finance and Operations	Reporting results and providing data accurately	Somita Yogi	Tim White	2	5	10	3	5	15	Impact increased to reflect the recognition that the lack of dependable and accessible MI can pose a limit to further improvements in business processes and ways of working. Project Arrow has been initiated and was presented to GE in November 2017 & got approval from CAG in Jan 2018. Currently engaging with GE members to get Data strategy completed and will present Data Strategy in March 2018. Started working on Data Governance, Data Quality, Data Operations and other streams of Arrow. We will also have a proof of concept delivered for Visualisation tool under Arrow.	△
6	Limited DR/BCP plans, largely untested increase the impact of systems and site loss.	Finance and Operations	BCP (excl ITDR)	Various	Tim Armit	3	3	9	4	3	12	Impact increased due to increasing risk posed by aged systems and untested plans. Plans are under way to test Chesterfield in March and Bolton in April 2018. Swindon relies on aged legacy IT systems and work will be carried out with IT to gain a better understanding of the IT DR requirements of the site before planning a live test.	△
7	Loss of Swindon operation causes widespread product loss.	Finance and Operations	BCP (excl ITDR)	Russell Hancock	Tim Armit	3	3	9	4	3	12	Impact increased due to increasing risk posed by aged systems and untested plans. Possible options for the Swindon site have been considered and we are now engaging with Royal Mail to establish what both businesses want from the relationship, which will inform our final decision on the site and future IT solutions.	△
8	Financial Reporting is inaccurate creating reputational damage.	Finance and Operations	Reporting results and providing data accurately	Michael Passmore	Johann Appel	5	2	10	5	2	10	The Financial Reporting Controls project scope is currently being extended to cover Masterdata and FSC processes. Further work will be performed to extend this to cover agent debt, POMS processes, and cash management and forecasting. Existing controls are self-assessed by owners on a monthly basis in TrAction and sample testing is performed within the FRC team. Results of external testing of controls by PwC have been reported to RCC/ARC and were generally good; improvements were recommended in relation to spreadsheet controls and these have now been implemented. PwC are performing further testing prior to FY17/18 year end. Risk remains the same in areas not yet covered by the project, we will have a better view of any new risks emerging as we complete these areas and identify gaps.	◁▷
9	Informal controls and compliance over Operations, weakens the internal control environment, leading to oversight failure.	Finance and Operations	Reporting results and providing data accurately	Various	Johann Appel	2	5	10	2	5	10	See risk 8.	◁▷

POL00401626

Appendix 5 (cont)

F&O Dashboard

Top Risks by Risk Score

F&O Top Risks by Score						Q3			Q4				
#	Risk Description	Business Area	Principal Risk	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Impact	Likelihood	Risk Score	Q4 Commentary	Movement
10	Our change is delivered late, risking costs and benefits or has unintended consequences.	Finance and Operations	Managing change	Angela Van-Den-Bogerd	Tim White	2	5	10	2	5	10	A series of proposals on structure, governance, culture and competency elements of Post Office change management were presented at the November 17 GE and approved. Work has commenced with PA to: • Transfer the executive sponsor of change to Rob Houghton and recruit a new Change Portfolio and a new Finance Lead. Both Rob and Tim have vast experience of managing large change portfolio which will benefit POL – Complete • Share with L300 the new vision and cultural shift for change, this will help to get management to understand the importance of change and support the new ways of working – Complete • Implementation of a Strategic Portfolio Office (SPO) and recommend the Target Operating Model which should be in place, this will ensure POL maximise the RoI on strategically aligned initiatives – End of Mar 18 • Create a new Investment Committee – develop TOR, attendees, roles and responsibilities, again this will support POL to maximise the RoI on strategically aligned initiatives – End of Feb 18 • Develop a project prioritisation methodology, which prioritises those initiatives that contribute the most to the PO's strategy and financial objectives – Mid Mar 18. • Build a phased transition plan to implement the new strategic portfolio office and processes which help increase delivery success and reduce the risk of late / poor delivery (including the introduction of an agile delivery and governance process) - End of Mar 18	◁▷
11	Unable to demonstrate compliance on agent vetting and training.	Finance and Operations	Compliance with laws and regulations	Angela Van-Den-Bogerd / Mark Ellis	Various in LRG	2	5	10	2	5	10	Smart ID (part of EUM) rolled out to 1000 branches (including top FS branches) but not fully implemented as old sign on still operational.	◁▷
12	Loss and churn due to a lack of training and support for newer agents.	Finance and Operations	Manage process and deliver services	Mark Ellis	Jackie Newton	2	5	10	2	5	10	Structural review of field teams completed and phase 1 of restructure commenced end January. Phase 2 to take effect in April 2018. 1 month and 3 month post-appointment visits now taking place. Initial training package reviewed and pilot being carried out in Q4. Joint wider review of training strategy to be carried out with Learning & Development team, due to report in Q2.	◁▷
13	Lack of effective communication resulting in lower levels of staff engagement.	Finance and Operations	Communicate, inspire and align	Russell Hancock	Mark Davies	2	5	10	2	5	10	Efforts being made to use Yammer to encourage more open communication throughout Finance and Operations. Unit programme in Supply Chain is starting to bring operational teams together to work through local issues and solutions.	◁▷
14	Cash is not managed efficiently, leading to increased risk of loss, funding costs and restrictions on change funding.	Finance and Operations	Sufficient cash / headroom	Russell Hancock	Mark Dixon	3	4	12	3	3	9	Likelihood decreased due to improved controls over cash management. Cash Management Project due to complete March 2018. IRRELEVANT IRRELEVANT IRRELEVANT . Increased reliability of CViT performance helping to move this in the right direction too. Have now started to map impact of potential increased transactions as a result of banking framework.	▽

POL00401626

Appendix 5 (cont)

F&O Dashboard

Top Risks by Risk Score

F&O Top Risks by Score						Q3			Q4			Q4 Commentary	Movement
#	Risk Description	Business Area	Principal Risk	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Impact	Likelihood	Risk Score		
15	Failure to transition agents pay from HR SAP, which is unsupported to CFS could result in none payment of remuneration and tax payments to HRMC leading to regulatory action and/ or loss of reputation.	Finance and Operations	Managing change	Angela Van-Den-Bogerd	Nick Beal	4	3	12	4	2	8	Likelihood decreased due to successful testing. The process for transferring agents pay from HR SAP to CFS has been thoroughly tested and we are confident this will be as successful as the employee payroll transferred in January. On track to transfer by end Feb.	▽
16	We do not have sufficient funds to create a sustainable business.	Finance and Operations	Ensuring sustainable profit	Michael Passmore	Johann Appel	4	2	8	4	2	8	A number of initiatives are in place to ensure efficient use of our working capital (particularly our cash inventory) to ensure we create as much headroom under our facilities as possible. In addition, we are formulating IRRELEVANT IRRELEVANT IRRELEVANT Both these initiatives will create additional headroom capacity under existing facilities.	◁▷
17	Limited cash data and forecasting leads to a facility breach.	Finance and Operations	Sufficient cash / headroom	Michael Passmore	Johann Appel	4	2	8	4	2	8	We continue to focus on improving cash flow forecasting. The Cash Management project is due to complete in March 2018. Due to resource constraints in the Wholesale Cash Team it has not yet been possible to implement the new model which has been developed for forecasting Note Circulation Scheme balances but the old model continues to work effectively albeit with room for improvement. KPMG have completed their review and are working to present their results. The same team is also working on a project with Supply Chain.	◁▷
18	We cannot report, forecast or optimise branch cash.	Finance and Operations	Reporting results and providing data accurately	Russell Hancock	Mark Dixon	2	4	8	2	4	8	New system Cash Web Community (CWC) fro IRRELEVANT being implemented as part of the Back Office Programme will enable more accurate forecasting and allow branches to order cash online. Pilot of CWC at Belfast cash centre due to go live March 18. The other cash centres are due to move to CWC by June 2018. Once the system is up and running smart technology will be progressively rolled out to frontline CVIT crew which will allow Supply Chain to introduce greater flexibility into cash deliveries and collections allow better optimisation of cash.	◁▷
19	Unable to achieve operational conformance due to limited monitoring of and communication with agents.	Finance and Operations	Compliance with laws and regulations	Mark Ellis	Various in LRG	2	3	6	2	4	8	Likelihood increased to reflect the fact that technology solutions (EUM) have not yet been fully implemented. Measures in place to improve conformance include the planned implementation of EUM (Smart ID now rolled out to 1000 branches), the Cash Management project, technical changes including the automation of cash declarations and changes in incentivisation for the Mail Segregation targets. Communication is being improved through an improved capacity to make calls in the Branch Standards Team, improved training and support from the Network Operations field teams and the roll out of the Agent Portal.	△

POL00401626

Appendix 5 (cont)

F&O Dashboard

Top Risks by Risk Score

F&O Top Risks by Score						Q3			Q4				
#	Risk Description	Business Area	Principal Risk	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Impact	Likelihood	Risk Score	Q4 Commentary	Movement
20	We are not compliant on tax attracting fines and censure.	Finance and Operations	Record and pay taxes	Michael Passmore	Jane MacLeod	3	2	6	3	2	6	Tax manager in post and processes being embedded. Additional support provided by external specialists.	◁▷
21	We procure badly, destroying value.	Finance and Operations	Procure	Barbara Brannon	Jane MacLeod	3	2	6	3	2	6	Work is under way to procure and implement a Contract Management System.	◁▷
22	Telephony system is unstable and we cannot maintain service to customers and agents.	Finance and Operations	Business Interruption (ITDR)	Mark Ellis	Roger Gale				3	2	6	Transfer from BT to Verizon implemented 3 Nov 2017 but system lacks functionality. High levels of calls due to POCA letter in w/c 13 Nov required interim solution in which POCA calls are handled by BT - this is due to be transferred to TalkTalk mid-Feb. Phase 2 will be to move rest of POEX call plan from Puzzel to Talk Talk. Current uncertainty about capacity of system when BT contract ends (March 2018) - Verizon are supposed to be providing a solution. Overall solution will be fragmented and involve Verizon, TalkTalk and Puzzel.	NEW
23	Financial forecasting is limited.	Finance and Operations	Sufficient cash / headroom	Michael Passmore	Johann Appel	1	5	5	3	2	6	Permanent head of FP&A took up post in February 2018.. Current reporting and forecasting processes will be reviewed to identify opportunities for improvement.	△
24	We appoint unsuitable applicants leading to performance issues and re-work due to increased terminations through losses.	Finance and Operations	Manage process and deliver services	Mark Ellis	Roger Gale	2	5	10	2	3	6	Organisational changes to bring all the field teams into Network Operations (from April 2018) and realignment of objectives have reduced the likelihood of accepting unsuitable applicants. Work is underway to implement the recommendations of the review of the applications process but progress is hampered by a lack of capacity in the Agents Contracts Team due to increased workload.	▽
25	We procure illegally, attracting fines and censure.	Finance and Operations	Procure	Barbara Brannon	Jane MacLeod	2	3	6	2	3	6	No change for Q4.	◁▷
26	We do not keep cash physically secure resulting in financial loss to PO.	Finance and Operations	Physically secure	Russell Hancock	John Flood	5	1	5	5	1	5	No change for Q4.	◁▷

POL00401626

Appendix 5 (cont)

F&O Dashboard

Top Risks by Risk Score

F&O Top Risks by Score						Q3			Q4			Q4 Commentary	Movement
#	Risk Description	Business Area	Principal Risk	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Impact	Likelihood	Risk Score		
27	Risk of kidnap in Supply Chain and branch network.	Finance and Operations	Keep our people, customers and third parties safe	Mark Ellis	Martin Hopcroft	5	1	5	5	1	5	Tiger Kidnap policy and procedure in place. Procedure being revised to call police directly, instead of via Grapevine, in the event of an incident. Due to go live April 2018. Training delivered annually to all staff in Supply Chain.	◁▷
28	Risk of political/social violence in Northern Ireland.	Finance and Operations	Keep our people, customers and third parties safe	Mark Ellis	Mark Davies	5	1	5	5	1	5	No change for Q4.	◁▷
29	Unable to perform client settlement.	Finance and Operations	Make payments	Stuart Nesbit	Johann Appel	4	2	8	4	1	4	Likelihood decreased due to successful live testing of contingency plans. Contingency plans in place and live testing carried out resulting in successful and accurate settlement.	▽
30	Fail to pay suppliers within timeframes required by statutory payment guidelines.	Finance and Operations	Compliance with laws and regulations	Stuart Nesbit	Barbara Brannon	1	4	4	4	1	4	Processes in place and working to at over 95% of invoices paid within 30 days, with actions to move to full conformance.	◁▷
31	Failure to migrate staff payroll from HR SAP, which is unsupported, to SuccessFactors could result in delayed and / or inaccurate salary payments to staff and some agents. This could lead to regulatory action and/ or loss of reputation, also potential employee relations issues at a time of heightened tension.	Finance and Operations	Managing change	Angela Van Den Bogerd	Nick Beal	4	3	12	3	1	3	Impact and likelihood decreased due to successful migration at end of January. Staff payroll migrated to SuccessFactors completed January 2018. All employees successfully paid at the end of January, very few issues reported and all problems relating to employee pay fixed almost immediately.	▽
32	Insurance coverage is insufficient to cover risks or liabilities.	Finance and Operations	Ensuring sustainable profit	Michael Passmore	Jane MacLeod	3	1	3	3	1	3	The broker (Lockton) has been engaged for the past 3 years. The broker understands the business and engagement is good. Appropriateness of coverage is considered at renewal.	◁▷

POL00401626

Appendix 6

LRG Dashboard

Top Risks by Risk Score

LRG Top Risks by Score					Q3			Q4			Q4 Commentary	Movement
#	Risk Description	Principal Risk Category	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Impact	Likelihood	Risk Score		
High Risk												
1	Failure by Post Office to ensure operational activities, IT infrastructure/security and related services are PCIDSS compliant may cause challenges during external audit, require significant remediation activities and attract unbudgeted costs. This may result in a failure to obtain the required certification, breach our agreed banking framework and may lead to a legal/regulatory breach, financial loss and reputational damage.	Information Protection	Jules Harris	Ehstham Ali	5	4	20	5	4	20	Our ability to achieve and maintain **PCI accreditation** is a significant challenge and if we are unable to achieve compliance could lead to significant fines or the removal of our ability to process card payments. The standards are predominately set to ensure security of card data. Non-compliance may result in Post Office being considered an easy target to fraudulently obtain card data. The cost of any such breach could be far higher (both financially and reputational). Next steps: • Audit against V3.2 of the PCIDSS Standard was not successful resulting in failure to obtain a positive Report on Compliance (RoC) • Remediation is underway by Fujitsu and Computacenter • Physical Audit is continuing across our Branch Network • Target date for a successful RoC is 31 March. However, this is dependent on Computacenter's remediation activities being delivered on time. PO confidence in the ability of ComputaCenter to deliver by the new deadline is low.	◁▷
2	There has been a material delay to the programme that has been caused, principally, because of: - A lack of documentation - Scale and complexity - Availability of resources Further delay could impact upon POL's ability to achieve effective compliance by the time GDPR comes into force on 25 May 2018.	Information Protection	Jules Harris	Claire D'Netto	3	3	9	4	4	16	The Programme delivering GDPR compliance for Post Office is challenged, and the ability to achieve effective compliance by the implementation of the act is also at risk. Additional resource is being allocated to ensure that key deliverables remain on-track. **Getting the information we need** To baseline the scope of assets, we need to identify PO products, suppliers, systems and contracts and prioritise based on risk. We need confirmation of Product and Contract Managers to validate our view. The documentation / corporate knowledge we would expect is not readily available so we need to work with suppliers and their Contract Managers to create it. We will be completing retrospective PIAs with Product Managers and the business to create records of processing activities. **Scale and Complexity** The sheer scale of Post Office operations in terms of numbers of products (c117), IT suppliers (100+) (and associated systems) and contracts (600+) means that we have prioritised analysis into tranches and are running this on an agile basis. We are now getting traction using this approach. The complexity is due to the dependencies with other projects which will impact on personal data. Specifically we need to align the GDPR Programme with key IT transformational projects to ensure the appropriate controls are built into third party contracts that are being renegotiated or replaced. **Availability of resources** There are capacity constraints in the BAU DP Team, so we are recruiting interim Data Protection SMEs which are scarce due to demand in other GDPR programmes. It has taken us 3 months to fill a key senior role (ETA 2/10) and we are now looking for a more junior DP resource to provide additional capacity.	△

POL00401626

Appendix 6 (cont)

LRG Dashboard

Top Risks by Risk Score

LRG Top Risks by Score					Q3			Q4				
#	Risk Description	Principal Risk Category	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Impact	Likelihood	Risk Score	Q4 Commentary	Movement
3	Failure to identify and control the insider threat and include security controls in contracts with suppliers.	IT Security	Jules Harris	Mick Mitchell	4	3	12	4	3	12	The Security Operations Centre (SOC) will be established in the over the next 6 to 9 months, providing oversight of all security controls from each provider, centralise and aggregate events and incidents to enable POL to react against security issues efficiently and effectively, thereby reducing our risk exposure.	◁▷
Medium Risk												
4	Adverse outcome from current Group litigation.	Litigation	Jane MacLeod	Mark Underwood / Rodric Williams	5	2	10	5	2	10	POL has in place a Steering Group with attendees from across the business with appropriate level of seniority to ensure that the resource, decisions, materials and documentation necessary for POL to be able to robustly defend its position are available to it.	◁▷
5	Failure to comply with contractual requirements.	Contract Management	Ben Foat	Ben Foat	3	3	9	3	3	9	The Bravo central contract repository system is owned by the Procurement Team but maintained by both Procurement and Legal teams. Contracts are required to formalise our commercial relationships and transactions. The terms and obligations in those contracts need to be managed / adhered to. As of February 2018, a business case has been drafted and is being driven by Ben Cook's team (CIO Back Office Technology & Transformation) for a longer term contract management system solution accommodating legal needs. The Legal Team has been involved throughout the project and been feeding in requirements which will form part of the business case. As of February 2018, the Contract Obligations Spreadsheet has been updated and will be finalised shortly. The Contracts Obligations Spreadsheet will reflect the current position of material contracts (Legal).	◁▷
6	Poor contract management.	Contract Management	Ben Foat	Ben Foat	3	3	9	3	3	9	LRG SLT member is to attend the Finance and Operations Lead Team meeting. Members of the Legal team currently attending various Lead Team meetings (including the Financial Services Lead Team meeting the Banking Lead Team meeting and others) to discuss Framework / minimum control standards for Contract Management. As of February 2018, a business case has been drafted and is being driven by Ben Cook's team (CIO Back Office Technology & Transformation) for a longer term contract management system solution accommodating legal needs. The Legal Team has been involved throughout the project and been feeding in requirements which will form part of the business case.	◁▷

POL00401626

Appendix 6 (cont)

LRG Dashboard

Top Risks by Risk Score

LRG Top Risks by Score					Q3			Q4				
#	Risk Description	Principal Risk Category	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Impact	Likelihood	Risk Score	Q4 Commentary	Movement
7	Regulatory Compliance and increased visibility of POL and POMS to regulators e.g. ICO re GDPR, HMRC re AML/CTF, FCA re POMS expansion, FCA via Banking Framework, OFCOM re Mails and Telco.	Compliance with laws and regulations	Jane Macleod	Ben Foat	3	3	9	3	3	9	A Regulatory and Legislative Framework has been developed and circulated to the GE for their business areas as well as tabled at RCC last September. Earlier this year, GE accountability for the key piece of legislation and regulation applicable to POL has assigned to GE members. Since then, the Regulatory and Legislative Framework has been shared with the business areas through the Law and Trends Forum. The Regulatory and Legislative Framework will be maintained and periodically reviewed and updated by the Legal team. Follow up meetings have been held with each GE member to agree accountabilities and responsibilities. A gap analysis will be performed. A second paper has been discussed at RCC on the Criminal Finances Act. In addition, POL is putting together a case with relevant stakeholders in Government regarding the increasing compliance requirements and their impact on the POL business. As of February 2018, the Legal team is working on the Directors Induction Pack, a document to be shared with new directors/executives which will provide an overview of any regulatory impact on POL/POMS.	◁▷
8	Risk management isn't fully developed and embedded, e.g., no mature risk culture, monitoring, oversight, appetite, policy and compliance framework.	Governance	Richard Williams, Deana Herley	Richard Williams, Deana Herley	3	3	9	3	3	9	The Placemat approach / methodology is being rolled out across the business to formalise, embed and create a single view of the risk and control environment. The Placemat outputs have been aligned to the Enterprise Risk Management Framework. Further enhancements, such as appetite will be considered in 2018.	◁▷
9	We do not have sufficient or appropriate BCP arrangements in place that are documented, understood and tested.	BCP	Tim Armit	Tim Armit	3	3	9	2	3	6	BC risks, impacts and strategies will be developed across all areas in 2017/18. Development of business continuity plans has started. Business awareness and training sessions have commenced and will continue through the next quarter. Process to invoke Business Protection Team in case of incidents has been put in place and is working effectively. As a result the impact of incidents has reduced, however, the likelihood remains unchanged due to lack of documented plans and testing (that will follow once plans have been documented).	▽
Low Risk												
10	Policies do not exist or have not been properly reviewed.	Governance	Jane MacLeod	Jane Macleod	2	2	4	2	2	4		◁▷

POL00401626

Financial Crime Pilot

Author: Ashish Singh/Sally Smith Sponsor: Jane MacLeod Meeting date: 13 March 2018

Executive Summary

Context

The purpose of this paper is to provide the Committee with an overview of the 'Horizontal' Placemat governance and reporting context and proposed approach.

Questions this paper addresses

1. What is the purpose of 'Horizontal' Placemat governance and reporting?
2. How are we planning to do it?
3. What are the next steps in the rollout?

Conclusion

1. The Risk Placemat roll-out will provide each business area (verticals) with a 'bottom-up' view of their risks, and an assessment of how effectively those risks are being managed. This in turn will facilitate the reporting of their 'top risks'. The rollout of the Risk Placemat is on track to be completed by June 2018.
2. To further enhance our understanding and management of risk, we are developing an approach to test the integrity, and formalise the governance and reporting, of the key principal risks (horizontals), ready for embedding prior to full Placemat implementation.
3. Pilots are underway, covering Information Protection, IT Security and Financial Crime principal risks. We are also proposing to run pilots for BCP and Health & Safety.
4. The pilots focus on governance, assurance and reporting over principal risks, including risk profile, risk appetite, key risk indicators, risk exceptions, controls effectiveness, policy compliance, incident management and action tracking.
5. The outputs from the pilots will support our understanding of how we should 'end to end' assure the completeness, quality and consistency of the business areas view (verticals), to support the formulation of a consolidated Post Office view. The overall risk picture will help to focus dialogue on the highest risk items.
6. We expect to report on the 4 pilots at the June Committee.

Input Sought

The Committee is asked to note this paper, provide comment as necessary, and approve the Terms of Reference for the Financial Crime Committee.

POL00401626

POST OFFICE

The Report

What is the purpose of 'Horizontal' Placemat governance and reporting?

1. The Risk Placemat roll-out will provide a comprehensive baseline view of the top risks facing each business area, and an assessment by respective management of how effectively those risks are being managed (verticals). The rollout of the Risk Placemat is on track to be completed by June 2018.

2. However the vertical view, by itself, will provide an incomplete view of the overall risk profile for the Post Office on account of the following:
   a. No visible linkage of Placemat to minimum controls in policies;
   b. No visible linkage or consideration of incidents and exceptions in the Placemat roll-out;
   c. No functional assurance on Principal Risks which appear across multiple verticals; and
   d. No reflection of performance against risk appetite

3. To further enhance our understanding and management of risk, we are developing an approach to test the integrity and formalise the governance and reporting of the key principal risks (horizontals), ready for embedding prior to full Placemat implementation.

4. It will enable us to review the reporting in relation to the current 'perimeter' risks to ensure they align to the Placemat, reflect the policy requirements and enable consistent use of data sets.

5. The purpose of horizontal governance and reporting is to provide the GE owners for the Principal risks, and through them, to this Committee:
   a. Assurance over the consistency of Placemat roll-out across Businesses for the same principal risk;
   b. Assessment of root causes and common themes underpinning vertical risk assessment;
   c. Identification and consideration of interdependencies between Business areas in managing their risks;
   d. Review of material incidents and risk exceptions across Post Office for the relevant principal risks;
   e. Assurance over effectiveness of controls and compliance with applicable policies
   f. Progress on agreed actions in relation to improved mitigation of principal risk across the organisations; and
   g. An overall assessment of the principal risk position at the Post Office level and in comparison to its stated risk appetite for that principal risk.

POL00401626

POST OFFICE

How are we planning to do it?

6. We are running a series of pilots to develop and validate our approach to Horizontal governance and reporting. In Wave 1, currently underway, our pilots cover the following principal risks:
   a. Financial Crime – *via the Financial Crime pilot*
   b. Information Protection – *via the Information Security pilot*
   c. IT Security during - *via the Information Security pilot*

7. These principal risks have been selected as they have a cross-business footprint, have a set of Post Office policies defined for them, and are key areas of focus for both the RCC and the ARC. Governance fora are also being developed for each.

8. The scope of these pilots includes developing proposals for:
   a. Establishing Terms of Reference for relevant governance bodies;
   b. Clarifying ownership and accountability between the Business (risk owners) and Functions (assurance providers);
   c. Developing MI for tracking risk performance, including assessment against risk appetite;
   d. Designing dashboards for risk and compliance reporting; and
   e. Defining functional assurance scope and approach

9. Stakeholders from across the relevant business and functional areas are actively involved in these pilots.

10. Appendix 1 includes the Terms of Reference for the Financial Crime Committee, which has been reviewed by the Financial Crime Committee. It is proposed that the Financial Crime Committee will be a sub-committee of the Risk and Compliance Committee, hence we seek approval for these Terms of Reference.

11. Appendix 2 includes the Risk and Compliance reporting dashboard for Financial Crime. *(A3 copies will be provided during the Committee meeting)*

POL00401626

POST OFFICE

What are the next steps in the rollout?

12. Wave 1 pilots will be completed and results compiled and reviewed by the Financial Crime Committee and Information Security Committee, respectively, before the end of June. We will start reporting on these Principal risks on an ongoing basis to the RCC and the ARC from July onwards.

13. We will also be commencing Wave 2 pilots. Subject to the views of the RCC, we propose to cover the following principal risks:
    a. Business Continuity Planning
    b. Health and Safety

POL00401626

POST OFFICE

Appendix 1

Financial Crime Committee Terms of Reference

1. Purpose:

The overall objective of The Financial Crime Committee (FCC) is to provide oversight of Post Office's management of Financial Crime related risks, internal controls and compliance on behalf of the Risk and Compliance Committee (R&CC), including:

i. Assessing Financial Crime risk causes and impacts so that they are properly understood, and proportionately, consistently and effectively managed across Post Office, in line with the Board approved risk appetite;
ii. Monitor compliance by Post Office, its products and services, and its partners, suppliers and employees, with relevant regulatory requirements including Anti Money Laundering (AML), Counter Terrorist Financing (CTF) and Anti Bribery and Corruption (ABC);
iii. Enabling the Senior Officer (the Group Director of Legal, Risk and Governance) to oversee business regulatory obligations in compliance with the 2017 Money Laundering Regulations
iv. Reviewing Financial crime policies that impact AML, CTF and ABC, including minimum control standards;
v. Recommending remediation activities and monitoring their completion in respect of:
    a. Functional assurance and Internal Audit
    b. Regulatory changes
    c. Incidents
    d. The HMRC audit action plan
    e. Product and Service risk assessments; and
vi. Assessing external threats and regulatory developments.

2. Scope:

The scope of the FCC includes Anti-Money Laundering, Counter Terrorist Financing and Anti-Bribery and Corruption.

3. Specific responsibilities of the FCC will include:

- Reviewing the overall Post Office risk profile against risk appetite and the effectiveness of the control framework
- Reviewing draft and updated policies, prior to submission to the R&CC and Audit & Risk Committee (ARC) for approval
- Reviewing risk profile at individual Business Unit or Function level ensuring there is sufficient and effective mitigation activity
- Reviewing functional and independent assurance results to corroborate management's self-assessment, ensure consistency across Business Units and Functions, and discuss common risk themes and root causes
- Reviewing any proposed policy exception requests
- Monitoring the progress of remediation plan activity
- Reviewing residual risk from product and service risk assessments
- Reviewing non-conformance and 'Fit & Proper' status issues across the Network
- Reviewing any material Financial Crime issues or incidents affecting Post Office, including supplier related issues

POL00401626

- Reviewing operational resource to ensure adherence to regulatory requirements relating to Suspicious Activity Reporting submission and transaction monitoring
- Monitoring the status of change programmes that impact the risk
- Maintaining oversight over current and emerging threats and developments that could impact Post Office
- Discuss and agree R&CC and ARC report subjects/content

4. Authority

Decision making will be made within the FCC members usual business delegated authority.

5. Membership

The membership shall comprise:

- Group Director of Legal, Risk and Governance (chair)
- Director of Risk & Compliance/MLRO
- Head of Financial Crime
- Head of Financial Service and Telecoms Risk and Regulation
- POMS Director of Risk & Compliance
- Network Operations Director

Attendees must nominate a deputy of sufficient seniority who can represent them should they be unavailable to attend the meetings.

The Chair may require other colleagues to attend all or part of meetings as appropriate, including (but not limited to):

- Relevant Product Managers
- Head of Fraud Analysis and Branch Standards
- Sales and Trade Marketing Director
- Network Development Director
- Government and Payment Services Director
- HR Director

The quorum shall be a minimum four members one of which must be the Chair (or their designated representative).

6. Meetings

- The FCC shall meet monthly.
- Minutes of each meeting will be issued to all members.

7. Standing Agenda Items

- Approval of previous minutes and review of actions
- Review of Financial Crime risk dashboard and Business Unit or Functional summaries
- Financial Crime MI:
    - Key risk indicators and metrics

POL00401626

POST OFFICE

  - Incidents
  - Non-conformance/Fit & Proper issues
  - Operational activity
- Review of internal and external audits and actions plans impacting Financial Crime, including HMRC
- Review of product and service risk assessments
- Review of material issues/incidents
- Review of regulatory change and emerging threats

8. Reporting

Bi-monthly noting or escalation papers to R&CC and, as required, the ARC.

POL00401626

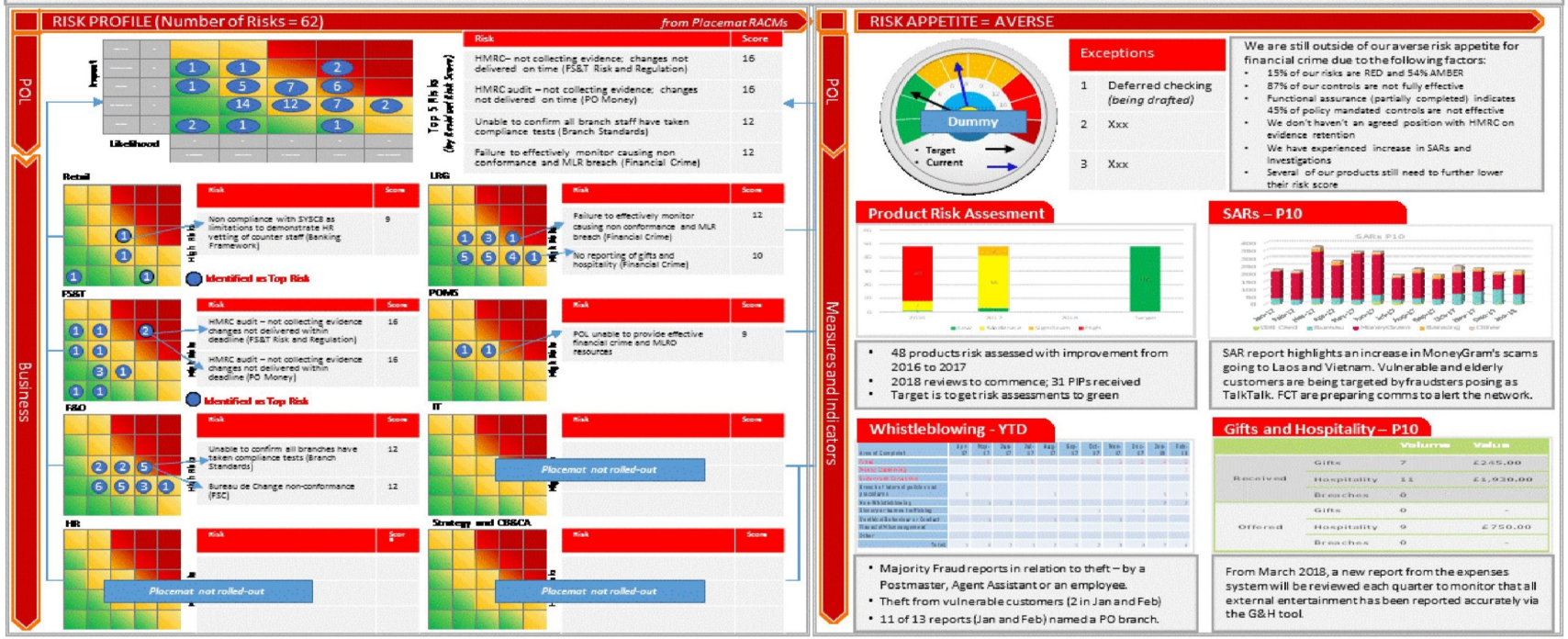
POST OFFICE

Financial Crime Risk Dashboard

Appendix 2

FINANCIAL CRIME – RISK REPORT [March 2018 (Q4)] — **Financial Crime Committee**

- The HMRC audit identified we are not collecting or can not evidence the required information required by the AML requirements in respect of our bureau transactions in the network. However there is a risk we may not delivery the required changes within the deadlines outlined in the plan. Risk has increased as HMRC are changing their position in relation to KYC recording requirement. Regular engagement continues with HMRC.
- Progress has been made on risk assessing and remediating product risks. Awaiting updated Product Information Packs to commence 2018 assessment and further reduce product risk.
- c33% of risks (20 out of 62) are currently owned by LRG. Since LRG (and the FC team within it) is predominantly an advisory and assurance function (2nd line), we would expect to see more Financial Crime related risks being identified, owned and managed within the business areas (esp Retail).



Caveat: The Dashboard is based on currently reported data. Other actions are being planned to mature the quality, completeness and integrity of data

Page 1 of 2

POL00401626

POST OFFICE

Financial Crime Compliance Dashboard

Appendix 2

FINANCIAL CRIME – COMPLIANCE REPORT [March 2018 (Q4)] | **Financial Crime Committee**

- c13% (8 out of 62) controls have been self assessed as fully effective (per Placemat). However remediation actions have not been identified for all risks assessed as partially effective or ineffective. These actions are currently not being formally tracked and/or reported.
- Ineffective controls are in known areas of Bureau, PEPs and Sanctions, and Fit and Proper. Remediation actions are being implemented
- Functional assurance has commenced on effective implementation and operation of minimum controls in relevant policies. Based on partial completion, c55% of controls assured are effective.
- 6 significant incidents reported in the current year, across Retail and LRG. Need to continue to strengthen and monitor vetting process

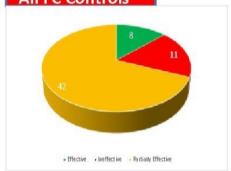
CONTROLS AND POLICY COMPLIANCE

POL

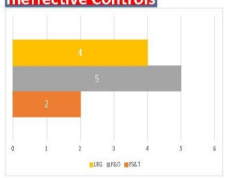
POLICY

Self Assessment *(from Placemat RACMs)*

All FC Controls



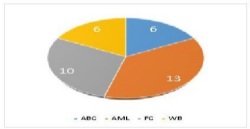
Ineffective Controls



Functional Assurance*

Minimum Controls

AML and CTF	6
ABC	13
Financial Crime	10
Whistleblowing	6



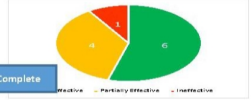
Impact on Risks



Current Status

- For the controls assured to date, c55% are effective
- The ineffective control is around sanctions screening, where IT solution is planned for implementation

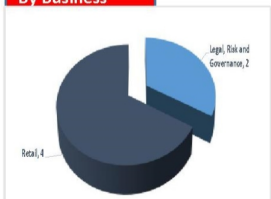
Partially Complete



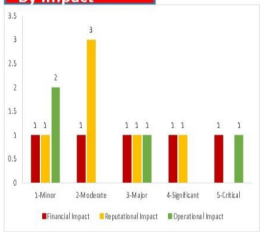
*In subsequent periods we expect to report functional assurance results by Policy and Business Area

SIGNIFICANT INCIDENTS - YTD

By Business



By Impact



By Root Cause



By Theme

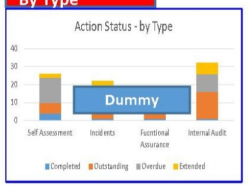


Top Incidents *(and financial impact)*

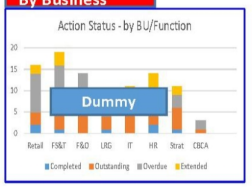
1. Potential Terrorist Financing - Crwys Road Post Office *(Significant)*
2. Potential Money Laundering – Woodland Parade *(Major)*
3. Suspicious SSK Activity - Prepay Tech Ltd *(Moderate)*
4. One4All - Gift Card Top Ups *(Minor)*
5. HMRC Branch Premises Registration - Bureau de Change *(Critical)*
6. HMRC – High value Santander Cash Deposits (£6m in six months)

ACTION STATUS

By Type



By Business



- Xxx
- Xxx
- Xxx
- Xxx
- xxx

(Comments)

OTHER CONSIDERATIONS AND MATTERS

Investigations – P10

Due to the branch contact embargo implemented throughout December, FCT were unable to conduct any Bureau investigations until January, hence the high volume in P10.



NCA Disclosures – P10

Suspicious personal financial activity relating to a Post Master. Post Office unable to comment on personal financial activity, however, the Postmaster submitted their resignation in September and is currently serving their 6 month notice period. No concerns with individual or Post Office branch.

JMLIT s7 requests – P10

- 8 s.7 requests received in P10 listing 62 subjects for screening
- In P10, 3 subject matches were identified and data provided to the NCA
- We have completed searches on 216 known terrorists as per P9, and data on 27 matched subjects has been shared with the NCA

***Caveat**: The Dashboard is based on currently reported data. Other actions are being planned to mature the quality, completeness and integrity of data*

POL00401626

Internal Audit Report

Author: Johann Appel | Sponsor: Jane MacLeod | Meeting date: 13 March 2018

Executive Summary

Context

The purpose of this paper is to update the Committee on the PO Internal Audit activity and key outcomes. This includes details of the work completed since the last Risk and Compliance Committee (RCC) and Audit, Risk and Compliance Committee (ARC) meetings in January and progress on the 2017-18 Internal Audit Plan.

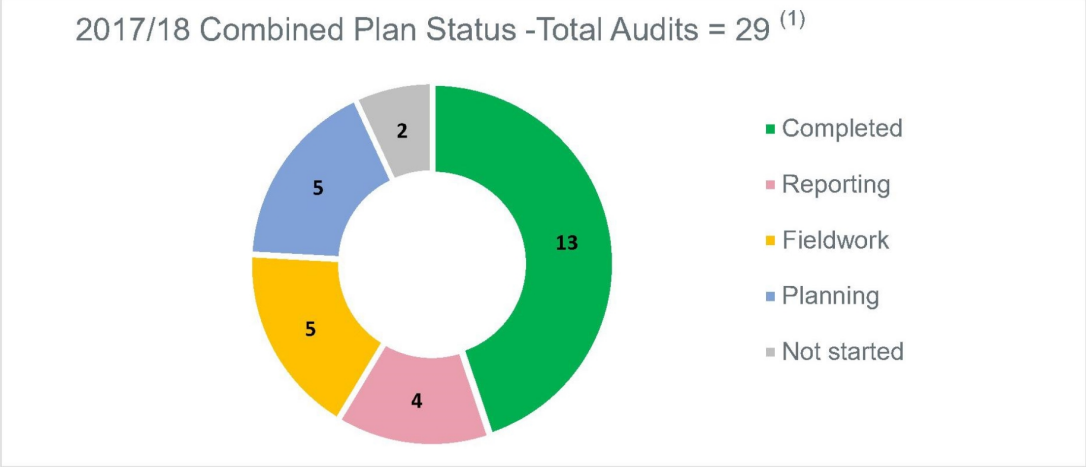
Questions this paper addresses

- Is the Internal Audit Plan on track? What progress has been made since the November RCC meeting?
- What progress is being made with completion of audit actions?
- Have any significant issues arisen that the committee should be aware of?

Conclusion

1. Progress against plan:

Delivery of the 2017-18 audit plan is making good progress and year to date we have now finalised 13 reviews, with a further four reviews currently in reporting. At the time of writing this report five audits were in fieldwork and a further five were being scoped for delivery between March and May. Current progress against plan is as follows:



(1)ARC approved baseline plan for 2017/18 (16 internal control reviews & 13 change assurance reviews)

A full summary of the 2017/18 audit plan status is included in **Appendix 1**.

POL00401626

2. Open and Overdue Audit Actions (as at 28 February 2017):

Audit Action Status:	
Open (not yet due)	38
Overdue (<60 days)	3
Overdue (>60 days)	0
Total	41

More detailed information is provided in paragraphs 10 – 11 of the report.

3. Significant Issues:

There are no significant issues we believe the committee should be made aware of.

Input Sought

The Committee is asked to note and provide comment as necessary.

POL00401626

The Report

Changes to plan since January RCC and ARC meetings

4. No changes to the plan were made during this reporting period.

Internal audit reviews completed

5. Since the January ARC meeting we have finalised the following review:
   - Compliance with Banking Services Framework agreement

   Our findings and observations are summarised below:

Audit	Key Messages
Banking Services Framework (Ref. 2017/18-20) Appendix 2a Needs Significant Improvement ***Sponsor:*** *Debbie Smith* Audit actions: P1: 2 P2: 11 P3: 16 Advisory: 5 Total: **35**	The objective of this audit was to assess adherence to the Framework Agreement by Post Office and its Agencies. With regards to the controls which are specific to the Framework, we observed that Management have implemented effective oversight in relation to the continuing operations of the key Framework processes. However, accountabilities for some services contained in the Framework Agreement have not been clearly assigned to different areas of the business. This contributed to the fact that some of the documentation (i.e. a fraud prevention policy and the Link Information Security Standard) have yet to be developed. With regards to controls which have wider business impact and are critical in supporting the Framework, it was noted that processes need to be strengthened in order to: (i) effectively monitor compliance with the financial crime policy; (ii) implement an effective governance (including planning and testing) of business continuity management (BCM); (iii) improve the IT Disaster Recovery (ITDR) governance arrangements and the oversight of the testing programme; (iv) update information security policies and procedures. Also, for Payment Card Industry Data Security Standards (PCI DSS), back office processes are not included in the PCI scope and neither are users with access to Primary Account Numbers (PAN). There is no ongoing monitoring outside of the annual (external) audit. This report has been rated 'Needs significant improvement' as it highlights weaknesses in internal controls, in particular within the supporting activities across Post Office, which may result in non-compliance with the Framework.

POL00401626

Reviews in Reporting

7. Reports for the following reviews are currently being drafted or cleared through management and is expected to be finalised in time for the March ARC meeting:

	Review	Status / Remarks
1	Customer Complaints	Final draft with exec sponsor for comment
2	Project Solar - HNGT Lite	Draft report being reviewed by project team
3	Back Office Transition	Draft report being reviewed by project team
4	SAP SuccessFactors Payroll - Lessons Learned	Report being drafted

Reviews in Progress

8. The following reviews were in fieldwork at the time of writing this report:

	Review	Status / Remarks
1	Branch Technology - EUC Transition	Fieldwork 5-16 March
2	Network Transformation	Fieldwork 5-16 March
3	Financial Reporting Controls	Nearing completion
4	Pension Schemes	Fieldwork 5-20 March
5	Data Protection (GDPR)	Nearing completion

Reviews in Planning

9. We are currently scoping the following reviews scheduled for delivery in Q4:

	Review	BAU / Change	Timing
1	Telecoms Control Framework	BAU	12-30 March
2	Business Continuity	BAU	12-30 March
3	IT Governance and IT Risk management (Operations)	BAU	March
4	Back Office Transformation - Cash Processing	Change	April
5	Back Office Transformation - POLSAP to CFS	Change	March
6	EUM	Change	April

Updates on Internal Audit Open and Overdue Actions

10. Audit actions are generally being completed on time and year to date 119 audit actions have been completed (103 BAU and 16 Change Assurance actions). At 28 February 41 actions remained open, three of which were overdue.

Audit Action Status:	BAU	Change	Total
Open (not yet due)	36	2	**38**
Overdue (<60 days)	3	0	**3**
Overdue (>60 days)	0	0	**0**
Total	39	2	**41**

POL00401626

11. Following is a summary of the overdue actions, reasons for delay and latest status update:

Description of action and Priority rating	Due date & GE Sponsor	Reason for delay and status update
Data Protection (2016-17)		
Create a Document Retention and Disposal policy.	28/02/18 Jane MacLeod	The new Data Retention and Disposal policy is being created and will be submitted for approval to RCC in March.
NBSC - Handling of Branch Queries and Complaints		
Project to improve the Dynamic System, including system integration, re-design of the knowledge base/ call guides, improved data capture and reporting, and system configurability.	28/02/18 Al Cameron	Project delayed due to technical issues identified during testing which has had a major impact on go live dates. Completion date is now 28/2/18. Project further delayed due to technical issues with drop 1 - dates further extended until end April 2018.
Banking Services Framework		
The Banking Framework services manager will document and submit their product information pack. This will then be used to inform an assessment of the inherent risks, control strengths and residual risks by the Financial Crime Team.	28/02/18 Debbie Smith	Product Information Pack is partially complete and expected to be completed in full by 23 March.

END OF REPORT

POL00401626

Appendix 1

2017/18 Internal Audit Plan - Status as at 5 March 2018					
No.	**Title/Subject**	**Sponsor**	**Original / Addition**	**Timing**	**Status / Rating**
Internal Control Reviews					
1	VAT Process	A. Cameron	**Addition**	May	**Needs Improvement**
2	Lottery Prize Pay-out (Design effectiveness)	K. Gilliland	**Addition**	August	**Satisfactory**
3	Financial Spreadsheet Controls	A. Cameron	**Addition**	August	**Needs Improvement**
4	IT Control Framework (Advisory)	R. Hougton	Original	March - Aug	**Advisory Report**
5	Mails Process	K. Gilliland	Original	July	**Satisfactory**
6	Information Security (2016) Follow-up review	R. Hougton	Original	September	**Needs Significant Improvement**
7	IT Security Transformation (Advisory)	R. Hougton	Original	March - Dec	**Advisory Report**
8	Compliance with Banking Framework	N. Kennett	Original	August	**Needs Significant Improvement**
9	Customer Complaints	A. Cameron	Original	November	**Reporting**
10	MoneyGram: AML Compliance	J. MacLeod	Original	September	**Satisfactory**
11	Telecoms Control Framework	N. Kennett	Original	March	Being Scoped
12	Business Continuity	J. MacLeod	Original	March	Being Scoped
13	Data Protection (follow up) (GDPR)	J. MacLeod	Original	January	**Fieldwork**
14	Pension Scheme(s)	A. Cameron	Original	March	**Fieldwork**
15	Financial Control Framework	A. Cameron	Original	February	**Fieldwork**
16	IT Governance and IT Risk management	R. Hougton	Original	March	Being Scoped
	FRES	N. Kennett	**Postponed**	2018/19	
	Client Settlements Process	A. Cameron	**Postponed**	2018/19	
	Cyber Security (Ph 2)	R. Hougton	**Postponed**	2018/19	
	Branch Cash Forecasting & Management	A. Cameron	**Postponed**	2018/19	
Change Assurance					
1	SAP SuccessFactors - Payroll	M. Kirke	Original	June	**Needs Improvement**
2	Integrated Change Plan (Advisory)	A. vd Bogerd	Original	July	**Advisory Report**
3	IT Networks	R. Houghton	Original	October	**Needs Improvement**
4	SAP SF Payroll Go-Live Readiness Review	M. Kirke	**Addition**	December	**Acceptable (PwC)**
5	SAP SF Payroll Lessons Learned	M. Kirke	**Addition**	January	**Reporting**
6	Back Office Transformation - POLSAP to CFS	A. Cameron	Original	March	Being Scoped
7	Back Office Transformation - Cash Processing	A. Cameron	**Addition**	March	Not started
8	Back Office Transition	A. Cameron	**Addition**	January	**Reporting**
9	Project Solar - HNGT Lite (Prev. Chameleon)	K. Gilliland	Original	January	**Reporting**
10	Network Transformation	K. Gilliland	Original	February	**Fieldwork**
11	Branch Technology - EUC Transition	K. Gilliland	Original	January	**Fieldwork**
12	EUM	K. Gilliland	Original	March	Being Scoped
13	Peer to Peer Encryption Implementation	J. MacLeod	**Cancelled**		Cancelled
	Placeholder (FS Customer Hub?)	N. Kennett	Original	tbc	Not started
	Placeholder (Project Panther?)	K. Gilliland	Original	tbc	Not started
	Agile Methodology and Governance	J. MacLeod	Original	tbc	Not started
	Gating Process - Effectiveness	A. vd Bogerd	**Postponed**	2018/19	Not started
Note: Target audit delivery per original approved plan is for 29 audits (16 internal control reviews and 13 change assurance reviews).					

POL00401626

Appendix 2a

POST OFFICE LIMITED – Internal Audit REPORT
AUDIT TITLE: Banking Counter Services Framework Review
REFERENCE: 2017/18-20 DATE ISSUED: 17 January 2018

Executive Summary

Background

A number of banking institutions (hereafter referred to as "Institutions") appointed Post Office Limited (POL) as their agent to perform services on their behalf at POL outlets as set out in the "Terms and Conditions to Members of Post Office Banking Counter Services Framework version 1.2 January 2017" ("the Framework Agreement"). The services performed by POL include automated services (e.g. cash withdrawal, etc…) and manual services (e.g. cash deposit via magnetic swipe banking card/barcoded deposit slip or pre-encoded personalised deposit slip; cheque deposits, etc...).

Scope & Approach

The objective of this audit was to assess adherence to the Framework Agreement by POL, including its Agencies. This review was not designed to be a deep dive into each area but rather to provide a high level view of the current Framework control environment.

Conclusion

The Framework Agreement includes specific requirements for the processes which directly enable the delivery and monitoring of the service (such as financial processes, management information, counter transaction processes and Link information security processes). For supporting processes (such as Financial Crime, Business Continuity, IT Security and Disaster Recovery processes), the Framework refers to the set of policies and procedures which are expected to be in place for the wider business activities.

With regards to the controls which are specific to the Framework, we observed that Management have implemented effective oversight in relation to the continuing operations of the key Framework processes. However, accountabilities for some services contained in the Framework Agreement have not been clearly assigned to different areas of the business. This contributed to the fact that some of the required documentations (i.e. a fraud prevention policy and the Link Information Security Standard) have yet to be developed.

With regards to controls which have wider business impact and are critical in supporting the Framework, it was noted that processes need to be strengthened in order to: (i) effectively monitore compliance with the financial crime policy; (ii) implement an effective governance (including planning and testing) of business continuity management (BCM); (iii) improve the IT Disaster Recovery (ITDR) governance arrangements and the oversight of the testing programme; (iv) update Information security policies and procedures. Also, for Payment Card Industry Data Security Standards (PCI DSS), back office processes are not included in the PCI scope and neither are users with access to Primary Account Numbers (PAN). There is no ongoing monitoring outside of the annual (external) audit.

This report has been rated 'Needs significant improvement' as it highlights weaknesses in internal controls, in particular within the supporting activities across Post Office, which may result in non-compliance with the Framework.

Management Comment

"Banking Framework management welcomes the findings in the report. Of particular note are the POL-wide findings revealed (PCI, IT security, BC/DR policies that impact all services) – and their potential impact on Banking Framework compliance. Framework specific issues identified are under active management to address." *Martin Kearsley (Director of Banking Services)*

Report rating:



Needs significant Improvement

POL00401626

Internal Audit Report: Banking Counter Services Framework Review

Summary of Findings

The table below provides a summary of the P1 and P2 findings and their ratings. The report also included 16 P3 observations and 5 advisory recommendations which have not been listed below.

Finding		Rating*	Action Owner	Date
Scope Area: Financial reconciliation				
1	No financial reconciliation between invoicing and settlement of transactions values.	P2	Dave Jenkins	31 March 2018
Scope Area: Business process integrity				
2	Inconsistent practices across the branch network for accepting Location Exercise based Santander Business deposits	P2	Martin Kearsley	31 March 2018
Scope Area: Financial Crime				
3	No documented fraud prevention policy / operating level process.	P2	Sally Smith	31 March 2018
4	There is no mechanism within POL to monitor compliance with the financial crime policy.	P2	Sally Smith	30 April 2018
Scope Area: Operational stability and resilience				
5	Governance of the business continuity management programme is ineffective.	P2	Tim Armit	31 March 2018
6	Agreed business impact assessments, business continuity strategies, business continuity plans and associated testing is not in place.	P2	Tim Armit	31 March 2018
7	The ITDR programme governance is not formalised.	P2	Mick Mitchell	31 March 2018
8	Recovery Point Objectives have not been defined.	P2	Mick Mitchell	31 March 2018
9	IT have limited oversight of the current ITDR testing programme.	P2	Mick Mitchell	31 March 2018
Scope Area: IT Security				
10	No evidence of the Link Information Security Standard	P1	Jules Harris	30 April 2018
11	Back office processes are not included in PCI scope.	P1	Jules Harris	30 September 2018
12	No ongoing monitoring of PCI DSS controls outside of the annual audit.	P2	Jules Harris	28 February 2018
13	Users with access to PAN are not included in PCI Scope.	P2	Jules Harris	30 September 2018

* P1 = High Priority, P2 = Medium Priority, P3 = Low Priority

POL00401626

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE

Internal Audit Plan 2018-19

Author: Johann Appel Sponsor: Jane Macleod Meeting date: 13th March 2018

Executive Summary

Context

1. The Post Office annual risk-based audit plan for 2018-19 has been prepared in accordance with the applicable requirements of the revised Internal Audit Charter as approved by the ARC in March 2017, as well as the professional standards of the Institute of Internal Auditors (IIA).

Questions addressed in this report

2. What processes, activities and programmes should be assured by Internal Audit in 2018-19? Does the proposed plan focus on the right priorities to support the Post Office strategic objectives?
3. What are the resource requirements to deliver this audit plan and how much will it cost?

Conclusion

4. An integrated audit plan has been prepared to provide assurance over principle business risks and significant change activities. The proposed plan can be summarised as follows:

Category	Number of audits	Estimated effort (days)		Approximate cost of co-source
		Total	Co-source	
Business Risks	16	585	130	£182k
Change Portfolio	10	270	270	£378k
Total	**26**	**855**	**400**	**£560k** [N1]

[N1] 2017-18 Co-source cost budget was £692k. The cost reduction of £132k is after providing for an increase in co-source day rates, but will be partially off-set by hiring a new in-house IT auditor. Overall comparative cost will remain broadly unchanged or marginally favourable compared to the prior year.

Input Sought

5. The Committee is asked to:
   a. Consider the proposed Internal Audit Plan for 2018-19 and confirm that individually and collectively these reviews represent an appropriate programme to support senior management in their activities and to provide assurance to the Audit, Risk & Compliance Committee (ARC) over key risks to the Post Office.
   b. Recommend the proposed Internal Audit Plan to the ARC for approval.

POL00401626

Detail

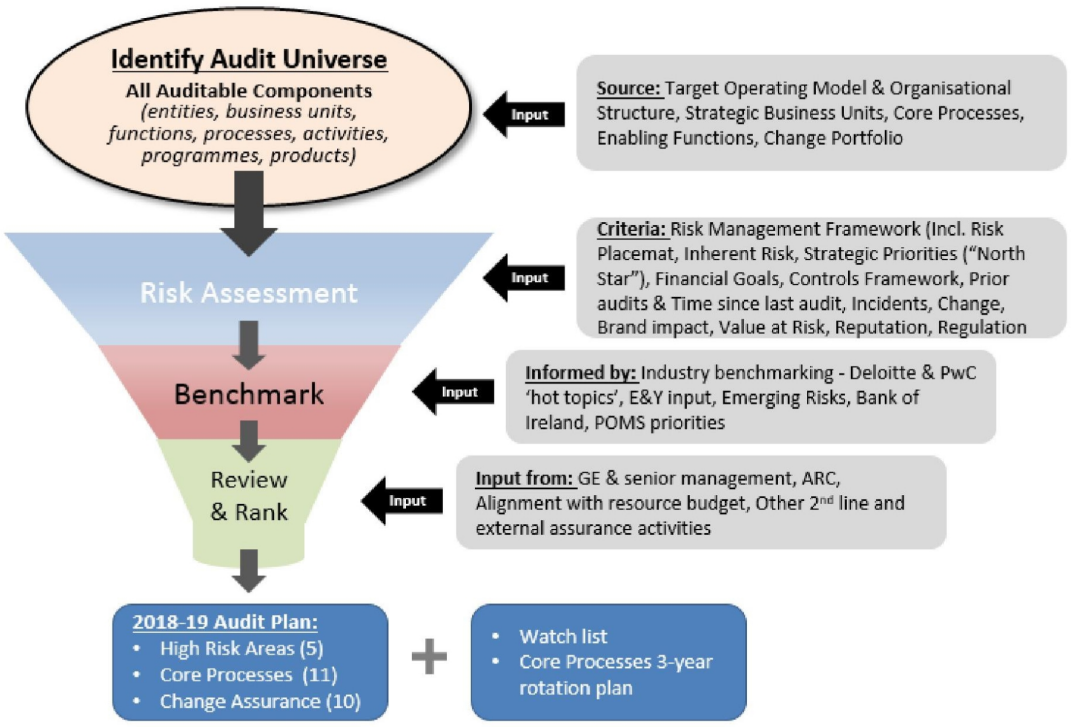
The Planning Context

6. Post Office risk profile is impacted by continued and significant internal change, increased regulatory scrutiny and market pressures. The 2018-19 Internal Audit plan is designed to provide assurance over the organisation's principle risks, core processes and material change activities.

7. As from 2017-18 we have introduced a three year rotation plan for core processes. Core processes are usually mature and generally assumed to be well controlled, but warrant cyclical validation due to their pervasive nature and criticality to the business. The 2018-19 plan includes the second tranche of core processes to be reviewed over a three period.

The Planning Process

8. The following diagram depicts the process we followed to identify, assess and prioritise the processes and activities to be assured in 2018-19:



The Planning Results

9. The proposed list of audits was discussed with GE members and senior management.

10. The tables below outline the proposed audits to take place in 2018-19. However, internal and external events may cause priorities and risk profiles to change, and management may have additional requests during the year for advisory support

POL00401626

or audit assistance. In consequence, we may consider amending the plan as the year progresses. We will seek ARC approval for all material changes to the plan.

11. **Table 1** represents the baseline plan for internal control reviews, of which the target delivery is 80% or 16 reviews.

1. Internal Control Reviews – Target = 16 reviews			
Rank	**Proposed Review**	**Sponsor(s)**	**Timing**
1	Payroll	Al Cameron & Martin Kirke	Q2
2	Accounts Payable	Al Cameron	Q1
3	Branch Cash Forecasting & Management	Al Cameron	Q1
4	Cyber Security	Rob Houghton	Q2
5	Supply Chain	Al Cameron	Flex
6	Contract Management	Al Cameron	Q3
7	IT Control Framework	Rob Houghton	Q2
8	Employee Expenses	Al Cameron & Martin Kirke	Flex
9	Client Settlements Process	Al Cameron	Q3
10	Digital Strategy & Capability	Owen Woodley & Rob Houghton	Flex
11	Whistle-blower Process	Jane MacLeod	Q4
12	Accounts Receivable	Al Cameron	Flex
13	Agents Remuneration	Debbie Smith & Al Cameron	Q3
14	Financial Control Framework	Al Cameron	Q4
15	FS Training & Competence	Owen Woodley & Martin Kirke	Flex
16	Online Sales (Product / Channel to be determined)	Owen Woodley	Flex
17	FRES Governance	Owen Woodley	Flex
18	Procurement (Pre-award)	Al Cameron	Flex
19	Marketing Process / Activities	Owen Woodley	Flex
20	Data Privacy	Jane MacLeod	Q4

12. **Table 2** represents planned reviews of significant change activities. The baseline plan is for 10 Change Assurance reviews. This is an indicative list based on the current change portfolio and will be reviewed and updated continuously as the portfolio of change programmes develops and the risk profile changes. The plan includes at least one thematic review focusing on programme governance (e.g. gating effectiveness, investment committee, agile methodology). In addition we will provide assurance over 9 change programmes – this could be assurance at a point in time or ongoing / real time assurance depending on the project.

POL00401626

2. Change Portfolio / Programme Assurance – Target = 10 reviews			
Rank	**Proposed Review**	**Main Sponsor**	**Timing**
1	Change Programme Governance	Rob Houghton	Q3
2	Panther (Business Integration)	Debbie Smith	Q2/3
3	DMB Strategy	Debbie Smith	tbd
4	Customer Hub – Horizontal & Travel	Owen Woodley	tbd
5	Postmasters Portal	Debbie Smith	tbd
6	Identity Services	Martin Edwards	tbd
7	Tracked Online / Disintermediation Risk	Debbie Smith	tbd
8	Customer Hub (Additional Verticals)	Owen Woodley	tbd
9	Banking Framework – Cash Management	Debbie Smith	tbd
10	Project Everest	Rob Houghton	tbd

13. **Table 3** is our 'watch list' of additional areas for consideration during the year, should either the assurance needs for the priority areas decrease or risk levels for items on our watch list increase. The watch list will also inform the 2019-20 audit plan.

	Topic / Area
1	Payment Services / Bill Payments
2	FS - Branch Sales: New distribution model (Customer Relationship Managers)
3	Asset management - Software licensing management
4	Equal Pay
5	Diversity & Inclusion
6	Sales – Post Office Money Mortgages
7	IR35 Adherence
8	DMB Stationery (WHSmith consignment stock)
9	Money Laundering Directive
10	Revenue Contracts (e.g. POCA)
11	New Agents Process (New Agent On-boarding)

POL00401626

Three Year Rotation Plan

14. In 2017-18 we introduced a rotational audit plan to assess core business processes over a three year cycle. This will provide regular assurance on the effective operation of controls over critical business processes. The rotational plan in the table below has been based on the last review of these processes, known issues and ongoing remedial programmes.

Core Processes – 3 Year Rotation Plan		
Year 1: 2017-18	**Year 2: 2018-19 (in plan)**	**Year 3: 2019-20**
Financial Reporting Controls	Financial Reporting Controls	Financial Reporting Controls
Branch Cash Forecasting & Management [1]	Bill to Cash (Accounts Receivable)	Record to Report (Financial Close)
Sales (Mails Process)	Sales (Rotate Sales Channels)	Sales (Rotate Sales Channels)
Business Continuity	Payroll	Treasury Operations
IT Operations (IT Governance and IT Risk management)	Procure to Pay	Regulatory Compliance
Client Settlements Process [1]	Supply Chain Management	FS Conduct Management Framework
	Contract Management	Fixed Assets
	Agents Remuneration	
	Employee Expenses	

[1] Postponed to 2018-19

Resource Requirements

15. The approved headcount for the internal audit team is 5 FTEs. We are currently recruiting for two vacancies. The co-source requirement to support delivery of the 2018-19 plan was estimated at approximately 400 days with a total cost of £560k. The cost is indicative only and likely to change once the new co-source provider has been selected.
16. The current co-source agreements with PwC and Deloitte runs until September 2018. It is our intention to replace the current arrangements with a single provider by August 2018 and we are in the process of inviting professional firms to tender for provision of these services.

END OF REPORT

POL00401626

GDPR Programme Update

Author: Clare D'Netto Sponsor: Jane MacLeod Meeting date: 13 March 2018

Executive Summary

Context

The General Data Protection Regulations ('GDPR') come into effect in May 2018. Post Office has a project underway to implement the necessary changes to achieve compliance with the GDPR requirements. As a key stakeholder, the Risk and Compliance Committee of Post Office Limited has requested updates on the progress of implementing the necessary changes as they impact Post Office. This update is following the paper submitted to RCC on the 18th January and the training session provided to the ARC on 23rd January.

Questions this paper addresses

1. Where are we relative to where we said we would be?
2. Where are we behind where we said we would be and do we have a path to green?
3. What are the key delivery risks to May?
4. What are the material risks to compliance?

Conclusion

1. Where there has been considerable progress since the programme last presented to the RCC on 18th January, this paper outlines where the certainty of delivery by May has decreased, and the mitigations in place for the following 'at risk' areas:
   (i) 100% of data breaches follow the updated procedures
   (ii) 100% processes updated for new employees, agents and job applicants
   (iii) 100% Privacy Notices and Privacy wording updated to existing employees and agents
   (iv) All contracts will be updated to reflect the GDPR, using a risk-based approach by May 2018.
2. This paper also identifies key material risks to compliance which the RCC is requested to note.

Input Sought

The RCC is requested to:

- note the material risks to effective compliance identified within this paper which will be formally addressd at the programme steering committee.

POL00401626

The Report

1. Where are we relative to where we said we would be?

1. The paper presented to RCC on 18th January described the components of 'effective compliance' that we aim to have in place by May 2018 and described our then level of certainty, in meeting that timeline in light of operational and technical capacity and other key dependencies. It also identified those activities which would therefore extend beyond that date.
2. Annex 1 summarises our current level of certainty in comparison to the position we stated in January, in relation to all new activities which were intended to be compliant with the GDPR by May 2018.
3. Progress has been made in many areas and our overall level of certainty has increased, including privacy notices and marketing permissions for new customers. This is based on our continued work with the business and partners to agree wording and commit to timescales. In addition, we have raised change requests for the POL technical changes. However, delivery of changes for marketing permission for Financial Services (BOI) products is currently at risk as this was dependent on a commercial agreement (see 18 (i)) on whether or not BOI can market to POL customers and then an agreed wording as a result.
4. The Education and Awareness activity in the run up to May is in train, with targeted face-to-face training for priority audiences and themed weekly comms going out to the business.
5. Annex 2 summarises our current level of certainty for all existing activities that will be remediated by May 2018 within the PO's risk appetite.
6. The key area of progress is that the Programme has completed an assessment of the potential impact of GDPR on the number of permissions in the back book to which we can continue to market, using Legitimate Interests.
7. As a result of this analysis, we have a med-high confidence that we can use Legitimate Interests to continue to market to leads who were active within the last 3 years where there is evidence of a relationship based on click through and web browsing. This equates to 4.7m permissions overall and 2m of email permissions, which is a minimal impact to the current situation, whereby the business only actively markets to a proportion of the overall leads in Brands, predominantly those permissions which are less than 3 years old. In Phase 2 of the Marketing sub-project we are investigating the outliers at a more granular level to understand if legitimate interests can be applied.

2. Where are we behind where we said we would be and do we have a path to green?

8. Delays to getting planned resources for key roles, including workstream leads for Governance & Framework, HR and Agents and Contracts, as well additional DP and HR PM resources have impacted on the following deliverables:

   (i) 100% of data breaches follow the updated procedures

POL00401626

(ii) 100% processes updated for new employees, agents and job applicants

(iii) 100% Privacy Notices and Privacy wording updated to existing employees and agents

(iv) All contracts will be updated to reflect the GDPR, using a risk-based approach by May 2018. This includes material (c 80) and non-material contracts (c.400) and SPM contracts.

9. We are working with the HR Business Partner to progress these roles through a mix of interim and consultancy/legal resources and have re-allocated critical tasks within the existing team. In addition, we have recruited a Programme Director to free up additional Programme Management capacity to focus on high-risk areas, including Contract remediation.

10. The remediation of existing contracts has been delayed as a result of a review of the POL DP clauses against the CCS PPN announced in December 2017. This has now been completed and has resulted in changes to the remediation packs. On the advice of Legal, we have also added an additional step to review the liability and insurance risk in existing contracts.

11. Both these factors have has delayed mobilisation of the business for contract remediation, therefore the Programme Team has looked at ways to streamline the process for remediation for non material and low risk contracts in order to minimise the impact. We are also progressing a streamlined process to assess liability and insurance risk in house and using WBD by exception.

3. What are the key delivery risks to May?

12. Delays to planned resources will continue to have an impact on these workstreams.

(i) 100% of data breaches follow the updated procedures

(ii) 100% processes updated for new employees, agents and job applicants

(iii) 100% Privacy Notices and Privacy wording updated to existing employees and agents

(iv) All contracts will be updated to reflect the GDPR, using a risk-based approach by May 2018. This includes material (c 80) and non-material contracts (c.400) and SPM contracts.

13. Quick resolution of resources for (i), (ii) and (iii) will enable us to get back on track for delivery May and this is an urgent focus for the Programme.

14. However, Contract remediation will continue to be at risk due to the delayed mobilisation and the timescales to complete the end-to-end remediation process, particularly high and medium risk contracts. We are prioritising POMS contracts and Tower IT contracts to mobilise first, however there is a dependency on agreement as to the personal data that Tower Vendors process on behalf of the Post Office.

15. A potential blocker for contract remediation will be the capacity of Contract Owners, which particulary applies to high and medium risk contracts, where they will be required to be more involved in the remediation process.

POL00401626

16. We will need confirmed Contract Owners for all contracts, including non-material contracts otherwise we will be unable to remediate. The Programme will be sending out a communication to GE to get confirmation of Contract Owners and to identify any contracts that are not currently on Bravo, and therefore we are not aware of, so we can progress these.

17. Although we have increased confidence regarding delivery of customer-facing changes for new privacy notices and marketing permissions, the timescales for operational and technical changes remain tight. The key risk areas are changes to in branch materials and technical changes on the *partner's* side. The Project Manager is continuing to work with the business and partners to track delivery risk and identify remediations.

4. What are the material risks to compliance?

18. The following material risks have been identified i.e. where there is a risk that the agreed remediation may be considered to not be compliant with the GDPR. The programme is documenting these risks for decision / acceptance by the business via the Programme Governance. All risk-based decisions, including rationale, will be held on OneTrust.

(i) **IRRELEVANT**

(ii) Telecoms currently retain telecoms data at 7 years, which is non-compliant, however they are working towards implementing a 24 month retention period. This will take 12 months to implement, which we consider to be a defensible position.

In the meantime, not being able to delete data that is more than 7 years old before May, could result in fines and compensation if there is a customer complaint.

(iii) Where ever we rely on legitimate interests, including Marketing to the back book and Telecoms, for credit referencing/debt management, there is risk. However we are documenting our rationale for using Legitimate Interests via positioning papers for decision through Programme Governance.

(iv) Due to gaps in Product Manager knowledge and documentation, there is a risk that we have not captured all data types and data flows as part of the information audit and this impacts on the information we provide in the privacy notices. The information captured by the Programme will be held in One Trust and we will establish processes, including the PIA, to ensure that documentation will be updated and maintained to reflect subsequent changes.

(v) Due to gaps in business knowledge and documentation on the personal data processed by IT vendors, there is a risk that we have not captured

POL00401626

all data types and data flows as part of the information audit. This presents a potential risk to the accuracy of processing schedules and therefore the accountabity of our processors in the case of a data breach. Again, improved processes, including PIAs and Change Requests, need to be in place to ensure documentation is maintained in BAU.

(vi) There is risk that the Programme does not have a complete view of all the personal data held by non-IT vendors and in software licenses, due to limited available information in the business. We may not be able to complete personal data analysis which may cause fines from ICO for failure to maintain an up to date inventory and or / if there is a data breach for an unidentified vendor. The Programme is currently working with IT and Procurement on this, however there will be a requirement for tighter controls for new IT vendors and software.

POL00401626

Annex 1 - All <u>new</u> activities are compliant with the GDPR in the following areas by May 2018

Deliverables	Certainty (Jan 18)	Certainty (Mar 18)	Commentary
Privacy Management Governance framework will be implemented to demonstrate Accountability	Medium	Medium	• **No change**: We are engaging specialist resource to lead the Governance & Framework Workstream and increasing the capacity in the DP team, however this activity has a lead time. • However, the team is building the structure for the One Trust Tool which will be the key repository and tool to demonstrate accountability via holding PIAs, LIAs, records of processing activity.
100% privacy notices and privacy wording updated – all channels	Medium	Medium-High	• **Increased**: Considerable progress has been made in drafting of the Privacy Notices, including the overall Privacy wording for Post Office. We are advanced in our discussions with BOI and FRES. The POCA privacy notice has been approved and Telecoms and POMS Travel Insurance are complete. CRs have been raised for POMs TI and POL Digital and Horizon Changes for a go live by end of April. • There are delays at specific partner / product level e.g. Tif/RLG aren't ready with their privacy notices and other journey changes, however we are working with them.
100% Marketing Permissions updated – all channels / partners	Low/ Medium	Medium	• **Increased certainty**: Considerable progress as stated above, including the approval and dissemination of the new Marketing Permissions. Plans are advanced with POL, POMS and partners and CRs has been raised for POL technical changes. • There are Product/Partner-specific dependencies, including the commercial decision for BOI which has impacted on the

POL00401626

Deliverables	Certainty (Jan 18)	Certainty (Mar 18)	Commentary
			time taken to agree the wording for the marketing permissions. Telecoms has flagged capacity constraints to implement across all channels, including product packs. • Timescales to implement operational and technical changes are tight, specifically for technical changes on the partner side and for updating materials in branch.
100% processes updated for new employees, agents and job applicants	Medium	Low/ Medium	• **Decreased certainty:** There is limited time to complete changes by May 2018, however activities are being prioritised using a risk based approach so some activities will continue after May 2018. • The onboarding of a Workstream lead and additional HR PM resource is critical to progress this workstream.
100% of requests follow new and updated procedures for rights	Medium	Medium	• **No change:** Subject to engagement of the Governance & Framework Workstream Lead. Resources identified to update the procedures for individual rights however are potential DP constraints • The known – unknown is the capability of providers to delete data which is already a requirement of current contracts. This is being validated via the Systems Workstream.
100% of data breaches follow the updated procedures	Medium – High	Medium	• **Decreased certainty:** We are engaging specialist resource to lead the Governance & Framework Workstream and increasing the capacity in the DP team, however this activity has a lead time and we planned to complete Testing in March. • Potential issues have been identified with the Atos Incident Management Process which will need to be reviewed as part of this workstream.

POL00401626

Deliverables	Certainty (Jan 18)	Certainty (Mar 18)	Commentary
100% of new contracts contain the new DP clauses and schedules	High	High	• **No change:** P Suite further updated in Feb, to reflect the CCS PPN and security wording.
100% new contracts contain the new security standards	High	High	• **No change:** The existing documentation is being updated to provide a fully updated policy and set of standards for Post Office by June. However we have removed the hard dependency for the Contract Remediation workstream by inserting a short form of words and updating the existing schedule 16 in line with GDPR.
An audit and due diligence process for suppliers will be ready for implementation from May 2018	High	High	• **No change:** Work is currently underway to develop this using the OneTrust tool.
100% of new projects complete a Privacy Impact Assessment (high risk projects)	High	High	• **No change:** However the existing PIA will be launched via OneTrust and there is a requirement to fully embed this process for all products.
100% of relevant employees have received Training and Comms	Medium – High	High	• **Increased certainty**: A new workstream lead is in role, plans are well developed and a training provider has been identified.

POL00401626

Annex 2 - Existing activities that will be remediated by May 2018 within the PO's risk appetite

Deliverables	Certainty (Jan 18)	Certainty (Mar 18)	Commentary
Information audit completed, using a risk-based approach	Medium	Medium	**No change:** • Product Reviews**:** T1 products analysis has been completed but there are some information gaps due to lack of knowledge / documentation in the business. There is a risk that Completion of the remaining T2 & T3 product will continue beyond May. • Systems questionnaire: IT Vendors have provided incomplete information (See systems) • Business Functions: We have agreed an approach using a risk-based approach.
100% Privacy Notices and Privacy wording updated to existing customers	Medium	Medium	**No change:** • Activities agreed with e.g. POMS via renewals and Telecoms. This is included in planning discussions with partners where relevant and is subject to the same dependencies as for privacy notices for new customers.
Continuation of marketing to the back book using legitimate interests	Medium	High	**Increased certainty**: • Positioning Paper agreed at the last Programme Steering Group to support Marketing to the Back Book.
100% Privacy Notices and Privacy wording updated to existing employees and agents	Medium	Low-Medium	**Decreased certainty:** Risk to timescales to implement all changes by May 2018 due to resource constraints.
All contracts will be updated to reflect the GDPR, using a risk-	Medium	Low-Medium	**Decreased certainty:** Delayed mobilisation as we needed to review and update the DP clauses against the CCS PPN

POL00401626

Deliverables	Certainty (Jan 18)	Certainty (Mar 18)	Commentary
based approach by May 2018. This includes material (c 80) and non-material contracts (c.400) and SPM contracts			clauses. The inclusion of the risk assessment for liabilities and insurance had increased end to end timescales. The Programme is planning to on-board a specialist resource to lead this workstream as there will be strong business engagement with Contract Owners. Potential blocker: Contract Owners are still not confirmed and they are critical to this workstream. Constraints: Contract Owners time constraints to engage with this activity.

POL00401626

PCI-DSS Compliance Status Report

Authors: Jules Harris/Nicholas Spicer Sponsor: Jane Macleod/Debbie Smith Meeting date: 13 March 2018

Executive Summary

Context

Post Office (PO) processes c85m transactions worth c£4.5bn of card payments to our card acquirer Global Payments (GP). As part of the payment card industry requirements, and due to our large numbers we are classified as a level 1 merchant, there is a requirement to obtain an external audit verified Report on Compliance (RoC) to the Payment Card Industry – Data Security Standards (PCI-DSS). This is an annual process. The Payment Council regularly update the control requirements, in order to ensure that new threats and vulnerabilities are covered. The standard was substantially updated in 2017, and the new version V3.2 put more control requirements on Post Office compared with the previous version to which we achieved compliance last year.

PO appointed a new external auditor this year, and this new auditor is well known for being very thorough in their approach to completion of the audit testing.

The existing RoC expired on 28th December 2017. We have shared our remediation plans with GP, and to date they are satisfied with our expectation to receive a passing RoC by 31st July 2018. Whilst GP could levy penalties against PO, currently they have not chosen to take this action.

Questions this paper addresses

- What were the issues to getting the RoC in the first place?
- What have we already fixed and what remains?
- GP has given PO dispensation to resolve certain issues over a longer period – what are the implications of this?
- What other actions are PO taking in regard to our PCI-DSS compliance?

Conclusion

1. PO are required to be certified to PCI-DSS standards by a number of contracts, most notably the Banking Framework. It is the opinion of the authors that with the relationship we have with our acquirer we will be able to satisfy the banks that their customer data is not at risk.
2. RCC are asked to note that there is a risk in this regard.

Input Sought

RCC is requested to note this paper.

POL00401626

Report

What were the issues to getting the RoC in the first place?

3. There are extra requirements that have been added to the standard during 2017, which owing to the age of our estate are extremely challenging to implement. Additionally, the new auditor has taken a much more forensic approach than previous auditors, and through this has identified further areas of non-conformity.

4. This is the first year that ComputaCenter (CC) have been included in the scope of our PCI certification. Despite engagement since April 2017, they have not been able to complete their required actions in a reasonable timeframe. This has been escalated to senior CC account management in order to try to resolve the issue.

5. CC have struggled to understand the principles of PCI despite escalation to get a qualified PCI expert on board, they have only done this in the last month.

What have we already fixed and what remains?

6. There were 35 items for Fujitsu (FJ) to fix. Of these 3 have been closed, 25 have been completed, and the remaining 7 are on schedule to be fixed by mid-April.

7. There were 32 items for CC to fix. Of these 5 have been closed, 17 have been completed. A further 6 are due be fixed by mid-April. The remaining 4 items are now being worked on by CC, PO are waiting for a confirmed completion date. Initial feedback is that one will take 3 to 6 months to resolve. PO has fed back that this is unacceptable, and are looking at different ways to achieve the desired outcomes without CC effort. There is a possible option to use Verizon and FJ to achieve a suitable set of controls, so as a precaution Change Requests (CRs) have been submitted and we are awaiting formal proposals.

8. The dates have been booked for the external auditor to visit both CC and FJ to see the evidence that the closed controls are all now in place.

Where have PO been given dispensation by GP to allow us longer to resolve some complex issues?

9. There is a back office system called TESQA which is used by the fraud and operations teams to monitor activity and support fraud and police queries related to banking transactions. This system has to retain the full 16 digit card number in order to be able to function. As this system has very limited access (4 terminals in all) and was not previously within scope GP have issued a dispensation for 2018 to allow the external auditor to exclude it from our RoC. PO are looking at options to bring the system within compliance by as part of a wider payment technology upgrade programme.

What other actions are PO taking in regard to our PCI-DSS compliance?

10. The PCI steering committee "PCI SteerCo" has been stood up to ensure focus on resolution by bringing all relevant parties to the table on a weekly basis. The PCI SteerCo programme team has worked with internal and external stakeholders to

POL00401626

track each remedial activity for each of the Vendors (FJ, CC, Accenture, etc.), and provide a weekly update report to PCI SteerCo members. The most recent report has been included as a supporting document. The Steerco programme team also raised the aforementioned CRs for the outstanding CC remedial items that CC have been commercial disputing as out of scope.

11. The legal team is support the CC vendor manager to resolve the CC claim that their contract did not require them to be PCI compliant. PO have paid CC to perform the remedial actions to stop the delays, this will be reviewed and if found to be in PO favour, the monies will be claimed back.

12. PO has a historic issue with the contract with FJ on the version of PCI they will comply with, so this will also be renegotiated after the RoC has been received.

13. PO will run a discovery exercise later in 2018 to test where else payment card details are stored. This will be commissioned once the RoC has been received.

POL00401626

Project Dashboard – *PCI DSS SteerCo*

Minutes (23/02/18):

- Branch visits (48) now complete. Tamper check procedure note sent to branches
- FJ on track for end of March – although additional risk raised for "unknown unknowns" resulting from Segmentation and penetration testing remediation

- Computacenter QSA assessments are scheduled to start w/c 19/3
- Computacenter POAP provided high level view of remediation actions to descope non-payments infrastructure and address network segmentation. POL requested detailed implementation plan
- Network segmentation at Computacenter is a pre-requisite for segmentation and penetration testing
- Solution options proposal for CRs to be presented on 27/2
- A resource constraint (Security Architect) was identified as a possible risk

- Credence: issues getting access to test env, however now on track for 4/3 delivery
- Analysis and rework to implement APADC scripting required after implementation of the Credence cleanup activity

Actions (23/02/18):

- Angus requested meeting on Monday 26/2

POL00401626

Project Dashboard – *PCI DSS RAG / Summary*

Project Name	*PCI DSS*	**Reporting Date**	*02/03/18*
Project Leads	*PM: Chris Eluwa, BA: Simon Woods, Business Owner in Post Office: Nicholas Spicer,*		
Purpose	IRRELEVANT		

Overall	Delivery	Cost	Benefit	Risk
R →	R →	R ↓	A →	R →

Actions Outstanding	Actions For Review	Actions Resolved
17 ↑	42 ↑	8 →

Arrows indicate movement from previous period (downward worsening, upward improving, horizontal no change)

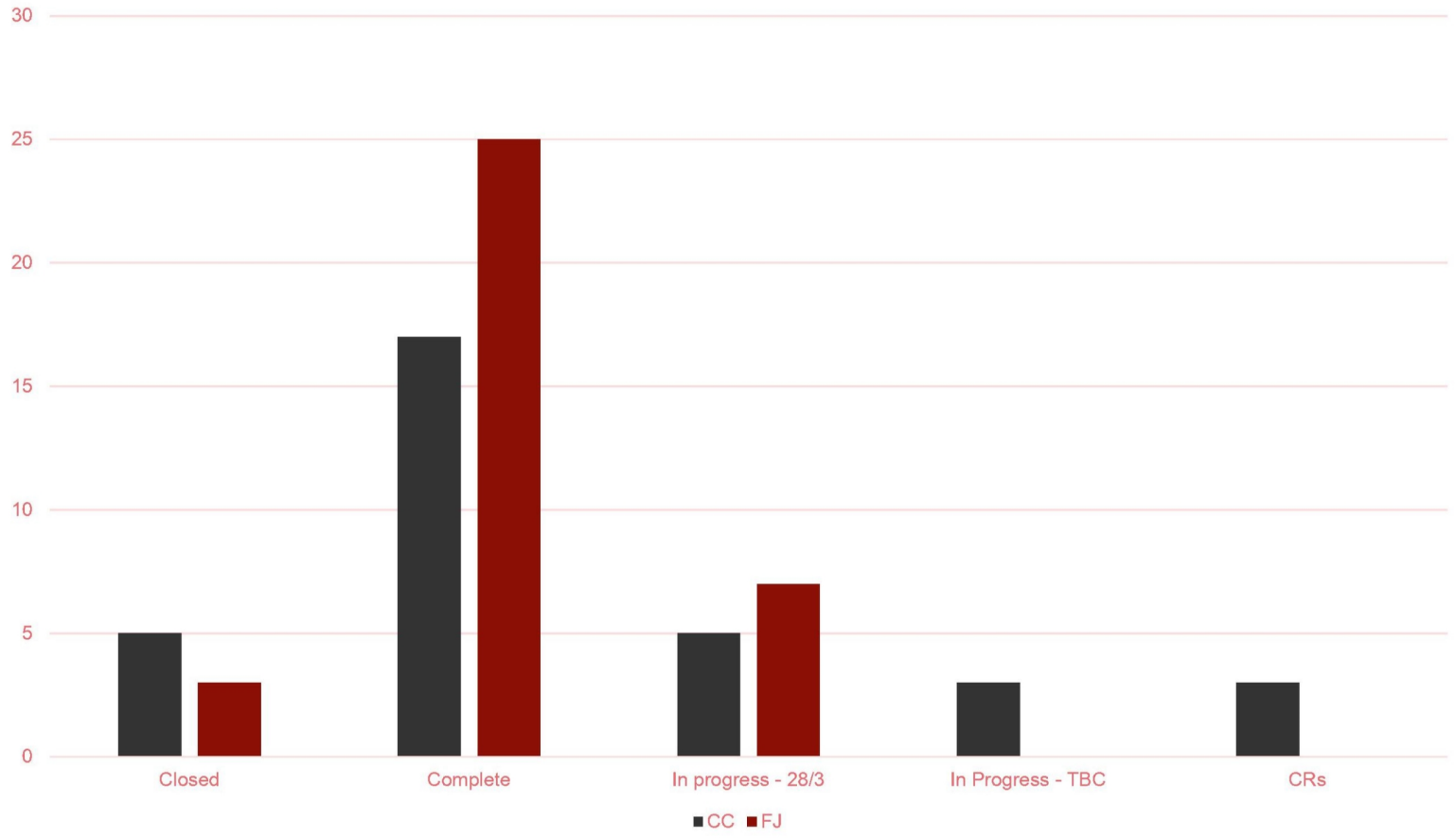
Actions outstanding relate to the remediation plan activities which are grouped by area. Further detail of actions being undertaken is provided on the "Update on suppliers" slide

Executive Summary and Route to Green

IRRELEVANT

POL00401626

Progress Snapshot – *PCI DSS (as at 28/02/18)*



POL00401626

Risks / Issues

Risk / Issue	Top Project Risks/Issues (With Impact)	Likelihood (Current 1-5)	Impact (Current 1-5)	Risk Score (Current)	Mitigation (Route to Green)
~~Risk 1~~	~~There is a risk that the business will not be PCI compliant within the required deadline - 28th December 2017.~~	4	4	~~16~~	~~Engage stakeholders and PM/BA to monitor the remediation plan~~ ~~Note: We did experience the same challenges last year and we were able to manage/ mitigate this successful with our QSA and card acquirer Global Payments. This has been raised to both FST and Retail risk managers.~~ Risk superseded by risk 3.
Risk 2	There is a risk that the business will not be PCI compliant by the IPA-proposed remediation date of 30th March 2018	5	5	25	Formation of a weekly stakeholder steering committee every Friday and updating of RCC. Setting accountabilities with Nettitude. QSA peer review of findings. Commencement of remediation plan including tracking actions. Measurement/Output – achievement of PCI certification by or before revised 31/3/18 deadline. Engage with Acquirer, Partner Banks and Gov Clients to advise of current position and provide high level plan to compliance
~~Risk 3~~	~~There is a risk that POL change freeze (commencing 20/11) will prevent remediation activities from being completed, increasing the likelihood of risk 1.~~	~~1~~	~~5~~	~~5~~	~~Request dispensation with system Owners to conduct change-related activities inside of change freeze window.~~ Risk closed: POL change freeze has ended.
Risk 4	There is a risk that the scope of actions identified falls outside of the contracted services provided by suppliers, requiring contract revision or amendment and increased cost of service provision.	4	4	16	Agree scope of service with suppliers and procurement Estimate additional costs and present business case for future funding approval 3 CRs have been raised to CC to resolve the disputed scope of their obligations.
Risk 5	IRRELEVANT				
Risk 6	There is a risk that the segmentation/penetration test results identify additional remediation activities that will take until after 31/3 to complete.	1	3	3	Agree with FJ to remediate Seg/pen test results as matter of priority Note: as the potential seg/penetration issues are "unknown unknowns" is it not possible to know all mitigation activities at this early stage.
Issue 1	IRRELEVANT				
Issue 2					

POL00401626

Update on Suppliers

Supplier	Target Resolution Date	Update on Remediation	Status ("In Progress"/"Cannot Address"/"Closed")	Mitigation If Status = "Cannot Address"
Fujitsu	31/03/18	Fujitsu 35 Emerging Findings 3 Finding Closed by QSA 25 Findings marked as Complete (QSA to review and close) 7 Emerging findings In Progress 0 Emerging Findings To Initiate CR raised and approved for FJS to provide consultancy assistance for an "at source" solution for the data flowing from Horizon through PODG and Credence.	In progress	
Computa-Center	31/3/18	Computacenter 32 Emerging Findings 5 Finding Closed by QSA 17 Complete to be closed by QSA 10 Emerging findings In Progress 4 Findings above in progress Change Requests have been raised.	In progress	
Verizon	28/12/17	Verizon's scope for remediation is limited but may include wi-fi vulnerability scanning and identifying unauthorised connected devices. Scope to be confirmed	In progress	
IPA	30/3/18	Organising outstanding audit activities with QSA: • 46 branches visits were completed over the past 3 weeks • Completed the planned sample size of 60 branches • Arranged the Fujitsu Belfast site visit which shall take place W/C 5th March • Article on card machine tamper checks was published onto branch focus	In progress	
Accenture	04/03/18 ~~21/02/18~~ ~~12/02/18~~ ~~08/02/18~~	Issues in test identified; awaiting resource from data team to confirm issues resolved. Targeting 28/2 for forward fix, 4/3 for historic cleanse CR approved for Accenture to obfuscate the PAN data from Credence – due for delivery approx. 12th Feb 18 CR raise for Accenture to provide a solution to remove the PAN data from the Credence server (which the data lands on from PODG before being FTP to Credence	In Progress	

POL00401626

Procurement Compliance Reporting

Author: Barbara Brannon Sponsor: Al Cameron Meeting Date: 13 March 2018

Executive Summary

Context

As a business in receipt of public funds POL is bound by the Public Contract Regulations (2015). PCR 2015 oblige POL to behave in a fair, objective & transparent way when contracting with 3rd party suppliers. Additionally, set procedures must be followed for spend above £25k and £181,302 (total contract value, increased from £164,500 in 2018).

Failure to abide by the legislation or "slicing and dicing" contracts exposes POL to risk, both as far the commercial outcomes of the contracts as well as the reputational damage, legal remedies, censure & fines that can follow the discovery of a breach. Our compliance to PCR can be requested under a Freedom of Information request at any time.

The PCR Compliance Register allows for the tracking of breaches to PCR regulations at the Post Office and internal governance processes. One aim of collating this information is to drive improvement in awareness and compliance behaviour across the organisation. The second and primary aim is to work with GE and Business Units to commence commercial reviews in a more timely way ensuring POL obtains value, commercial and contractual flexibility fitting the requirements and business strategy of the organisation.

Questions addressed in this paper

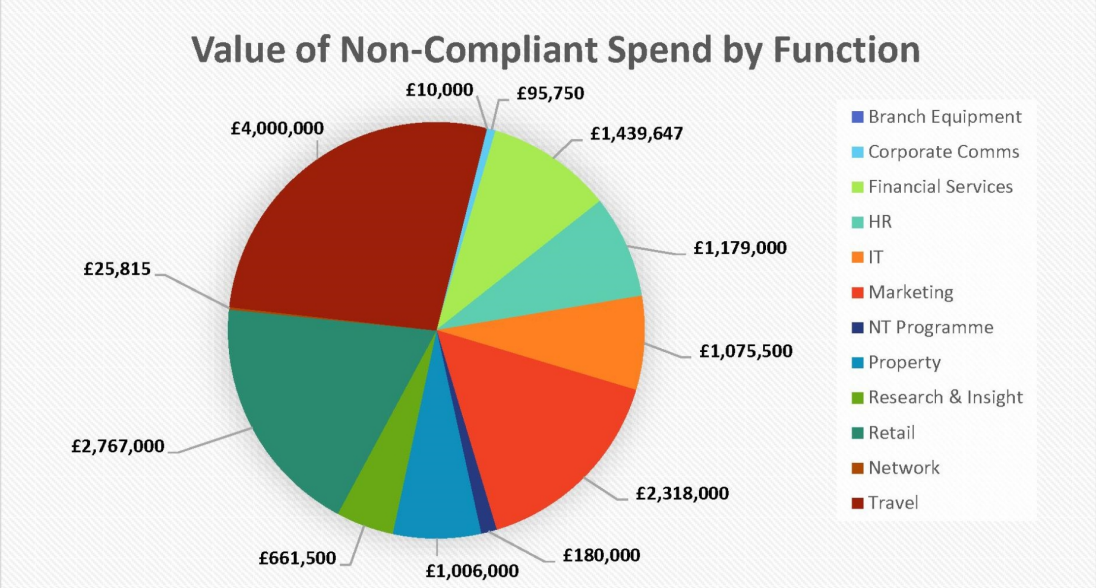
1. *How many and what types of procurement non-compliance have occurred in the past quarter?*
   Since the last RCC in October there have been a total of 0 non-compliant incidents with a total value of £0.

2. *What are we doing about it?*
   In the past quarter, while we have no new non-compliant spend we have reviewed and adjusted forecast spend data against actuals resulting in a small reduction in risk exposure overall. Our overall value has therefore dropped from £15m in January to £14.75m in March.

POL00401626

Open non-compliant awards since January 2017 are outlined below:

Function	January - Sum of Value	March - Sum of Value
Branch Equipment	£ 10,000	£ 10,000
Corporate Comms	£ 95,750	£ 95,750
Financial Services	£ 1,289,647	£ 1,439,647
HR	£ 1,579,000	£ 1,179,000
IT	£ 1,075,500	£ 1,075,500
Marketing	£ 2,318,000	£ 2,318,000
NT Programme	£ 180,000	£ 180,000
Property	£ 1,006,000	£ 1,006,000
Research & Insight	£ 661,500	£ 661,500
Retail	£ 2,767,000	£ 2,767,000
Network	£ 25,815	£ 25,815
Travel	£ 4,000,000	£ 4,000,000
Grand Total	**£ 15,008,212**	**£ 14,758,212**



3. *What are the potential consequences?*
    a. Pre-contractual remedies overview: During a Procurement, an aggrieved party can seek an interim injunction suspending the tender or the implementation until the court decides on an outcome.
    b. Post-contractual remedies: The court can order an 'ineffectiveness order' rendering the contract void &/or can award damages.

4. *Why are these incidents occurring, and what can be done about it?*

Non-compliant awards are made for a variety of reasons at the Post Office.

POL00401626

a) Low value, time constrained or highly sensitive/specialist engagements are common. For example, the Board have requested a number of expedited reviews since the New Year on a short turn-around time.
b) Large commercial arrangements cannot often be easily competed or unravelled without operational impact, and re-procurement may be subject to a pending evolution of a supporting Business Strategy.
c) The contractual arrangements may pre-date PCR 2015 regulations or the contract novated during separation from RMG, automatically becoming non-compliant at the renewal point. Non-compliant awards are frequently made on a tactical basis to extend contractual services while public tender processes are executed.
d) Delays to public sector panels of suppliers becoming available. The Post office makes extensive use of this low cost route to market and new/refreshed panels are subject to frequent delays from Crown Commercial Services. Single interim extensions [of periods under 12 months] while tender processes are run are considered to be low risk legally.
e) Changes in scope or value over the term of a contract may render the extension or renewal of services non-compliant. Material changes to the scope of a contract may render the whole contract non-compliant.
f) Disregard for, or lack of understanding of the regulations.

5. *Why are we receiving this report now?*

A decision to collate this information into a single location was taken in the Autumn of 2016. The aim is to track and improve our overall compliance and commercial results as an organisation, while also ensuring perceptions are accurate. However it should be noted that it will facilitate timely responses to Freedom of Information requests which adds risk to the Post Office commercial landscape.

6. *What is in the current Procurement pipeline which is high value and at risk of being awarded non-compliantly?*

A full list is appended at Appendix B. Since the last RCC in January 2018, three material items have been added. Two short term contract extensions for Internal Communications services and Events Management have been proposed while tender processes are concluded however, the extension provides commercial and contractual cover with no commitment to spend. The aim is to expedite the tenders to ensure any pending large value work goes under a new supply agreement.

POL00401626

The last item is for POL's ATM supply and maintenance services currently provided by Bank of Ireland. The value of this contract is £30m (p.a.) in income/revenue to POL. It was exempt from PCR when awarded in 2005 and the re-stated contract in 2014 but any new contract that POL intends to enter into will now be subject to the Concession Contracts Regulations 2016 and is therefore requires to be published. The current contract expires on 31st March 2022.

BoI and POL have agreed in principle to extension of the individual [ATM] Licences that expire during the period of the current contract, up to 31st March 2022 and that this has been recorded in the POL/BoI ATM Monthly Board April 2017.

As the current contract was not subject to CCR and the PCR, it is unlikely that the above variation (extension) can be successfully challenged under those Regulations.

Conclusion

Non-compliant awards of contracts are already subject to extensive internal governance, legal and risk review, explicit GE and Board approval where value/risks reach a minimum threshold.

*The YTD non-compliance value is high at £**14,758,212** the majority of which are interim extensions while procurement processes are run and to allow for operational migration risk to be mitigated. Individually, all large value non-compliant contracts have been reviewed by appropriate Post Office governance forums with agreement on next steps and actions towards remediation allocated where appropriate.*

Executive support towards moving POL towards a more compliant footing is very strong, but equally as important there is extensive support towards the cultural change required to ensure that Procurement activities and outcomes will support longer term business strategies and we reduce commercial risk making our 3rd party arrangements fit for purpose.

Input Sought

Review and note content only.

POL00401626

The Report

1. *Are any of these breaches arguable on regulatory grounds or are they all breaches?*

A full explanation of the individual compliance breaches for direct awards over £181k [previously £164k] threshold is attached in Appendix A. Each entry details the nature of, and the value of the breach.

The Procurement Compliance Register does not at present give an indicative risk level attached to the award. This information is provided to the accountable executives under internal governance processes in the form of a PCR risk note before a contract above threshold is entered into, and if necessary under Legal Privilege. In addition, all signatories to a contract have sight of the Risk note as part of the Contract Authorisation Form [CAF].

All entries are compliance breaches. A period of challenge applies to each PCR breach once an aggrieved party becomes aware or ought to have become aware. This risk finally expires at 6 years from the date of breach. The defensibility of a legal challenge is outlined within a Risk Note.

2. *How many of the breaches were approved in advance and how many retrospectively?*

All contracts entered into during this period were compliant with internal governance processes on contract and commercial review. All were for awards of between £0 and £4,000,000.

3. *Why were the approvals given?*

The rationale for approval is relevant to the individual service and is detailed within Appendix A.

4. *What were the unapproved, material breaches?*

There were no unapproved, material breaches during this period.

5. Describe the causes of non-compliance to PCR regulations

Non-compliant awards of contract are made for a variety of reasons at the Post Office:

a) Low value, time constrained or highly sensitive/specialist engagements are common. For example, the Board have requested a number of expedited reviews since the New Year on a short turn-around time.
b) Large commercial arrangements cannot often be easily competed or unravelled without operational impact, and re-procurement may be subject to a pending evolution of a supporting Business Strategy.
c) The contractual arrangements may pre-date PCR 2015 regulations or the contract novated during separation from RMG, automatically becoming non-

POL00401626

compliant at the renewal point. Non-compliant awards are frequently made on a tactical basis to extend contractual services while public tender processes are executed.

d) Delays to public sector panels of suppliers becoming available. The Post office makes extensive use of this low cost route to market and new/refreshed panels are subject to frequent delays from Crown Commercial Services.
e) Changes in scope over the term of a contract may render the extension or renewal of services non-compliant. Material changes to the scope of a contract may render the whole contract non-compliant.
f) Disregard for, or lack of understanding of the regulations.

6. *Describe what you are doing about the breaches. Where we are in breach, do we have a plan to come back into compliance and over what time period will that plan take effect?*

a) A forward view of material contracts falling under each Business Unit is currently prepared by the relevant Procurement Manager for discussions with their key stakeholders. The maturity of this look ahead view does vary currently and is a high priority activity within the team.
b) Sourcing options papers are prepared for review by contract managers and key stakeholders [risk, legal, security] with routes to market agreed. In many cases these are dependent on evolving business and operating model strategies and the Procurement team are now actively involved with some units helping to advise as thinking evolves.
c) Where a non-compliant award is proposed due to time pressure, Procurement are actively working on long term mitigation with awards made on an interim basis to meet urgent operational needs.
d) Each RCC member will now receive a regular report on compliance within their business unit[s].
e) A new Risk & Governance process requires a Risk Exception report to be created for non-compliant direct awards with SLT or GE sign off.
f) All Professional Services engagements must be approved in writing in advance by the COO. A compliant panel of preferred consulting partners has been appointed and proposed engagements outside of this panel are subject to additional review and challenge.
g) Procurement will now provide training as part of the revised Induction process for new staff. Training packs are being updated for existing staff and made available on the Intranet and ad hoc training sessions for interested Business Units are being run.
h) A new Intranet site has been launched for Procurement to improve visibility of process, regulation, and the panels of approved compliant suppliers available to POL business units.
i) A revised POL Procurement Policy is being drafted giving more granular guidance.
j) Using Crown Commercial Services frameworks, panels of Preferred Suppliers are being refreshed and updated across a wide range of spend categories to reduce time to market, improve compliance and greatly improve commercial outcomes and legal risk.

POL00401626

k) A planned change to operational systems will, once live, give Procurement earlier visibility of potential compliance issues eg: contractual value thresholds.

Appendices

1. Appendix A PCR Compliance Risk Register [Attached]
2. Appendix B Procurement Pipeline [Attached]

POL00401626

APPENDIX A

Incident Ref No	Date	Category Manager	Procurement Category	Function	GE Member	User / Staff Name	Value/ Income	PCR Compliance Resolved	Supplier Name	Breach Type 1 - PCR Threshold	Event (what happened) ONLY FOR £25K>	Actions Taken ONLY FOR £25K>	Further Planned Actions ONLY FOR £25K>
2017/0009	21 March 2017	Nicola Sams	Comms, R&I & PR	Research & Insight	Paula Vennells	Ruth Moyer	£ 652,000	OPEN	Inmoment	PCR - >£164.5k	Voice of Customer tracking is used as a performance measure for the business. It used to be a measure for the whole business but is now a measure for the individual Post office's performance	Due to the tracker still being an important measure for the individual post offices the supplier's contracgt will be extended.	Once POL understands how it wants to measure performance a review of current CCS framework that may be applicable or an full OJEU for the requirement will be conducted. Pending Long term requirements and budget from Marketing.
2017/0013	23 March 2017	Antony Ray	Professional Services	HR	Martin Kirke	Stacie Drury	£ 300,000	OPEN	Various	PCR - >£164.5k	Requirements and HR personnel changed. OLD PSL fell into disuse.	As a temporary measure, a short term agreement with standardise commercial terms and fees has been implemented with approximately 50 suppliers. The agreement effective from 1st July 2017 is in place until 31st March 2018 with an option to extend if necessary.	Current short term agreements in place with recruitment agencies due to expire on 31st March 2018. As the new CCS isn't available yet, these will be extended for a further 6 months before we move to a permanent solution. HR is now undertaking a review to determine agency use and spend, hence we will be extending only with the agencies we used the most and performed well. CCS now finalizing tender documents for new Permanent Recruitment framework which
2017/0016	12 April 2017	Nicola Sams	Marketing	Marketing	Nick Kennett	Louise Fowler	£ 2,000,000	WIP	Latitude	PCR - >£164.5k	Latest requisition is sub-OJEU threshold but there are several per month that support mainly Credit Cards, Loans and Mortgage products.	Seeking proposal from Carat (Media Agency) for consolidation within their compliantly let contract.	If proposal is acceptable from Carat then consolidate with them enabling an integrated approach to our full media investment.
2017/0019	01 June 2017	Antony Ray	Professional Services	HR	Martin Kirke	Harpreet Singh	£ 400,000		Towers Watson	PCR - >£164.5k		It was agreed to close the RMPP (DB Pension scheme) in 2016, closure required actuarial advice from a provider that knew the history and complexity of the RMPP. It was necessary to keep Towers Watson for their expertise.	In line with the Board strategy to de-risk the RMPP as far as possible, PO has requested that the Trustee of RMPP look to buy-out the liabilities of the RMPP as soon as possible whilst not requiring further money from PO. The earliest this can happen is 1 April 2018. It is anticipated that the majority of RMPP liabilities will be bought out by 1 April 2019 at the latest. Actuarial advice will be required during this phase. Anticpated spend to 2019 will be £135k. If buy-out occurs in 2018 spend will be £75k.
2017/0028	01 May 2017	Kelly Snares	IT Software	Financial Services	Nick Kennett	John O'Nell	£ 700,000	OPEN	Salesforce	PCR - >£164.5k	Continuation of POL CRM system. 1 year award. Awaiting strategy.	Non-compliant extension in place	CRM Platform to be re-tendered as it has previously been purchased non-compliantly. Awaiting strategy and confirmation of requirements from IT before Procurement approach can be agreed. Renewal due in April 2018.
2017/0036	30 October 2017	Antony Ray	Professional Services	Financial Services	Nick Kennett	Nick Kennett	£ 450,000	OPEN	McKinsey	PCR - >£164.5k	Direct award with no contract or CAF. Steps are being taken to rectify this but work already completed.	Contract and CAF being raised by business retrospectively	Contract and CAF being raised by business retrospectively
2017/0038	01 January 2018	William Porter	Property	Property	Alisdair Cameron	Steve Norris	£ 1,000,000	OPEN	BNP Paribas	PCR - >£164.5k	Non-compliant but competitive process process for the provision of Estates Management, Rates Management & Treasury Services run in late 2016. Subsequent negotiations have been extended. Contract now finalised.		
2017/0041	10 January 2018	Angela Lamarra	Travel	Travel	Alisdair Cameron	Barbara Brannon	£ 4,000,000	OPEN	CAPITA	PCR - >£164.5k	POL contract with Capita Travel & Events originally commenced on 01 st April 2014 with an initial term up to 30th September 2015 and an option to extend until 15th November 2015.The Contract was subsequently varied to extend for two years until 30th September 2017. The two year extension was non-compliant under the Public Contracts Regulations 2015 as the extension was not provided for under the original terms of the contract.	The Mitigation plan agreed by the Sourcing Council was the following: extending the Capita contracts expiring on the 30th Sept 2017 for 6 months with commitment to utilise the new CCS framework once available. This was supposed to be be awarded on the 31st October 2017 but CCS decided to cancel this and re-issue a new OJEU. The new Framework will be available in March 2018 therefore our Mitigation Plan has been modified. Current contracts will be extended until 31st March 2018. After March 2018 the contracts will continue on a roll-over	CCS have just communicated that the tender process is now complete and suppliers have been selected. Details of the award will be published via the Official Journal of the European Union in the following weeks. Once the agreement is made available and the effective date is communicated, we will be able to run a Tender as part of the Call Off Process in order to refine our requirements
2017/0042	10 January 2018	Angela Lamarra	Professional Services	HR	Martin Kirke	Sean Leahy	£ 400,000	OPEN	Experian	PCR - >£164.5k	A non-compliant interim solution (6 month contract) was put in place with the supplier Experian following a Mini Tender. The agreement effective date is the 8th Feb 2017. At the end of the initial term (6 months), the agreement continues unless terminated by giving 2 month notice	The 6 month Initial Term with Experian terminated on the 8th Aug 2017, a 2 month roll-over solution is now in place. In the past few months the Business Unit wasn't able to finalize the scope of service because the Government was still in the process of issuing/publishing the new Vetting Regulation for all public companies; - HMRC have now published the new regulation and POL is in consultation with them in order to define what is applicable for our business and	The Internal solution (Identity Assurance platform to be extended) is now being discussed as a possible option rather than tendering the requirement
2017/0043	10 January 2018	Anne Cundy	Goods for Resale	Identity	Martin Edwards	Jonathan P Evans	£ 2,500,000	OPEN	Digidentity B.V	PCR - >£164.5k	Initial contract awarded following a non-compliant tender process (RFI with selected Bidders v full OJEU) to support award to POL under the Government FWA (Cabinet Office) for Identity Assurance for a 21 month period to 30/11/17.) 12 month extension required whilst POL strategy is determined.	Current strategy meetings being undertaken.	Legal risk note from Womble Bond Dickinson November 2017 "a medium risk of breach of procurement law though, absent any notice having been received from other providers in the intervening period, the likelihood of a challenge being brought against the extension and variation is probably low." Current strategy meetings being undertaken. **05/03/18 Confidential: Options may include the forming of a subsidiary company.**
2017/0044	10 January 2018	Shahab Hasan	IT Software	IT	Rob Houghton	Andy Garner	£ 788,000	OPEN	NCR	PCR - >£164.5k	Contract about to expire, contract value to be reached imminently. Need to continue to procure additional SSK units and ongoing support and maintenance services (including for existing units) for up to 6 months whilst we compliantly reprocure via OJEU and successful bidder completes set up	Working with business to understand other compliant routes to source ongoing provision whilst OJEU is carried out and successful supplier can complete set up	
							£ 12,538,000						

POL00401626

APPENDIX B : Procurement Pipeline - High Value Forecast or At Risk of Non Compliance

Date Logged	Procurement Category Manager	Procurement Category	Function	GE Member	SLT Owner	Description of Service	Supplier Name	Contract Expiry Date	*Estimate Value / Income per annum	Description of Issue >£164k	PCR Risk Rating H/M/L	Current Status / Mitigation Actions Taken	Key Decisions Outstanding
10/01/2018	Rhona Mclaren	Marketing	Marketing	Owen Woodley	Louise Fowler	Print Services	HH Global	31st March 2018	£ 4,000,000	Contract due to expire March 2018. A short term non compliant contract extension will be needed to give sufficient time to complete the procurement activity and potential transition time. Plan in place to complete 4 month extension proposed to cover this period of risk.	L	Tender is now live with responses and supplier pitches taking place in March.	Formal agreement for a non compliant contract extension and support for agreed timetable across POL.
10/01/2018	Rhona Mclaren	Marketing	Marketing	Owen Woodley	Louise Fowler	Media Buying	Carat	30th April 2018	£ 25,000,000	Contract due to expire Nov 2018. CCS have not completed the retender of the framework, this is now due to be awarded May 2018 with go live Nov 2018. Marketing have agreed to await the outcome of the CCS framework in May and review their supplier options at that point.	L	Extension of current contract to Nov 2018 to maintain contract compliance is now underway.	Formal agreement for a compliant contract extension. **Risk of SME resource shortage due to senior leadership changes**
10/01/2018	Rhona Mclaren	Marketing	Marketing	Owen Woodley	Louise Fowler	Data Services	RAPP	31st March 2018	£ 1,300,000	Contract has been extended non-compliantly for several years and has been under review between IT and Marketing for almost 12 months as part of a possible CRM / Data strategy. Decision made to proceed on basis of current scope for IT requirements but marketing seeking to change their aspect of the commercial model. GDPR concerns which are under investigation.	M	The current plan is to extend non compliantly to 31st March 2019 (12 months) while the business – marketing teams stated preference is OJEU for full service, IT have yet to confirm that this approach is acceptable. An OJEU process is likely to take up to 12 months with a transition of live service thereafter.	Formal agreement for a non compliant contract extension and support for agreed timetable across POL. **Confirmation that the OJEU route to market is acceptable to both IT and marketing**
10/01/2018	Rhona Mclaren	Marketing	Marketing	Owen Woodley	Louise Fowler	Creative	Mullen Lowe	31st March 2018	£ 1,800,000	Contract due to expire March 2018. Reprocurement exercise is now underway using the CCS framework. A non compliant extension is required until Oct 2018 to cover period of delay.	M	Extension of current contract until Oct 2018 to allow time for reprocurement	Formal agreement for a non compliant contract extension and support for agreed timetable across POL.
01/03/2018	Rhona Mclaren	Marketing	Marketing	Owen Woodley	Louise Fowler	Market data	Media Lab	14th April 2018	£ 175,000	Contract was awarded under an OJEU but the ability to extend compliantly has now ended. A 1 year non compliant extension is now required while marketing review their strategy and GDPR implications of utilising cold data	M	Non compliant 1 year contract extension with 3 months termination for convenience rights in the contract	Formal agreement to a non compliant contract extension
01/03/2018	Rhona Mclaren	Marketing	Marketing	Owen Woodley	Louise Fowler	Market data	CACI	14th April 2018	£ 110,000	Contract was awarded under an OJEU but the ability to extend compliantly has now ended. A 1 year non compliant extension is now required while marketing review their strategy and GDPR implications of data analysis services.	L	Non compliant 1 year contract extension with 3 months termination for convenience rights in the contract	Formal agreement to a non compliant contract extension
10/01/2018	Angela Lamarra	Services	Human Resources	Martin Kirke	Sean Leahy	Employee Vetting Services	Experian	8th August 2017*	£ 400,000	Initial 6 month contract is now rolling on a monthly basis while POL agrees sourcing strategy for delivery of service.	M	Stalled: Pending identity strategy and whether POL will insource the service/provide through a subsidiary. Currently at risk of challenge with value increasing monthly.	Timetable.
10/01/2018	Anne Cundy	Retail	Retail	Debbie Smith	Keith Maple	DMB Retail Audit - stationery mailing products	OCS Group UK Ltd (MORECAMBE)	31st May 2018	£ 850,000	Contract will exceed the posted OJEU value during the original procurement to the value of est. £850k (20% over forecast).	L	Service will transfer to WHS - no action required. One final audit due this month Jan then services being undertaken by WHS under the new Retail Arrangement.	None. Termination notice will be issued post audit. Reported January 2018
10/01/2018	Anne Cundy	Retail	Retail	Debbie Smith	Nick Spicer	Visa & Master Card	Global Payments	8th May 2019	£ 10,000,000	The Original Global Pay Agreement was compliantly awarded under a public PCR procedure, covering a period of 5 years to 08/05/17. With TWO x 12 month options to extend. It has become non compliant only because it is now over the forecast value during the OJEU process.	L	A 3rd extension is also being sought for 19/20 pending planned technology roadmap/upgrades.This extension would be legally non-compliant but allow the tender process to be completed at low risk [CMS McKenna]. The intention is to tender under CCS Framework agreement [Merchant Acquiring] effective for award by 09/05/20. The extension period could be reduced in part if the incumbent retains the business. If technology upgrades are completed by FJ, switching provider becomes faster and safer.	Legal advice is that this is low risk. **Detailed paper going to May Board.**
10/01/2018	Kelly Ross	Software	IT/FS	Owen Woodley / Rob Houghton	Jeff Smyth	Salesforce CRM Software	Salesforce	01/05/2018	£ 1,000,000	Contract is currently non-compliant and rolling annually	M	Separate risk paper going to RCC. Compliant route to resolve has been identified and legal advice obtained to that effect. Now subject to supplier negotiations.	None, other than review and approval of commercial outcome. **Risk of increased cost.**
02/03/2018	Angela Lamarra	Comms &PR	Comms	Mark Davies	Paul Swanton	Events Management	Live Union	31/03/2018	£ 500,000	Contract due to expire March 2018.	L	Currently reviewing the possibility to use CCS Frameworks (1. Communication services - Events. Framework has been awarded and it's available; 2. CCS Framework for Venue (Framework hasn't been officially awarded yet)	Agree strategy with Communications team
02/03/2018	Angela Lamarra	Comms &PR	Comms	Mark Davies	Paul Swanton	Internal Comms	AB Publishing; W&J Linney	31/03/2018	£ 300,000	Contract due to expire March 2018. A short term non compliant contract extension will be needed to give sufficient time to complete the procurement activity and potential transition time.	L	A suitable CCS Framework for Communication Services has been identified.	BU and Procurement working on tender Document
05/03/2018	Anne Cundy	Retail	Retail	Debbie Smith	Andrew Goddard	ATM maintenance	BOI	22/03/2022	**£ 30,000,000**	Whilst the BOI POL/ATM Agreement runs to 31/03/22, individual ATMs, start to fall out of contract after October 2018, on a gradual basis up to 31/03/22, however the POL/BOI ATM Board have agreed any such ATM's to continue to be in operation until 31st March 2022. The original contract (2005) and the contract variation (2014) were in place prior to the 2016 Concession Contract Regulations (CCR2016) came into force, therefore the risk of a successful challenge under the CCR 2016 is considered to be low given that the Regulations did not apply to this contract.	L	The ATM team are looking at POLs ATM strategy post 2022 (liaising with the wider supply chain cash strategy) which is being presented to the Board in May. Depending on the outcome of the strategy will impact on the Procurement Risk assessment i.e exit/reduce ATM estate v grow ATM estate. A further update will given at the May R&CC meeting.	ATM strategy - **Detailed paper going to May Board.**
									£ 75,435,000				

Note re *: Where compliant contracts are expiring the financial risk commences from the start of the new non-compliant term.
Where contracts are *already* non-compliant, an additional extension will also include the financial risk of the prior value committed.

POL00401626

Treasury Risk Management Framework, Policies and Authorities

Author: Mark Dixon Sponsor: Alisdair Cameron Meeting date: 13 March 2018

Executive Summary

Context

The Audit, Risk and Compliance Committee approved the most recent Treasury Risk Management Framework, Policies and Authorities (the "Treasury Policy") at its meeting in November 2016.

Our control framework requires an annual review and update of this document.

This paper provides an update as at March 2018 (the "March 2018 Treasury Policy Update").

Question addressed in this report

1. What changes have been made to the Treasury Policy?

Conclusion

We believe that the Treasury Framework, Policies and Authorities set out in the Appendix to this report are appropriate for an organisation of POL's size and complexity.

Input Sought

The RCC is asked to note the Treasury Risk Management Framework, Policies and Authorities set out in this paper for submission to the ARC Committee on 27 March 2018.

POL00401626

The Report

What changes have been made to the Treasury Policy?

1. The full Treasury Risk Management Framework, Policies and Authorities are set out in a Schedule to this paper.

2. The main changes proposed in March 2018 from November 2016 are listed below.

3. In order to conservatively manage its short-term liquidity the Group targets an investment reserve balance of £5m. At critical periods this may be varied. We have formalised delegated authorities around changes to this reserve such that the Head of Treasury, Tax and Insurance ("HoTTI") can approve a temporary change to the reserve so that the target is in the range nil to £20m and for a maximum of two weeks. Any changes outside this range or for a longer period will require approval by the CFOO. All changes will be reported to the Treasury Committee in the monthly Treasury Report. (See **3 Short-term Cash and Liquidity Management**.)

4. Drawdowns under existing facilities require approvals each time a drawdown is made. The delegated authorities vary according to the drawdown period. The delegated authorities for drawing under Other External Borrowings (up to £50m) now include an authority for the HoTTI to approve drawdowns up to 1 week. This has been added in order to ensure that drawings under the proposed £50m RCF (if implemented) can be made quickly and efficiently within deadlines. (See **3 Short-term Cash and Liquidity Management**.)

5. From time to time POMS may have surplus cash balances that it wishes to deposit with POL or may have short-term funding needs which can be satisfied by POL. The policy update delegates authority to the CFOO to agree and execute such loans on behalf of POL. (See **3 Short-term Cash and Liquidity Management**.)

6. Counterparty credit exposures primarily arise as a result of the investment of surplus cash. The March 2018 Treasury Policy Update recognises that other potential credit exposures may arise from the mark-to-market of our derivative activity and undrawn committed facilities provided by banks. The exposure on derivatives is currently minimal, as activity is limited to short-dated FX swaps and outrights, but potentially increases if we execute the POca interest rate swap. The exposure under undrawn committed facilities is currently limited to the undrawn portion of the £400 million of facilities provided by RBS in support of our participation in the Note Circulation Scheme. The exposure will increase if we enter into the £50 million Revolving Credit Facility which is likely to remain

POL00401626

undrawn. The Treasury Policy sets out limits for these exposures. (See **5 Counterparty Credit Risk Management**.)

7. In connection with the investment of surplus cash balances the January 2018 Treasury Policy Update now sets out credit rating bands within which credit limits will be allocated. This allows limits to automatically adjust with changes in ratings. This provides broadly the same limits for counterparty banks as per November 2016 with the exception of RBS, which, as a BBB+, is now restricted to a limit of £30 million (previously £60 million). In addition we have also formalised the procedures for the reporting of limit breaches. (See **6 Investment Risk Management**.)

8. The section on Guarantees/Group Support has been rewritten to distinguish: POL support for POMS; bank guarantees provided to support financing and commercial activity; and, Government support for the Group. The Treasury Policy ensures that any guarantee arrangement entered into in connection with a financing arrangement would require Board approval but that where guarantees are to support commercial activity delegated authority rests with the CFOO. (See **13 Guarantees / Group Support**.)

9. The Treasury Policy sets out the new reporting obligations from January 2018 arising under the European Markets Infrastructure ("EMIR") as a result of changes to MiFID II. (See **14 Regulatory Obligations**.)

10. In order to execute the POca interest rate swaps and to improve the control environment around its other derivative activity (FX swaps and outrights) the Group entered into ISDA Master Agreements in December 2017 with three relationship banks (RBS, Lloyds and Barclays) having received approval from the ARC. The ISDAs also facilitate compliance with new reporting obligations arising under EMIR. The Treasury Policy states that POL will only enter into derivative transactions with a counterparty with which it has executed an ISDA and will ensure that ISDAs are broadly standard across all counterparties. The March 2018 Treasury Policy Update provides a new delegated authority to the CFOO to approve and execute new ISDA agreements on behalf of POL. (See **15 ISDA Master Agreements**.)

11. Minor changes have been made to the governance and reporting section to reflect that the Treasury Committee is now part of the monthly Operations Board. (See **16 Treasury Governance and Reporting**.)

POL00401626

Schedule – Treasury Risk Management Framework, Policies and Authorities - March 2018

POL00401626

POST OFFICE LIMITED AND SUBSIDIARIES (THE "GROUP")

TREASURY RISK MANAGEMENT FRAMEWORK, POLICIES AND AUTHORITIES - MARCH 2018

		Page
I - Introduction		
1	**Background**	**2**
2	**Policy Overview**	**3**
II - Detailed Policies for the Management of Financial and Other Risks Relating to Treasury Activity		
Key Policies		
3	**Short-Term Cash and Liquidity Management**	**5**
4	**Medium and Long-term Funding Management**	**8**
5	**Counterparty Credit Risk Management**	**10**
6	**Investment Risk Management**	**12**
7	**Foreign Exchange Exposure Management**	**16**
8	**Interest Rate Exposure Management**	**18**
9	**Bank Relationship Management**	**19**
10	**Commodity Price Exposure Management**	**20**
Other Guidelines		
11	**Operational Banking**	**21**
12	**Payments**	**23**
13	**Guarantees and Indemnities / Group Support**	**25**
14	**Regulatory Obligations**	**26**
15	**ISDA Agreements**	**27**
III - Governance and Reporting		
16	**Treasury Governance and Reporting**	**28**
APPENDICES		
A	Summary of Counterparty Relationships, Services and Exposures	**30**
B	CHAPS Banks	**31**
C	Delegated Authorities for Authorisation Panels	**32**
D	Delegated Authorities for Drawdowns under Credit Facilities	**33**
E	Individual Write-off Authority Levels	**34**
F	Summary of Delegated Authorities	**35**

POL00401626

I - Introduction

1. Background

1.1. This document sets out the risk management framework, policies and authorities adopted by Post Office Limited ("POL") and its subsidiaries (together the "Group") in relation to its treasury activities and is an update of the paper approved by the ARC Committee in November 2016. It is recognised that Post Office Management Services Limited ("POMS") is subject to regulatory and fiduciary obligations which require derogation from some of the following policies. POMS will determine where there is a conflict between its obligations and these policies and amendments will be agreed and documented. A service agreement will set out the treasury activities which will be carried out on behalf of POMS.

1.2 The treasury risk management framework has been designed to:

- protect financial asset values;
- minimise income statement volatility;
- ensure financial obligations are met as they fall due;
- secure long-term funding to meet overall business objectives and shareholder return requirements;
- ensure regulatory obligations are met.

1.3 The key treasury risks are:

- *Short-term cash and liquidity risk* – the Group does not have sufficient short-term liquidity to meet payment obligations;
- *Medium and long-term funding risk* – the Group does not have sufficient committed long-term funding in place to meet business objectives and going concern obligations;
- *Counterparty credit risk* – a financial institution counterparty cannot meet its obligations to the Group. Such obligations may arise from: investing the Group's surplus cash balances (see investment risk, below); entering into derivatives transactions; entering into committed facility arrangements; and certain other commercial arrangements with clients.
- *Investment risk* – arising from investing the Group's surplus cash balances;
- *Foreign exchange risk* - arising from holding currency note inventory in branches and cash centres to meet on-demand requirements from customers;
- *Interest rate risk* – arising from the impact of changes in interest rates on the cost of funding, the returns earned on the investment of surplus cash, and the returns earned on the POca cash balances;
- *Bank relationship risk* – the Group does not manage its bank relationships in an appropriate manner;
- *Commodity price risk* – arising from the impact of changes in commodity prices on operational costs;
- *Settlement risk* – the risk that operational and business payments are not executed in accordance with agreed policies and procedures, are not settled in a timely manner or are exposed to the possibility of fraud;
- *Regulatory risk* – arising from POL failing to meet its regulatory obligations around its treasury activities;
- Proper recording of treasury transactions, including the reconciliation of bank statement balances to ledger balances in a timely manner;
- Loss or theft of cash.

POL00401626

2. Policy Overview

2.1 The Board is averse to treasury risk. The risk management framework and policies have been designed to reduce risk and concentrate on five principal areas to achieve this:

- **Market Risk**: to minimise any potential loss due to a change in market factors (e.g. interest rates, exchange rates or commodity prices);
- **Credit Risk**: to minimise any potential loss due to a change in the credit-worthiness of a counterparty;
- **Business Risk**: to minimise any potential loss due to economic factors;
- **Operational Risk**: to minimise any potential loss due to system, people, legal and other external events;
- **Regulatory Risk**: to minimise the risk that POL fails to meet its regulatory obligations around treasury activities.

2.2 Day-to-day operation of treasury policy and the activities of the Treasury function are the responsibility of the Head of Treasury, Tax and Insurance (the "HoTTI"), who reports to the POL Finance Director (the "POL FD"). Treasury activities are reported on a monthly basis to the Treasury Committee, which is part of the Operations Board, for review and oversight. The composition and responsibilities of the Treasury Committee are set out in section 16.1.

2.3 Any proposed amendments to, or derogations from, policy will be considered in the Treasury Committee and approved by the Audit, Risk and Compliance ("ARC") Committee or, if appropriate, by the Board.

2.4 Treasury is responsible for the following activities. These activities will only be undertaken by Treasury unless an alternative arrangement has been formally approved by the ARC Committee or the Board:

- management of bank account structures to provide automated concentration of cash and/or offset of balances;
- management of the Group's short-term cash flow forecasting process;
- arrangement and management of short-term committed funding;
- monitoring the debt capital structure to ensure that the Group has sufficient funding to support medium and long-term forecast requirements and to minimise refinancing risks;
- management of short, medium and long-term borrowing requirements;
- providing input to and critical review of the Group's medium and long-term cash flow forecasting process;
- fulfilment of obligations under the rules of the Bank of England's Note Circulation Scheme;
- setting counterparty limits for the financial institutions with which Group does business;
- short-term liquidity management and the investment of surplus cash balances;
- executing FX hedges in accordance with the instructions of the FX Committee, using approved instruments to hedge out to a maximum of 3 months;
- monitoring net interest rate exposure;
- managing bank relationships, in relation to corporate treasury activity;
- monitoring exposure to commodity price volatility;
- executing payments and administrating payments systems;
- acting as a centre of excellence in providing guidance and advice on all operational banking, payments and other treasury-related matters;
- regularly reviewing mandates;
- ensuring adherence to internal controls around internet banking systems and security;
- ensuring adherence to treasury-related regulatory obligations.

2.5 Cash forecasting must be completed in accordance with Treasury's instructions and deadlines and will support short-term, medium-term and long-term forecasting with the current Strategic Plan of the Board (currently the 5-year plan to 2020/21). Any material variances are to be escalated to the POL FD.

2.6 Compliance with the treasury policies set out in this document is mandatory, subject to the derogations provided to POMS noted in 1.1 above.

POL00401626

2.7 **Delegated Authorities**

- *Approve treasury risk management framework, policies and authorities* - **ARC**
- *Approve amendments to or derogations from Treasury Risk Management Framework, Policies and Authorities* - **ARC**

POL00401626

II Detailed Policies for the Management of Financial and Other Risks Relating to Treasury Activity

Key Policies

3. Short-Term Cash and Liquidity Management

Business Context

3.1 On a daily basis the Group has significant operating, investing and financing cash flows across its bank accounts, arising in relation to client-related activity across our counters, and as well as its own business-related activity. Client-related inflows and outflows are material and volatile with approx. £65 billion of flows each year. Flows can vary significantly depending on the day of the week and time of year and can also be materially impacted by other factors, out of the Group's control, such as the weather. Even with appropriate long-term committed funding in place there is therefore a short-term liquidity risk that the Group does not have resources available to meet its day-to-day payment obligations as they fall due.

Risk Management Objectives

3.2 The objective of the short-term cash and liquidity management policy is to ensure that the Group has appropriate liquidity in the right place at the right time to meet its payment obligations as they fall due.

Main Policy Statement

3.3 Through a combination of efficient bank account structures and accurate short-term cash flow forecasting, together with access to appropriate levels of committed short-term liquidity, Treasury will ensure that the Group can meet its obligations as they fall due.

Supporting Policy Guidelines

3.4 Bank Account Structures

3.4.1 Where possible, Treasury will manage cash balances within pooling arrangements which enable cash to be efficiently and effectively concentrated and debit and credit balances to be offset. Business units are not permitted to operate bank accounts that are outside these pooling arrangements unless authorised in writing by Treasury.

3.4.2 **Delegated Authorities**

- *Approve addition of bank account to existing pooling arrangement* - IRRELEVANT
- *Approve removal of bank account from existing pooling arrangement* - IRRELEVANT
- *Approve creation of new pooling arrangement* - IRRELEVANT

3.5 Short-term Cash Flow Forecasting

3.5.1 Short-term cash flow forecasting is an essential tool for the Group and enables it to have confidence that its committed facilities are sufficient to provide the liquidity needed to meet its day-to-day payment obligations.

3.5.2 Treasury will prepare a short-term, daily rolling forecast of the utilisation of the BEIS Facility and the NRF. The forecast, by day, covers a period of up to two accounting periods. Treasury will issue:

- daily reporting to the HoTTI analysing variances of same-day and two-day forecasts to actuals;
- a weekly Liquidity Report to the CFOO and POL FD updating the forecast for the following week and providing a variance analysis for last week;
- a monthly Forecast Update to the CFOO and POL FD updating the forecast for the following two periods and providing a variance analysis for the last period.

3.5.3 The forecasts and variances will be reviewed on a daily basis by the IRRELEVANT Monthly

POL00401626

Forecast Updates will be included in the Treasury Report and reviewed by the Treasury Committee. The ARC will be updated by exception.

3.6 Committed Short-term Funding

3.6.1 Treasury's first responsibility is to ensure that sufficient liquidity and facilities are available to the Group to fund its operations. Funding is therefore negotiated and managed centrally and the management of individual cash pools will be dealt with by Treasury.

3.6.2 Short-term liquidity is managed as follows: POL has access to a £950m working capital facility provided by the Department of Business, Energy and Industrial Strategy ("BEIS") (the "BEIS Facility"). The BEIS Facility is available until March 2021. A utilisation request must be provided to BEIS two days before drawdown. Forecasting variances may lead to a shortfall between the amount drawn down and the actual amount required. The strategy to mitigate the risk of a shortfall between forecast and actual funding requirements is to hold IRRELEVANT Any changes to the IRRELEVANT will be reported to the Treasury Committee in the monthly Treasury Report. Treasury can also use IRRELEVANT IRRELEVANT and/or use the NRF (see 3.6.3 below).

3.6.3 In addition, POL is a member of the Bank of England's Note Circulation Scheme (the "NCS"). The scheme allows POL to declare and sell eligible notes to the Bank of England (the "Bank") overnight with a commitment to buy those notes back from the Bank first thing the next morning. This reduces the Group's overnight funding requirement. The NCS rules require the provision of collateral to the Bank. Collateral is currently provided on behalf of POL under a Facilities Agreement entered into by POL with IRRELEVANT IRRELEVANT[1] under which the bank makes available: a £400m intra-day facility; a £350m overnight NRF facility (for the purposes of providing overnight collateral to the Bank); and, a IRRELEVANT collateral facility, used in connection with our crime insurance.

3.6.4 The NCS rules also require that POL has a crime insurance in place that is compliant with BoE requirements.

3.6.5 The amount available to be used under the NRF over the course of the Bank's financial year (to October) is constrained by a cap (the "Cap") that POL generates, mainly as a function of outward rems processed from its NCS cash centres. Treasury will monitor utilisation of the NRF against the Cap to ensure that no more than the Cap generated is used over the course of the year and that financial penalties are therefore avoided. Cap generation and NRF utilisation will be reported to the Treasury Committee on a monthly basis via the Treasury Report.

3.6.6 Any new borrowings require Board approval. See 4 Medium and Long-term Funding Requirement.

3.6.7 The delegated authorities for drawdowns are set out in Appendix D and in 3.6.8 below.

3.6.8 **Delegated Authorities**

- *Approve change to Investment Reserve (in the range nil to £20m / for up to 2 weeks)* – IRRELEVANT
- *Approve change to Investment Reserve (up to £50m / for more 2 weeks)* – IRRELEVANT
- *Propose drawdown - under existing credit facilities* - **Dealing Panel**
- *Approve drawdown - under BEIS Facility* - **Various (see Appendix D)**
- *Approve drawdown - under other external borrowings (up to £50m)* - **Various (see Appendix D)**

[1] *These facilities are currently provided by* IRRELEVANT

POL00401626

3.7 Short-term Cash & Liquidity Arrangements with POMS

3.7.1 From time to time POMS may have surplus cash balances which it wishes to deposit with POL or it may have short-term funding needs which can be satisfied by POL.

3.7.2 POL is permitted to take loans from or make loans to POL.

3.7.3 All loans will be documented.

3.7.4 Margins on loans will be agreed between POL and POMS and will be on an arm's length basis.

3.7.5 For short-term loans and deposits up to 3 months, for amounts up to £50m, authority to agree margins and execute documentation, on behalf of POL only, is delegated to the CFOO.

3.7.6 For the avoidance of doubt, any loans to or from POMS will require the approval of the POMS Board.

3.7.7 At 2018 POMS is the only wholly-owned subsidiary of POL. In the event that new subsidiaries are introduced into the Group structure then, provided such subsidiaries are wholly-owned, then 3.7 will also be applicable for loans to/from those subsidiaries.

3.7.8 **Delegated Authorities**

- *Approve margin on intra-group loans to/from POMS on behalf of POL (up to £50m / up to 3 months)* - IRRELEVANT
- *Execute documentation for intra-group loans to/from POMS on behalf of POL (up to £50m and up to 3 months)* - IRRELEVANT
- *Execute documentation for intra-group loans to/from POMS on behalf of POL (over £50m or over 3 months)* - IRRELEVANT

POL00401626

4. Medium and Long-term Funding Management

Business Context

4.1 The Group develops its strategic objectives and prepares long-term business plans to meet those objectives. Such objectives will include the continued participation in the Bank of England's Note Circulation Scheme (the NCS") in order to ensure an adequate supply of notes for the branch network. The Group must ensure that it has sufficient committed long-term funding in place to meet these plans. There is a risk that the funding in place is not sufficient to achieve business objectives or to adequately withstand unforeseen changes to plans.

4.2 In order to present its financial statements on a going concern basis the Group must demonstrate, on an annual basis at each balance sheet date, that it has sufficient committed funding in place.

4.3 The Group's existing funding arrangements, including the facilities made available to enable participation in the NCS, are set out in 3 Short-term Cash and Liquidity Management.

Risk Management Objective

4.4 The objective of the medium and long-term funding management policy is to ensure that the Group has sufficient committed long-term funding in place to meet business objectives and going concern obligations.

Main Policy Statement

4.5 Through a combination of accurate medium and long-term cash flow forecasts and the monitoring of headroom, together with access to appropriate levels of long-term committed funding, the Group will ensure it has sufficient funding in place to meet business objectives and going concern obligations.

Supporting Policy Guidelines

4.6 Medium and Long-term Cash Flow Forecasting

4.6.1 Medium and long-term cash flow forecasting is an essential tool for the Group and enables it to have confidence that its committed facilities are sufficient to provide the liquidity needed to meet its business objectives and loan repayments.

4.6.2 Treasury will provide input to Group's medium and long-term forecasts, in particular the one-year and five-year strategic forecasts and in accordance with the current Board Strategy.

4.7 Funding Strategy

4.7.1 The CFOO and the POL FD will recommend to the Board the appropriate debt capital structure for the Group. The Group will have a debt maturity profile and funding structure adequate to meet its:

- business objectives, including growth strategy;
- going concern obligations.

4.7.2 The debt capital structure and maturity profile will be monitored by the CFOO and POL FD, and reviewed by the Treasury Committee to ensure that the Group has appropriate funding available to support its long-term plans. Where possible, the Group seeks to minimise its refinancing risk by adopting a range of maturities for its debt facilities. Maturity of existing facilities will be monitored to ensure that negotiations commence in a timely manner to extend or replace them.

4.8 Headroom

4.8.1 *Facility Headroom* - Facility Headroom is defined as the headroom available under the BEIS Facility. The Group will aim to maintain Facility Headroom of at least IRRELEVANT (the "Facility Headroom Buffer"). Any reduction in Facility Headroom Buffer will require Board

POL00401626

approval. It will be monitored and reported in the monthly Treasury Report and the monthly Performance Report to the Board.

4.8.2 *Security Headroom* - Security Headroom is defined in the BEIS Facility. Treasury will also monitor the asset security headroom of the BEIS Facility. It will be reported in the monthly Treasury Report and the monthly Performance Report to the Board.

4.8.3 Treasury will use a combination of the short-term forecasts outlined in 3.5 above and the medium and long-term forecasts to monitor headroom.

4.8.4 **Delegated Authorities**

- Approve amendment to Facility Headroom Buffer - **Board**

4.9 Borrowing Policy

4.9.1 Borrowing is only permitted in sterling unless approved by the ARC.

4.9.2 Borrowing should only be incurred in accordance with the restrictions under clause 10 of POL's Articles of Association and may require shareholder approval.

4.9.3 Additional borrowing is only permitted in accordance with the constraints imposed under the BEIS Facility which limits borrowings as follows:

- the existing £950m BEIS Facility itself, or any refinancing thereof;
- up to £50m of additional finance or capital leases;
- up to £50m additional other borrowings.

Together with the facilities in place to support POL's participation in the NCS, namely:

- the £400m intra-day facility;
- the £350m overnight NRF facility.

4.9.4 **Delegated Authorities**

- Approve new medium and long-term funding - **Board**

POL00401626

5. Counterparty Credit Risk Management

Business Context

5.1 Counterparty credit risk arises where a financial institution counterparty cannot meet its obligations to the Group. Due to the nature of POL's business activities such exposures arise both as part of POL's normal corporate treasury activities and its other client-related activities. Exposures arise primarily as follows:

Corporate Treasury Activity

5.1.1 *Investment of Surplus Cash Balances* - Total exposure of approximately £5m but may increase up to £50m when the investment reserve is increased during holiday periods. (See 6. Investment Risk Management.)

5.1.2 *Mark-to-Market of Derivatives* - Derivative contracts (including FX swaps, FX forwards and interest rate swaps) where the mark-to-market position has moved in favour of POL such that the counterparty owes money to POL under the contract. Exposure arises due to changes in market rates. Because FX maturities are managed within one month total exposure is currently minimal.

5.1.3 *Committed Facilities* - Commitments made by a bank or other funding provider under facilities that remain undrawn by POL. Such facilities currently comprise: the BEIS Facility; and, the £400m intra-day facility / £350m overnight NRF facility provided by Royal Bank of Scotland plc. The exposure relating to the BEIS Facility is considered to be nil but there is an exposure on IRRELEVANT that fluctuates during the day depending on how much is utilised under the facilities. If the £50m RCF is arranged with IRRELEVANT an exposure of £50m will exist in connection with the facility, while it is undrawn, split evenly between the three banks. Total exposure may be up to **£450m**.

Other Client-Related Activity

5.1.4 *Banking Framework* - Over-the-counter banking transaction services with retail and business customers. Transactions are cleared through the LINK system with daily settlement to POL received from IRRELEVANT this creates a daily net direct exposure to IRRELEVANT of up to **£30m**. In addition, POL would also be exposed to the failure of an individual client bank to meet its obligations under the LINK system.

5.1.5 *Debit and Credit Card Processing* - When a customer makes a payment to POL over-the-counter using either a debit card or a credit card settlement is received by POL via GPUK LLP ("GlobalPay") on the next business day. This creates a one-day credit exposure against GlobalPay. Total exposure fluctuates but is approximately **£75m**.

5.1.6 *Cheque Clearing* - when a customer makes a payment to POL using a cheque it creates a short-term exposure (up to two days) exposure against the bank on which the cheque is drawn. The total exposure on cheques is approximately **£25m** but this is disaggregated between the banks on which the cheques are drawn.

5.1.7 *Other Client-Related Activity* - Exposures arising from other client-related activities.

- ATM Withdrawals – Exposure to Bank of Ireland linked to cash withdrawals from ATMs. The exposure varies significantly, depending on the time of the year and day of the week, between IRRELEVANT.
- POca Related Flows – Exposure to IRRELEVANT in respect of POca-related flows across POL counters. Flows between 13:00 on the previous day and 13:00 are aggregated and paid same day. The exposure fluctuates significantly depending on the day of the week and time of the year and is impacted by holiday periods and winter fuel payments. It can vary between IRRELEVANT

5.2 This policy focuses on counterparty credit risk arising from POL's corporate treasury activities.

POL00401626

Risk Management Objectives

5.3 The objective of the counterparty credit risk management policy is to minimise the Group's risk of loss in its corporate treasury activities as a result of the failure of a financial institution counterparty.

Main Policy Statement

5.4 Treasury will minimise the risk of loss due to the failure of a financial institution counterparty to meet its obligations by only entering into corporate treasury transactions with highly-rated counterparties and through credit approvals, limits and monitoring procedures.

Supporting Policy Guidelines

5.5 Treasury will only enter into corporate treasury transactions with appropriately approved financial institution counterparties.

5.6 The Group's corporate treasury-related credit risk arises primarily from the investment of surplus cash balances. For the purpose of the investment of surplus cash balances limits are allocated according to rating band rather than specified counterparty. Approved counterparties and sub-limits applicable to deposits (as at March 2018) are set out in 6 Investment Risk Management. Deposit limits will fluctuate with changes to credit ratings.

5.7 When monitoring the credit quality of counterparties Treasury will use short-term and long-term credit ratings from S&P and Fitch. The weaker of the two ratings will be used for decision-making purposes.

5.8 Approved counterparties and credit limits for other transaction types are set out in Appendix A.

5.9 New counterparties and limits may be approved from time to time. Treasury will make a recommendation to the Treasury Committee based on credit ratings for consideration and recommendation to the ARC.

5.10 Exposures to investment counterparties will be monitored separately and reported to the HoTTI on a daily basis and to the Treasury Committee on a monthly basis in the Treasury Report. See 6. Investment Risk Management. Exposures to corporate treasury counterparty activities will be aggregated (including investment counterparties) and reported to the Treasury Committee on a monthly basis together with changes to credit ratings as part of the Treasury Report.

5.11 **Delegated Authorities**

- *Approve new financial institution counterparty* - **ARC**
- *Approve financial institution counterparty limit* - **ARC**
- *Approve temporary increase to financial institution counterparty limit* - IRRELEVANT

5.12 Note on the Implications of Ring-fencing - *Effective 1 January 2019 the major UK banks are required to implement the Government's ring-fencing requirements. In 2018 the Group's facilities with* IRRELEVANT *will be transferred to* IRRELEVANT *as part of the bank's restructuring to meet these requirements. From 2019 these facilities will sit inside the ring-fence. (It should be noted that any complex derivative activity would need to sit outside the ring-fence.) Provided that the S&P and Fitch long-term and short-term credit ratings of* IRRELEVANT *(or any other entity inside or outside the ring-fence) are the same as, or better than,* IRRELEVANT *then all references to* IRRELEVANT *are deemed to apply to* IRRELEVANT *(or those other entities). This approach will also be applied if* IRRELEVANT *plc adopt a similar strategy to ring-fencing in 2018.*

POL00401626

6. Investment Risk Management

Business Context

6.1 Treasury manages short-term liquidity to target a cash buffer of £5m. The buffer is reduced to nil at period ends and can be increased up to £50m around holiday periods when liquidity risks are highest. This creates surplus cash balances that can be invested by Treasury.

Risk Management Objectives

6.2 The three core objectives of the Group's investment risk management policy are: (i) *security* – to preserve the principal sum; (ii) *liquidity* – to ensure investments are accessible when needed; (iii) *yield* – to optimise return on investments.

Main Policy Statement

6.3 The Group's overall consideration when depositing surplus cash balances is the preservation of the principal sum. Surplus cash balances will be invested by Treasury to optimise return, subject to counterparty credit risk considerations. These investments will not be subject to fluctuation in capital values.

Supporting Policy Guidelines

6.4 Permitted Investment Instruments - Treasury are permitted to use the following investment instruments: bank term deposits and deposits on interest-bearing accounts; money market funds ("MMFs"); and, when appropriate, deposits with the Debt Management Office ("DMO").

6.5 Permitted Currencies – Treasury will only invest in £-denominated instruments.

6.6 Approved Bank Counterparties and Deposit Limits - It is the Group's policy to establish and monitor limits for each of the counterparties that it makes investments with.

6.6.1 Limits for term deposits and interest-bearing accounts ("deposit limits") are based on credit rating bands rather than specific counterparties. Counterparties are allocated to bands based on the lower of the S&P and Fitch long-term credit rating as follows:

Credit Rating (1)	Approved Limit (£m)
AAA	120
AA + to AA -	90
A + to A -	60
BBB +	30
BBB and below	0

(1) Based on lower of S&P and Fitch long-term credit rating

6.6.2 Counterparties must have a long-term S&P or Fitch credit rating of at least BBB+ and a short-term S&P or Fitch credit rating of A2/F2.

6.6.3 Counterparties must also be a member of CHAPS (see Appendix C for a list of CHAPS banks).

POL00401626

6.6.4 Approved counterparties and deposit limits based on credit ratings as at January 2018 are:

Financial Institution Counterparty	Credit Rating S&P Long-term	S&P Short-term	S&P Outlook	Fitch Long-term	Fitch Short-term	Fitch Outlook	Approved Deposit Limit (£m)
IRRELEVANT	A	A-1	Stable	A	F1	Positive	80.0
	BBB+	A-2	Stable	BBB+	F2	Stable	30.0
	A	A-1	Positive	A+	F1	Negative	60.0

6.6.5 The deposit limits against individual institutions are expected to change with changes in credit ratings.

6.6.5 *Exception* - IRRELEVANT, as our cash management bank, is allocated an additional limit of £20m to allow for cash held as operational balances on bank accounts from time to time. IRRELEVANT long-term rating of A would imply a deposit limit of £60m. The limit is increased to £80m.

6.7 Other

6.7.1 Unauthorised arbitrage is prohibited i.e. funds should not be specifically drawn down for investment purposes.

6.7.2 Only Treasury is permitted to invest surplus cash balances.

6.7.3 A proposal for the investment of surplus cash balances will be made by the Dealing Panel and approved by either the Treasury Authorisation Panel (see Appendix C – Delegated Authorities for Approval Panels) or in accordance with 6.11 below.

6.7 Deposit Tenor Limits

6.7.1 Deposits will be no longer than one month.

6.8 Money Market Fund Investment Criteria - It is the Group's policy to establish and monitor limits for each of the MMFs that it invests in.

6.8.1 The MMF must be rated by at least one of S&P and Fitch. If rated it must be rated AAAm by S&P and AAAmmf by Fitch.

6.8.2 POL's holding as a proportion of the fund size must not be greater than 10%.

6.8.3 MMFs must have a constant net asset value (CNAV) (also referred to as stable NAV) or a Variable Net Asset value (VNAV) (also referred to as accumulating NAV).

6.8.4 MMFs must have daily liquidity.

6.8.5 Investment is limited to £50m in any one MMF.

6.8.6 Investment in Prime Liquidity Funds is limited to £350m.

6.8.7 Investment in Government Funds is limited to £150m.

6.8.9 Where a single provider has segregated Prime Liquidity Funds and Government Funds, investments can be made in both MMFs subject to the limits above.

POL00401626

6.9 Approved MMFs and limits as at January 2018 are:

Name of Fund	Credit Rating S&P	Credit Rating Fitch	Asset Class	Currency	Name of Return	Fund Size (£m)	Approved Limit (£m)	Approved Limit / Fund Size (%)
IRRELEVANT	AAAm	AAAmmf	Prime	GBP	CNAV	14,400	50.0	0.3%
	AAAm	AAAmmf	Prime	GBP	CNAV		50.0	#DIV/0!
	AAAm	AAAmmf	Prime	GBP	CNAV	14,400	50.0	0.3%
	AAAm	AAAmmf	Prime	GBP	CNAV	36,800	50.0	0.1%
	AAAm	na	Prime	GBP	CNAV	11,800	50.0	0.4%
	AAAm	AAAmmf	Prime	GBP			100.0	
							350.0	
	AAAm	AAAmmf	Government	GBP	CNAV	2,400	50.0	2.1%
	AAAm	AAAmmf	Government	GBP			100.0	
							150.0	

6.10 DMO Investment Criteria – The Group may invest with the DMO on an unlimited basis.

6.11 Operational Approvals - For each individual investment made approval is required as per the table below:

Investment Amount	< £300m	< £100m	< £50m	< £300m	< £50m	< £50m
Term of Investment	< 1 month	< 3 months	< 6 months	< 1 year	< 1 year	< 1 year
Delegated Authority	*1 member from Treasury Authorisation Panel*	*1 member from Treasury Authorisation Panel*	*1 member from Treasury Authorisation Panel*	IRRELEVANT		

The POL FD is also authorised to approve investments with a maturity of up to 5 years for the purpose of providing collateral for the Note Circulation Scheme.

6.12 Monitoring

6.12.1 Exposures to investment counterparties will be monitored separately and reported to the HoTTI on a daily basis and to the Treasury Committee on a monthly basis in the Treasury Report.

6.13 Limit Breaches

6.13.1 When Treasury are aware of a potential breach in advance (for example, when Treasury choose to hold in excess of the authorised limit because no other investments opportunities are available) approval must be obtained from either the CFOO or the POL FD for a temporary increase to the limit. The temporary increase will normally be for no longer than one night.

6.13.2 When Treasury are not aware of the breach in advance (for example, where we receive more cash into our IRRELEVANT accounts than we had forecasted) Treasury will notify the CFOO of the breach immediately on becoming aware of it but in any event no later than close of business on the day after the breach occurred.

POL00401626

6.13.3 All limit breaches will be reported to the Treasury Committee in the monthly Treasury Report.

6.14 **Delegated Authorities**

- *Approve new investment counterparty - within approved credit rating bands* - IRRELEVANT
- *Approve changes to credit rating bands for deposit limits* - **ARC**
- *Approve temporary increase to investment counterparty deposit limit* - IRRELEVANT
- *Approve new permitted investment instrument* - IRRELEVANT
- *Propose investment of surplus cash balances* - **Dealing Panel**
- *Approve investment of surplus cash balances* - **Various (see 6.11)**

POL00401626

7 Foreign Exchange Exposure Management

Business Context

7.1 Foreign exchange risk principally arises from holding foreign currency note inventory in branches and cash centres to meet "on demand" requirements from customers. All currencies are purchased from FRES. The exchange risk arises from the time of purchase from FRES to the sale of currency to the customer. The size of balances on hand is determined by demand. POL holds note inventory balances in approximately 70 currencies. On average, currency holdings are c. £60m but can peak at over £100m during holiday periods.

Risk Management Objectives

7.2 The objective of the foreign exchange exposure management policy is to minimise the impact on the Group's income statement of foreign currency exposures arising from its day-to-day operations.

Main Policy Statement

7.3 Through a combination of periodic monitoring of foreign exchange exposures and entering into hedges within approved hedging bands the Group will ensure its exposure to fluctuations in exchange rates is minimised.

Supporting Policy Guidelines

7.4 The Head of Travel Money analyses the report of foreign currency note holdings in the network which is prepared by Supply Chain and the daily reports of foreign currency holdings provided by Treasury.

7.5 A monthly meeting of the FX Committee is held, attended by: the Managing Director Post Office Money; the Finance Director Financial Services and Telecoms; and the Head of Travel. The meeting is held to confirm the value of hedges and timescales of hedges in accordance with the FX risk management policy outlined below.

7.6 Detailed foreign exchange risk management policy statements

7.6.1 EUR and USD holdings will be hedged 100%; currencies with exposures over £1.5m will be hedged 90% to 100%; other currencies with exposures over £1 million will be hedged 70%.

7.6.2 At least 80% and no more than 120% of qualifying exposures will be hedged based on the average of (1) the previous period's actual holdings and (2) the forecast for one month forward.

7.6.3 Hedges will be closed out and reset to periods between two weeks and five weeks. Longer-dated hedges will be set to mature at a monthend and will be revalued at each intervening month end based upon the mark-to-market valuation provided by the hedging bank.

7.6.4 Hedging will be conducted with counterparties approved by the Treasury Committee (see 5 Counterparty Credit Risk Management).

7.6.5 Trades will be executed at a pre-arranged margin with all counterparties.

7.6.6 The maturity of financial instruments used to hedge foreign exchange exposures will normally be about a month but can be no longer than three months.

7.6.7 Permitted Instruments - Foreign currency exposures can only be hedged using foreign currency outright forwards or swaps.

7.6.8 FX hedging instruments can only be used to hedge exposures generated by holding currencies to meet on-demand transactions by customers.

POL00401626

7.7 Latest currency holdings and hedges will be reviewed at the end of each period immediately before the maturity of the monthly hedges by Financial Director Financial Services and Telecoms and the Head of POL Travel.

7.8 On a monthly basis the Finance Director Financial Services and Telecoms will report to the Treasury Committee on the gain or loss on foreign currency holdings.

7.9 Any proposed changes to the policies above will be presented to the ARC Committee for approval.

7.10 **Delegated Authorities**

- *Execute FX hedge trades, within policy, in accordance with instructions issued by FX Committee* - **Treasury**
- *Approve new permitted FX hedging instrument* - IRRELEVANT
- *Approve FX hedge trades for exposures not created by currency note inventory holdings – up to £50m* - IRRELEVANT
- *Approve FX hedge trades for exposures not created by currency note inventory holdings – above £50m* - **Board**

POL00401626

8 Interest Rate Exposure Management

Business Context

8.1 The Group is exposed to changes in interest rates via its Libor-linked funding and the returns it earns on cash balances. Increases in interest rates will increase the Group's cost of funding and increase the return it earns on cash, mainly linked to Post Office card account ("POca") balances.

8.2 The Group's funding is via the BEIS Facility maturing in 2021 and the NRF. Interest rates on both facilities are linked to Libor. POL also earns commission (credited to revenue) on the balances of benefit payments held by JP Morgan, the POca cash balances. The commission interest received is also linked to Libor. The interest receivable on the POca cash balances has historically exceeded the interest payable on POL's borrowings and is expected to do so for the foreseeable future, despite the long-term decline of POca cash balances. The interest payable on POL's funding is a natural hedge of the commission interest receivable.

Risk Management Objectives

8.3 The objective of the interest rate risk management policy is to minimise exposures to income statement impacts of changes in interest rates.

Main Policy Statement

8.4 The Group will monitor its exposures to changes in interest rates on a regular basis and recommend hedging strategies, if appropriate.

Supporting Policy Guidelines

8.5 Treasury will obtain forecasts of interest payable / commission receivable and the net interest rate exposure will be monitored by Treasury and, if appropriate, a proposal to hedge the exposure will be put to the Treasury Committee prior to approval by the Board.

8.6 The suitability and effectiveness of the interest rate risk management policy will be reviewed at each Treasury Committee meeting. Any proposed changes will be reported to the ARC Committee for approval and submission to the Board.

8.7 Permitted Instruments - Hedging will be by way of interest rate swaps. Other instruments may be approved by the ARC on a case-by-case basis.

8.8 The Government's Managing Public Money Guidelines allow organisations to consider the use of derivatives but require them to consider their use carefully especially to assess value for money. The Guidelines require POL to consult its sponsoring department / HM Treasury before executing any derivative for the first time.

8.9 **Delegated Authorities**

- *Approve new permitted interest rate hedging instrument* - **ARC**
- *Approve execution of interest rate hedging strategy* - **Board**

POL00401626

9. Bank Relationship Management

Business Context

9.1 Good long-term relationships with banks are crucial to the success of the Group around its corporate treasury activities. The Group requires support from banks across all its treasury activities and this support is particularly important for the provision of: short-term liquidity, including operational overdrafts; credit facilities to enable continued participation in the Note Circulation Scheme; and, FX instruments and other derivatives, requiring credit to be extended.

9.2 Due to the UK-focused nature of the Group, the limited requirement for external funding and a small amount of ancillary treasury business, the Group has historically focussed on building relationships with a small group of UK clearing banks.

Risk Management Objective

9.3 The objective of the bank relationship management policy is to establish, maintain and develop efficient and effective banking relationships with a core group of banks to provide the Group with long-term banking support irrespective of short-term business conditions and financial market turbulence.

Main Policy Statement

9.4 The Group will seek to build long-term relationships with two to three of the UK clearing banks.

Supporting Policy Guidelines

9.5 It is the Group's policy to build long-term relationships with providers of banking services and facilities in order to maximise mutual advantage. In allocating new business opportunities, preference will generally be given to banks where a relationship already exists, but this does not preclude the use of other banks identified by Treasury should it be appropriate. Any new relationships will be reported to the Treasury Committee in the monthly Treasury Report for approval.

9.6 Current counterparty relationships, including banks, are listed in Appendix B.

9.7 Management of the Group's bank relationships is the responsibility of the IRRELEVANT and the IRRELEVANT IRRELEVANT). Bank selection will be determined by a number of factors, including service, price, product range, geographic spread and willingness to provide services. The decision to develop a new relationship will rest with the Treasury Committee.

9.8 From time to time POL may require that banking partners enter into Non-Disclosure Agreements ("NDAs") to protect Group-sensitive information. Approval will be required by the IRRELEVANT

9.9 **Delegated Authorities**

- *Approve entering into relationship with new bank* - **Treasury Committee**
- *Approve entering into relationship with new bank (prior to Treasury Committee approval)* - IRRELEVANT
- *Approve entering into NDA with bank* IRRELEVANT

POL00401626

10 Commodity Price Exposure Management

Business Context

10.1 The Group is exposed to movements in the price of diesel, gas and electricity used throughout the business.

Risk Management Objectives

10.2 The objective of the commodity price exposure management policy is to minimise income statement volatility due to changes in commodity prices.

Main Policy Statement

10.3 Treasury will monitor exposures to these commodities and forecast price movements and may recommend hedging action to the Treasury Committee or directly to the IRRELEVANT to protect the Group from adverse price movements.

Supporting Policy Guidelines

10.4 The IRRELEVANT is authorised to hedge each commodity, where it is believed to be economic to do so, up to a maximum of 3 years based on forecast future usage.

10.5 Permitted Instruments - permitted hedging instruments are spot purchases, currency deposits, forward contracts, call options, matched options (e.g. cylinders) and swaps. Futures will not be used without specific authority of the IRRELEVANT

10.6 The Group will designate commodity cash flow hedges against forecast underlying exposures. Unrealised gains and losses on hedges will be deferred in reserves. This will be recycled to the income statement when the hedge matures to match forecast expenditure.

10.7 The suitability and effectiveness of the commodity price exposure management policy will be reviewed at each Treasury Committee meeting. Any proposed changes will be reported to the ARC Committee for approval and submission to the Board.

10.8 **Delegated Authorities**

- *Execute commodity price hedges within policy* - **Treasury**
- *Approve new commodity price hedge counterparty* - IRRELEVANT
- *Approve execution of commodity price hedge within policy* - IRRELEVANT

POL00401626

Other Guidelines

11. Operational Banking

11.1 Bank Facilities

11.1.1 Treasury is responsible for the negotiation of all operational banking facilities and any changes to existing operational facilities. Such facilities include overdrafts, fx lines, BACS limits, intra-day limits and any similar arrangements. Directorates do not have the authority to negotiate or commit to any new operational banking facilities without prior approval from Treasury and are not authorised to undertake any discussions regarding credit lines.

11.1.2 All changes to existing operational banking facilities or any new operational banking facilities must be agreed by the IRRELEVANT

11.2 Interest and Bank Charges

11.2.1 Bank transaction charges will be negotiated by Treasury to ensure minimum cost to the Group. Charges incurred will be reviewed by Treasury to ensure that the activity levels and unit costs applied by the banks to calculate charges are in accordance with agreed tariffs. Errors are to be notified directly to the bank.

11.3 Bank Accounts

11.3.1 It is the Group's policy to minimise the number of bank accounts it operates. Treasury will conduct a bi-annual audit to ensure it has an accurate record of bank accounts. Accounts not being utilised should be closed. This will be reconciled back to internal and bank records.

11.3.2 All new bank accounts will be approved by the IRRELEVANT

11.3.3 Where possible all accounts should be within a cash pooling arrangement. It is recognised that certain constraints apply to POMS cash, where restrictions may preclude pooling.

11.4 Bank Mandates

11.4.1 It is the Group's policy to standardise bank mandates wherever possible. Treasury will manage and administer all bank mandates centrally. Each bank account must be supported by a written, up-to-date mandate which is checked against a list of those colleagues leaving the business on a monthly basis.

11.4.2 Authority levels relating to internet banking systems will be documented separately.

11.4.3 Sole signatory on a bank account is not permitted except for cheques where one signatory may sign for amounts of up to £50,000.

11.5 Reconciliations

11.5.1 The Financial Accounting & Governance Manager is responsible for bank reconciliations.

11.5.2 The reconciliation process around certain bank accounts has been assigned to Treasury. For those accounts, Treasury will ensure that all bank accounts are reconciled to the underlying accounting records and all reconciling items are identified and cleared as appropriate, in a timely manner.

11.5.3 The IRRELEVANT will ensure that all Treasury-owned reconciliations have been properly carried out and provided to the relevant staff members reporting to the IRRELEVANT in accordance with prescribed deadlines.

POL00401626

11.6 **Delegated Authorities**

- *Approve amendments to existing operational banking facilities -* IRRELEVANT
- *Approve new operational banking facilities -* IRRELEVANT
- *Approve opening of new bank account -* IRRELEVANT
- *Approve closure of bank account -* IRRELEVANT

POL00401626

12 Payments

12.1 Manual Payments

12.1.1 Signing mandates are managed by Treasury and must be in place with a bank for any account on which cheques or similar manual payment instructions (e.g. direct debit mandates) are issued.

12.1.2 Cheques or other manual payment instructions up to £50,000 may be signed by one signatory. Cheques or other manual payment instructions greater than £50,000 must be signed by two signatories.

12.1.3 It is the responsibility of the paying department to ensure that there is adequate segregation of duties with regard to the preparation of manual payment instructions and cheques and that written procedures governing the processing of payments are in place.

12.1.4 Cheque books should be kept in a secure place.

12.1.5 Paying-in books should also be kept in a secure place. To prevent credits being made to unauthorised accounts, only pre-printed paying-in slips should be used when paying in cheques.

12.1.6 **Delegated Authorities**

- *Sign manual payment instruction - < £50k* - **Any 1 member of Banking Authorisation Panel**
- *Sign manual payment instruction - > £50k* - **Any 2 members of Banking Authorisation Panel**

12.2 Computer-Generated Cheque Payments

12.2.1 There should be adequate physical security over the hardware and software used for the preparation of computer-generated cheques. Detailed records should be kept of cheque stationery utilised and any missing cheque numbers investigated. A monetary limit should be set for the maximum value of any computer-generated or machine-signed cheque.

12.3 Manually-Instructed Payments

12.3.1 Where any use is made of electronic payment systems via a bank, staff must ensure that adequate written control procedures exist to ensure that the bank will only respond to verified requests from authorised personnel, these include:

- the use of code words;
- answer-back arrangements with the bank calling back to an authorised signatory (other than an authorised signatory who has signed the request);
- requests by telephone for transfers to be supported by a written request, signed in accordance with the mandate, received by the bank prior to dispatch of funds;
- transfer requests should only be sent on company headed notepaper, or pre-printed forms unique to the Group.

12.3.2 Treasury must approve any proposal to start using an internet banking platform and undertake a detailed security review.

12.3.3 If a bank requests any Group employee to sign an indemnity giving protection to the bank in respect of payment instructions actioned by the bank, then this document must be forwarded to Treasury for review and approval prior to signature.

POL00401626

12.4 Electronic Transfers

12.4.1 Electronic Funds Transfer (BACS/CHAPS/Faster Payments) is the preferred means of payment. Where internet banking systems are used to make such payments, care must be taken to ensure that there is adequate physical security over the system to prevent unauthorised access. The networking of internet banking systems should be approved collectively by the Treasury and IT departments.

12.4.2 It is the responsibility of Treasury to ensure that there is adequate segregation of duties in relation to initiating, authorising and releasing payments.

12.4.3 The authorisation process must be fully documented. Non-compliance with the agreed authorisation procedures will be referred to the CFOO and ARC Committee and is considered a serious breach of control.

12.4.4 BACS limits will be negotiated with the bank by Treasury and will be communicated to the relevant business unit. Any request for an increase to a BACS limit must be made by Treasury.

12.4.5 Any recommendations by a bank providing an internet banking system with regard to the control environment surrounding that system must be adhered to in all respects.

12.4.6 Treasury must approve any proposal to start using internet banking systems or other host-to-host solutions to initiate payments and ensure that a security review has been undertaken if appropriate.

12.4.7 **Delegated Authorities**

- *Release payment from Internet Banking System - < £50k* - **Any 1 Payment Panel (Internet Banking System)**
- *Release payment from Internet Banking System - > £50k* - **Any 2 Payment Panel (Internet Banking System)**
- *Release payment from Treasury Management System / SAP* - **Various (see Appendix C)**

POL00401626

13 Guarantees and Indemnities / Group Support

13.1 POL Support for POMS

13.1.1 POL may be asked to provide a letter of comfort, a letter of awareness or a direct guarantee or indemnity to a third party to support the activity of POMS. Although a guarantee creates a contingent liability on POL it does not increase the overall liabilities of the Group. It is considered reasonable to meet such requests on behalf of a wholly-owned subsidiary such as POMS.

13.1.2 Requests of this type will be reviewed on a case-by-case basis and POL will also consider whether it is more appropriate to issue a letter of comfort or letter of awareness. Generally such a guarantee will not have a cost for POL. The authority to approve and sign a direct guarantee to a commercial third-party for the benefit of POMS is delegated to the CFOO.

13.1.3 For the avoidance of doubt 13.1 does not apply to guarantees provided by POL in favour of POMS in connection with the raising of third-party finance by POMS. All such guarantees must be considered by the Board.

13.1.4 **Delegated Authorities**

- *Approve and execute a direct guarantee or indemnity to a commercial third party for the benefit of POMS* - IRRELEVANT

13.1.5 As of 2018 POMS is the only wholly-owned subsidiary of POL. In the event that new subsidiaries are introduced into the Group structure then, provided such subsidiaries are wholly-owned, then 13.1 will also be applicable for guarantees or indemnities for the benefit of those subsidiaries.

13.2 Bank Guarantees

13.2.1 POL may provide a counter-guarantee to a bank to support a guarantee made by that bank to a third party (a "bank guarantee") on behalf of POL. Such a bank guarantee may be used to support financing provided by a third party or to support a commercial arrangement. Such an arrangement may create a contingent financial exposure for the Group.

13.2.2 *To Support Financing* - Where the bank guarantee is used to support a financing arrangement approval will be by the POL Board.

13.2.3 *To Support Commercial Activity* - Where the bank guarantee is being provided to support commercial activity the authority to approve and sign the guarantee to the bank is delegated to the CFOO.

13.2.4 **Delegated Authorities**

- *Approve bank guarantee to support financing arrangement* - **Board**
- *Approve bank guarantee to support commercial arrangement* - IRRELEVANT
- *Execute counter-guarantee to bank in support of commercial arrangement* - IRRELEVANT

13.3 Government Support for the Group

13.3.1 From time-to-time the Group may be asked to obtain a letter of comfort, a letter of awareness or a guarantee from Government to support its activities. Such arrangements do not create a contingent liability of the Group.

13.3.2 Requests will be considered on a case-by-case basis and will require POL Board approval.

POL00401626

14 Regulatory Obligations

14.2 European Market Infrastructure Regulation ("EMIR")

14.2.1 Effective from January 2018, as a result of the changes introduced by MiFID II, the Group's derivative activity is subject to the requirements of EMIR.

14.2.2 POL is classified as a Non-Financial Counterparty "-" (an "NFC –")

14.2.3 As an NFC – EMIR places certain obligations on POL, namely:

a) *Reporting Obligations* – POL must report its derivative contracts to a trade repository no later than the working day after execution.

b) *Risk Mitigation Techniques* – POL must: (i) confirm trades in a timely manner; (ii) have dispute resolution processes in place; and (iii) engage in portfolio reconciliation.

14.2.4 POL will delegate reporting to its counterparty in derivatives transactions and will only execute derivative transactions with counterparties with which it has the appropriate delegated trade reporting agreements in place.

14.2.5 All trades will be confirmed by the end of the second day after execution.

14.2.6 POL will have ISDA agreements in place with all derivative counterparties to ensure that dispute resolution and portfolio reconciliation processes are documented.

POL00401626

15 ISDA Master Agreements

15.2 POL enters into ISDA[2] Master Agreements with potential derivative counterparties. The ISDA is an industry-standard agreement which governs the relationship between derivative counterparties and each transaction entered into under the ISDA. The key provisions of the ISDA include terms relating to payment and delivery obligations, termination rights, the close-out netting of transactions on termination, and representation and warranties. When executing derivative transactions POL enters into confirmations pursuant to the ISDA, which contain the economic terms of each transaction.

15.3 POL will only enter into derivative transactions with counterparties with which it has an ISDA agreement in place. POL will ensure that ISDA agreements are broadly similar in all material respects across counterparties. It is policy to standardise ISDAs where possible.

15.4 Only Treasury can negotiate ISDAs on behalf of POL.

15.4 **Delegated Authorities**

- *Agree changes to an ISDA Schedule* - IRRELEVANT
- *Approve and execute ISDA agreement on behalf of POL* - IRRELEVANT

[2] *ISDA – International Swaps and Derivatives Association*

POL00401626

Section III - Governance and Reporting

16 Treasury Governance and Reporting

16.1 Governance

16.1.1 PO Treasury risks are governed through the following structures:

16.1.2 **POL Board:** Authority to approve policies and approval limits relating to treasury risk management resides with the Board. Treasury risk management includes but is not limited to the following: short-term liquidity management, long-term funding, counterparty risk management, foreign exchange exposure management and interest rate risk management. The Board will delegate authorities to facilitate the operation of treasury risk management and the daily operation of the Treasury function.

16.1.3 **ARC Committee**: Financial risk management policies and approval limits are recommended to the Board for approval by the ARC Committee.

16.1.4 **Treasury Committee:** Is part of the Operations Board and meets on a monthly basis to review the Treasury Report, review financial risks, report on headroom and working capital, and report on and recommend changes to policy to the ARC Committee as required. The Treasury Committee is composed of the CFOO, the POL FD, the HoTTI and Finance Director Financial Services. Other members of the Operations Board may attend from time-to-time.

16.1.5 **FX Currency Hedging Committee**: Meets monthly or more frequently as required from time-to-time to confirm the value of hedges and timescales of hedges in accordance with the FX risk management policy. The committee is composed of: the Managing Director Post Office Money; the Finance Director Financial Services and Telecoms; and the Head of Travel.

16.1.6 The Board has delegated the following specific authorities to the **IRRELEVANT**

IRRELEVANT

- Approval of investment instrument limits
- Approval of counterparty selection criteria
- Approval of counterparties
- Approval of counterparty limits

- Approval of counterparties
- Approval of counterparty limits (within approved investment instrument limits)

16.1.7 The daily operation of treasury activity is delegated to the panels as shown on Appendix D. In all cases members of these panels will be appointed by the Treasury Committee.

16.1.8 Authority levels for write-offs are shown in Appendix F.

16.2 Treasury Management Reporting

16.2.1 The Treasury Report will be produced on a monthly basis. The contents of the report will include analysis of: note and coin inventory and how it is funded; insurance limits in cash centres; network cash holdings and inward rems; a monthly forecast update, including variance analysis for the prior period; Facility Headroom and Security Headroom; balances held in bank accounts; the net NRF Cap position; fx gains and losses; exposures to interest rate risks; treasury controls; as well as a summary of any project work currently being undertaken by Treasury.

16.2.2 The Treasury Committee will meet on a monthly basis as part of the Operations Board. It will review the Treasury Report and consider any other treasury risk management issues as required and make recommendations to the ARC.

16.2.3 Policy breaches will be immediately reported to the CFOO.

POL00401626

16.2.4 Treasury KPIs will be reviewed regularly.

16.2.5 Authorities to drawdown under established facilities are laid out in Appendix E.

16.2.6 An additional authority matrix is shown in Appendix F that relates to various items which arise during the normal course of business and for which individual write-off authorities are required. Examples of such items, which will normally be provided for, include:

- ATM cash trapping and retract fraud;
- Travelers' Cheque fraud;
- Camelot scratch cards failures in stock control due to master data errors.

Alisdair Cameron
March 2018

POL00401626

Appendix A: Summary of Counterparty Relationships, Services & Exposures

IRRELEVANT

POL00401626

Appendix B: CHAPS Banks

Bank of America (N.A)

Bank of England

Bank of Scotland (HBOS)

Barclays Bank PLC

Citibank N.A

CLS Bank International

Clydesdale Bank PLC

The Co-operative Bank PLC

Danske Bank

Deutsche Bank A.G

HSBC Limited

J.P. Morgan Chase Bank

Lloyds TSB Bank PLC

National Westminster Bank PLC

The Royal Bank of Scotland PLC

Santander UK PLC

Standard Chartered

State Street Bank

UBS A.G.

POL00401626

Appendix C: Delegated Authorities for Authorisation Panels

	Authorisation Panel	Delegated Authorities	Current Composition
Investment of Surplus Cash	Treasury Authorisation Panel	Approve investment of surplus cash balances - within policy Approve drawdowns - under existing credit facilities (up to 1 day)	Matrix securely maintained centrally by Treasury
	Dealing Panel	Propose investment of surplus cash balances Propose drawdowns - under credit existing facilities	Matrix securely maintained centrally by Treasury
Manual Payments	Banking Authorisation Panel *	Sign manual payment instruction (1) - < £50k - any 1 Banking Authorisation Panel member - > £50k - any 2 Banking Authorisation Panel members	Matrix securely maintained centrally by Treasury
Electronic Transfers	Payment Panel - (Internet Banking Systems) *	Release payment from internet banking system (2) - < £50k - any 1 Payment Panel (Internet Banking System) member - > £50k - any 2 Payment Panel (Internet Banking System) members	Matrix securely maintained centrally by Treasury
	Payment Panel - (Treasury Management System) ** *[BEIS Facility, NRF and file gateway payments]*	Release payment from TMS (2) - any 1 Treasury check AND - any 1 Banking Authorisation Panel OR Payment Panel member	Matrix securely maintained centrally by Treasury
	Payment Panel - (SAP) ** *[release of BACS payments]*	Release payment from SAP (2) - any 1 Amalgamated payment proposal AND - any 1 payment authoriser	Matrix securely maintained centrally by Treasury

(1) Cheques and direct debit instructions to bank - Banking Authorisation Panel members in accordance with mandates held by banks
(2) Aligned to authorisation rights in Internet Banking Systems / Treasury Management System / SAP

* *In respect of both the Banking Authorisation Panel and the various Payment Panels the lists are extensive and complex owing to the number of bank accounts used within the Group. The full listings are therefore not replicated here but are maintained and held securely by Treasury.*

** *In respect of the Treasury Management Systems and SAP, the controls around changes to master data (bank details), in particular around segregation of duties, are deemed to be strong enough that a two stage authorisation is not needed.*

POL00401626

Appendix D: Delegated Authorities for Drawdowns Under Credit Facilities

1. Approval of Drawdowns under BEIS Facility

Drawdown Amount	< £950m	< £950m	< £950m
Period of Drawdown	Up to 1 day	Over 1 day and up to 12 mths	over 12 mths
Delegated Authority	*1 member from Treasury Authorisation Panel*	**IRRELEVANT**	

2. Approval of Drawdowns Under Other External Borrowings

Drawdown Amount	< £50m	< £50m	< £50m	< £50m
Period of Drawdown	Overnight	Up to 1 wk	up to 6 mths	over 6 mths
Delegated Authority	*1 member from Treasury Authorisation Panel*	**IRRELEVANT**		

3. Leasing and Contract Hire

Amount	< £50m	< £50m
Maturity	Up to 8 years	Over 8 years
Delegated Authority	**IRRELEVANT**	

POL00401626

Appendix E: Individual Write-off Authority Levels

Authorities to write off provided-for items relating to external fraud and data errors:

Amount	< £1k	£1k to £10k	£10k to £100k	> £100k
Delegated Authority	**IRRELEVANT**			

POL00401626

Appendix F: Summary of Delegated Authorities

Separate attachment.

POL00401626

POST OFFICE LIMITED - Treasury Risk Management Framework, Policies and Authorities
Appendix F - Summary of Delegated Authorities - from March 2018

													Authorisation Panels						
																	Payment Panels		
	Reserved Matter	Ref.	Notes	Shareholder Consent	POL Board	Audit, Risk & Compl. Comm.	Treasury Comm.	FX Currency Hedging Comm.	CFOO	POL FD	Head of Treasury, Tax & Insuranc	Treasury Manager	Treasury Authorisation Panel	Dealing Panel	Banking Auth. Panel	Internet Banking Systems	Treasury Mgt. System	SAP
GENERAL	**General**																		
	Approve treasury risk management framework, policies and authorities	2.7	Must be			√													
	Approve amendments to or derogations from treasury risk management framework, policies and authorities (1)	2.7	Must be			√													
3. SHORT-TERM CASH AND LIQUIDITY MANAGEMENT	**Bank Account Structures**																		
	Approve addition of bank account to existing pooling arrangement	3.4.2	Any 1 from						√	√	√								
	Approve removal of bank account from existing pooling arrangement	3.4.2	Any 1 from						√	√	√								
	Approve creation of new pooling arrangement	3.4.2	Any 1 from						√	√									
	Committed Short-term Funding																		
	Approve change to Investment Reserve																		
	- in the range nil to £20m / for up to 2 weeks	3.6.8	Any 1 from						√	√	√								
	- up to £50m / for more than 2 weeks	3.6.8	Must be						√										
	Propose drawdown - under existing credit facilities	3.6.8	Any 1 from											√					
	Approve drawdown - under BEIS Facility																		
	- up to 1 day	3.6.8	Any 1 from						√	√	√		√						
	- over 1 day and up to 12 months	3.6.8	Any 1 from						√	√									
	- over 12 months	3.6.8	Must be						√										
	Approve drawdown - under Other External Borrowings (up to £50m)																		
	- overnight	3.6.8	Any 1 from						√	√	√		√						
	- up to 1 week	3.6.8	Any 1 from						√	√	√								
	- up to 6 months	3.6.8	Any 1 from						√	√									
	- over 6 months	3.6.8	Must be						√										
	Short-term Cash & Liquidity Arrangements with POMS																		
	Approve margin on intra-group loans to/from POMS on behalf of POL	3.7.8	Must be both						√		√								
	Execute documentation for intra-group loans to/from POMS on behalf of POL																		
	- up to £50m and up to 3 months	3.7.8	Must be						√										
	- over £50m or over 3 months	3.7.8	Must be		√														
4. MEDIUM AND LONG-TERM FUNDING MANAGEMENT	**Headroom**																		
	Approve amendment to Facility Headroom Buffer	4.8.4	Must be		√														
	Borrowing Policy																		
	Approve new medium and long-term funding	4.9.4	Must be both	√	√														
5. COUNTERPARTY CREDIT RISK MANAGEMENT	**Counterparty Credit Risk Management**																		
	Approve new financial institution counterparty	5.11	Must be			√													
	Approve financial institution counterparty limit	5.11	Must be			√													
	Approve temporary increase to financial institution counterparty limit	5.11	Must be						√										
6. INVESTMENT RISK MANAGEMENT	**Investment Risk Management**																		
	Approve new investment counterparty - within approved credit rating bands	6.14	Any 1 from						√	√									
	Approve changes to credit rating bands for counterparties	6.14	Must be			√													
	Approve temporary increase to investment counterparty deposit limit	6.14	Must be						√										
	Approve new permitted investment instrument	6.14	Must be						√										
	Propose investment of surplus cash balances	6.14	Any 1 from											√					
	Approve investment of surplus cash balances																		
	- Amount - < £300m / Term - up to 1 month	6.14	Any 1 from						√	√	√		√						
	- Amount - < £100m / Term - up to 3 months	6.14	Any 1 from						√	√	√		√						
	- Amount - < £50m / Term - up to 6 months	6.14	Any 1 from						√	√	√		√						
	- Amount - < £300m / Term - up to 1 year	6.14	Any 1 from						√	√									
	- Amount - < £50m / Term - up to 1 year	6.14	Must be both *		√				√										
	- Amount - < £50m / Term - up to 1 year	6.14	Must be		√														
7. FOREIGN EXCHANGE EXPOSURE MANAGEMENT	**Foreign Exchange Exposure Management**																		
	Execute FX hedge trades, within policy, in accordance with instructions issued by FX Committee	7.10	Any 1 from											√					
	Approve new permitted FX hedging instrument	7.10	Must be						√										
	Approve FX hedge trades for exposures not created by currency note inventory holdings																		
	- up to £50m	7.10	Must be						√										
	- above £50m	7.10	Must be		√														
8. INTEREST RATE EXPOSURE MANAGEMENT	**Interest Rate Exposure Management**																		
	Approve new permitted interest rate hedging instrument	8.9	Must be			√													
	Approve execution of interest rate hedging strategy	8.9	Must be		√														
9. BANK RELATIONSHIP MANAGEMENT	**Bank Relationship Management**																		
	Approve entering into relationship with new bank	9.9	Must be				√												
	Approve entering into relationship with new bank - prior to Treasury Committee approval	9.9	Must be						√										
	Approve entering into NDA with bank	9.9	Must be						√										
10. COMMODITY PRICE EXPOSURE MANAGEMENT	**Commodity Price Exposure Management**																		
	Execute commodity price hedges within policy	10.7	Must be											√					

Data: Confidential

Last Edit: 02/03/2018 10:02
Prepared By: Mark DIXON
F_Delegated Authorities_03.2018 Final.xlsx

POL00401626

POST OFFICE LIMITED - Treasury Risk Management Framework, Policies and Authorities
Appendix F - Summary of Delegated Authorities - from March 2018

	Reserved Matter	Ref.	Notes	Shareholder Consent	POL Board	Audit, Risk & Compl. Comm.	Treasury Comm.	FX Currency Hedging Comm.	CFOO	POL FD	Head of Treasury, Tax & Insuranc	Treasury Manager	Authorisation Panels: Treasury Authorisation Panel	Dealing Panel	Payment Panels: Banking Auth. Panel	Internet Banking Systems	Treasury Mgt. System	SAP
	Approve new commodity price hedge counterparty	10.7	Must be						√									
	Approve execution of commodity price hedges within policy	10.7	Any 1 from						√	√	√							
OTHER	**Operational Banking**																	
	Approve amendments to existing operational banking facilities (2)	11.6	Any 1 from						√									
	Approve new operational banking facilities (2)	11.6	Any 1 from						√									
	Approve opening of new bank account	11.6	Must be						√	√	√							
	Approve closure of bank account	11.6	Must be						√	√	√							
	Payments																	
	Sign manual payment instruction - < £50k	12.1.6	Must be 1 from												√			
	Sign manual payment instruction - < £50k	12.1.6	Must be 2 from												√			
	Release payment from Internet Banking System - < £50k	12.4.7	Must be 1 from													√		
	Release payment from Internet Banking System - > £50k	12.4.7	Must be 2 from													√		
	Release payment from Treasury Management System	12.4.7	Must be Treasury check and 1 from												√			
	Release payment from SAP	12.4.7	Must be 1 from															√
	Guarantees / Group Support																	
	Approve and execute a direct guarantee to a commercial third party for the benefit of POMS	13.1.4	Must be						√									
	Approve bank guarantee to support financing arrangement	13.2.4	Must be		√													
	Approve bank guarantee to support commercial arrangement	13.2.4	Must be						√									
	Execute counter-guarantee to bank in support of commercial arrangement	13.2.4	Must be						√									
	ISDA Master Agreements																	
	Agree changes to an ISDA Schedule	15.4	Any 1 from						√	√	√							
	Approve and execute ISDA agreement on behalf of POL	15.4	Must be						√									

** Must be CFOO and one other POL Board member*

(1) unless specifically stated as the Board (2) including overdrafts, fax lines, BACS limits, intra-day limits and similar arrangements

POL00401626

Document Retention and Disposal Policy

Author: Jules Harris Sponsor: Jane MacLeod Meeting Date: 13 Mar 2018

Executive Summary

Context

1. Post Office is subject to a number of legal and regulatory requirements regarding the retention and disposal of different types of data and documents. These include requirements under the Companies Act relating to statutory and financial records, the Financial Services and Markets Act relating to customers with regulated products, Telecoms in relation to Privacy and Electronic Communications (PECR), in relation to customers who have bought telephony products, as well under data protection legislation relating to documents which contain personal data.
2. Accordingly, Post Office needs to update its processes to ensure compliance. The draft Document Retention and Disposal Policy sets out the framework for compliance, and this paper sets out the steps to be taken to progressively implement the policy.

Questions addressed in this paper

- Why the policy is needed and what is incorporated
- Stakeholder inclusion in developing the policy
- How we will implement the policy
- How we will communicate the policy to staff
- Impact of delaying approval

Conclusion

3. The ***Document Retention and Disposal Policy*** has been created to:
   - Satisfy the requirements of the relevant legislation to ensure that information and documents which are subject to specific legal and regulatory requirements can be identified, retained for the correct periods, and then destroyed or disposed of;
   - Direct employees to useful resources via 'links' to provide support; and
   - provide advice to assist employees, and data owners and Departmental Data Stewards to make the right decisions;
4. A sub-project will be established as part of the GDPR programme to aid the business to identify relevant categories of information and documents, and ensure that there are proportionate processes in place to manage compliance.

POL00401626

Input Sought

The RCC is asked to approve the Document Retention and Disposal Policy, and the intended implementation plan.

POL00401626

The Report

Why the policy is needed, and what is incorporated

5. Both Post Office Limited and Post Office Management Services Limited ('POMS') are subject to the requirements of the Companies Act, various tax legislation and similar legal and regulatory requirements that require information and stated documents to be retained for a minimum period. Additionally certain types of products sold by both Post Office Limited and POMS are subject to specific regulatory requirements setting out minimum retention periods for documents and certain types of information.
6. Proportionate and appropriate document/data retention policies will assist Post Office and POMS to manage legal risk arising from excessive retention periods, as well as to minimise storage costs of documents, information and data that is no longer required to be held. It appears that a similar policy was approved within Royal Mail/Post Office in about 2011 however this is no longer embedded in business practices.
7. It is good business practice to determine what documents (both physical and electronic) are created in the ordinary course of business, and set guidelines as to how they will be used and stored, how long they will be retained for and in what format, and when and how they will destroyed/deleted. These practices aid compliance with applicable laws and regulations, reduce the risk of information and documents being unnecessarily retained, and reduces the likelihood of data breach, or other information security incident, as colleagues are clear about the sensitivity of any documents they access as part of their day to day business.
8. The risk appetite in relation to not complying with law and regulations or deviation from its business conduct standards, is Averse. In the absence of effective policies and procedures to manage this risk, we are therefore outside risk appetite, and this will become increasingly relevant – specifically in relation to personal data - once GDPR comes into force in May 2018. We therefore propose to establish a work stream within the GDPR programme to work with both Post Office and POMS to identify relevant legal and regulatory requirements, determine the categories of information and documents to which those requirements apply, and develop proportionate retention schedules, procedures and storage practices, as well as enhance awareness across the business of the need to understand and embed document management and storage protocols.
9. The policy contains a set of definitions which are aligned with the Data Management approach, and will be widely used within Post Office in the future.
10. Once created, these processes will be embedded into the change process.
11. The programme will also consider whether data retention requirements should be incorporated into contracts with our third party suppliers.

POL00401626

Stakeholder inclusion in developing the policies

12. The policies have been developed by Information Protection and Assurance (IPA), Head of MI, Analytics & Data Strategy, IT Security; in conjunction with Legal, Risk and Governance, and the Data Protection Officer.

How will we implement the policy?

13. The implementation of this policy will be undertaken by a separate workstream within the GDPR programme.
14. Funding proposals to be brought through the Change governance processes for funding in 2018-19 will include the cost of a small team to design the implementation plan, provide advice and guidance to the business in developing the required retention schedules. Priority will be given to documents and information relating to regulated products (e.g. within POMS and the wider FS & T business unit) as well as personal data held in relation to employees and agents.
15. The creation of Departmental Data Stewards is part of the Data Management programme being run by the Head of MI, Analytics & Data Strategy.
16. Many of the minimum control standards at 2.3 within the policy are dependent on the creation of Data Owners, and their acceptance of their responsibilities. The Head of MI, Analytics and Data Management and Head of Information Protection and Assurance are presenting to GE on this subject in April. Appropriate training for key roles will be developed and delivered. IPA will raise a risk exception to address the current risks. Nevertheless it is important for GDPR compliance.
17. Embedding the policy will be a significant exercise in order to bring Post Office within risk appetite. Post Office need to have the policy in place before GDPR implementation.

How will we communicate the policy to staff?

18. The mini project will:
    - Develop generic guidelines to support all staff in the interim pending roll out to specific areas, and these will be communicated via a 'One' Communication update on the Post Office Intranet;
    - update the policies on the SharePoint site for staff reference;
    - communicate the existence of the new policies in the all-staff Monthly Information Security Update publication;
    - create the area on SharePoint to store the retention schedules (and we will look at ways of creating and storing these schedules digitally rather than through Word or Excel schedules) ;
    - aid Company Secretariat in creation of relevant processes and procedures to maintain the SharePoint site, and
    - Provide targeted training and support to each business area as the protocols are rolled out.

POL00401626

Impact of delaying approval

19. Post Office is already outside its stated risk appetite for regulatory risk. Failure to address these issues could not only have financial implications in the event of regulatory involvement, however it also means that Post Office cannot take advantage of potential cost savings which should arise as a result of a more rigorous approach to deletion/destruction of documents and data at the end of retention periods.
20. Post Office also has contractual and certification requirements to have up-to-date policies and to review them annually. Further delay to the adoption of this policy could lead to issues in retaining our certifications, for example our ISO27001 Certification.

POL00401626



DRAFT

GROUP POLICIES

Document Retention and Disposal Policy

Version – V0.1

POL00401626

1. Overview 3
1.1. Introduction by the Policy Owner 3
1.2. Purpose 3
1.3. Core Principles 3
1.4. Application 4
1.5. Definitions 4
1.6. Legislation 5
1.7. Industry Guidance 5
2. Risk Appetite and Minimum Control Standards 6
2.1. Risk Appetite 6
2.2. Policy Framework 6
2.3. Minimum Control Standards 7
3. Tools – Retention Schedules 13
3.1. Functional Retention Schedules 13
4. Where to go for help 15
4.1. Additional Policies 15
4.2. How to raise a concern 15
4.3. Who to contact for more information 15
4.4. How to request an exception 15
Appendix A – Legislation details 16
Appendix B – Example Retention Schedule 18
5. Control 19
5.1. Policy Version 19
5.2. Policy Approval 19
4.3. Who to contact for more information ..... **Error! Bookmark not defined.**
5. Control ..... **Error! Bookmark not defined.**
5.1. Policy Version ..... **Error! Bookmark not defined.**

DRAFT

POL00401626

1. Overview

1.1. Introduction by the Policy Owner

This policy sets out Post Office's[1] commitment to the proper and lawful retention and disposal of its information assets. Information held for longer than is necessary carries additional risk and cost. Conversely, information not kept for long enough leaves Post Office vulnerable to knowledge or evidence gaps and sanctions from some of our regulators. Post Office recognises that failure to follow these principles will negatively impact business efficiency, and the ability to protect its interests as well as those of its customers and stakeholders.

1.2. Purpose

The Document Retention and Disposal Policy is a cornerstone for good information management in Post Office. Information management supports the delivery of Post Office services in an efficient and accountable manner, helping to maintain its position as a trusted provider, retaining information for operational use while ensuring adherence to the laws and regulations concerning them. The objective of this policy is to keep important information for future use or reference, to organize information so it can be searched and accessed at a later date and to dispose of information that is no longer needed. Retention and disposal requirements are mandated by a number of pieces of legislation and regulation to which Post Office is subject to.

This policy defines a set of high level principles to manage the retention and disposal of Post Office's information assets in a timely and secure manner according to business needs and legal and regulatory requirements.

All employees[2] have a responsibility to understand the requirements set out in this policy and seek clarification from their line manager or the Departmental Data Steward in the case of any uncertainty. A list of Data Owners and Departmental Data Stewards will be maintained on the Data Management area of the intranet and will be updated when staff change, or new ones are added. The address for the Data Management Site is:
https://poluk.sharepoint.com/sites/Extranet/FandO/DG/Data%20Glossary%20Wiki/Home.aspx

1.3. Core Principles

Compliance with this policy will assist in meeting the following principles:

Protection – Information that is needed to minimise the risk to Post Office from investigations, litigation or disputes will be easier to locate and will be retained systematically.

[1] [1]In this Policy "Post Office" and "Group" mean Post Office Limited and Post Office Management Services Limited.

[2] In this policy employee means employees permanent employees, temporary including agency employees, contractors, consultants and anyone else working on behalf of Post Office.

POL00401626

Employees will have clear guidelines for the secure disposal of information, protecting against misuse and data breaches.

Information that contributes to the Post Office's story in society will be protected, supporting corporate memory and brand identity through heritage.

Compliance – Post Office is subject to many laws and regulations which have information retention requirements. Compliance with these requirements will significantly reduce the risk of financial penalties, prosecution or reputational damage.

Accountability – Properly managed retention and disposal of information will allow Post Office to defend its actions by evidencing document destruction. Retention schedules and destruction/transfer documentation will underpin auditable disposal processes. In particular, this will support compliance with the Freedom of Information Act and the Data Protection Act as updated by GDPR and DPA 2018.

Efficiency – Timely disposal of information will lead to financial savings for document storage, as well as day to day efficiency savings when retrieving information.

1.4. Application

This policy applies to employees and, where applicable, Third Party Supply Chain.

1.5. Definitions

Information

'Information' is defined as a collection of data in the form of documents or other artefacts (such as spreadsheets, flow diagrams or reports) on which the business makes decisions.

Data

'Data' is defined as the elements that form part of systems and processes that are created or pass through our systems.

Documents

'Documents' are specifically a type of information which has been used to form the basis of decisions, or to support business processes, in the normal day to day running of Post Office.

Information assets

'Information assets' are collectively all of the above.

Departmental Data Steward

'Departmental Data Steward' is the person allocated by a Data Owner to undertake the day to day processes associated with the controls required by the Data Owner

Data Owner

'Data Owner' is the person (usually GE or GE-1) who is accountable for a data entity (or multiple data entities)

Data Entity

POL00401626

'Data Entity' is the term used to describe a concept in a data repository that is a container of data & relationships to other objects – such as Branch, Customer, Employee, Product etc.

Third Party Supply Chain

'Third Party Supply chain' refers to the organisations who provide services holding, storing or processing Post Office Information Assets.

Structured and Unstructured Data

'Structured Data' has pre-defined data models or schema within a database or system file. 'Unstructured Data' consist all those that do not have pre-defined data models or schemas thus can't be so readily classified and fit into a neat box. Unstructured data files often include text and multimedia content: photos and graphic images, videos, webpages, PDF files, PowerPoint presentations, emails, blog entries, wikis and word processing documents.

Document Retention Schedule

'Document Retention Schedule' is the document detailing the various requirements of the data owner in regard to documents under their sphere of control. An example of one is shown at Appendix B

1.6. Legislation

The following non-exhaustive list of legislation concerning the creation, management, disposal, use and re-use of documents and information is applicable to Post Office (a more extensive, but not definitive, list is available in Appendix):

- Postal Services Act 2000
- Data Protection Act (1998) [General Data Protection Regulations (Regulation (EU) 2016/679)]
- Freedom of Information Act (2000)
- Companies Acts (1985, 2004, 2006)
- Limitation Act (1980)
- Public Records Acts (1958, 1967)
- Financial Services and Markets Act (2000)

1.7. Industry Guidance

This policy is based on the international standard for records management, ISO 15489 and the Code of Practice on the management of records under Section 46 of the Freedom of Information Act 2000.

DRAFT

POL00401626

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

A Risk Appetite is the extent to which the group will accept that a risk might happen in pursuit of day to day business transactions. It therefore defines the boundaries of activity and levels of exposure that the group are willing and able to tolerate.

The Group takes its legal and regulatory responsibilities seriously and consequently has:

- **Averse** risk appetite in relation to not complying with law and regulations or deviation from its business conduct standards, of which this standard forms part
- **Averse** risk appetite in relation to any serious impact to the confidentiality, integrity and availability of information, leading to financial loss, business disruption, public embarrassment or legal consequences in line with risk impacts
- **Tolerant** risk appetite for legal and regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality
- **Averse** risk appetite for litigation in relation to high profile cases/ issues
- **Averse** risk appetite for data loss/ leakage that can lead to customer, commercial or reputational damage
- **Averse** risk appetite for inaccurate and unreliable processing of data
- **Averse** risk appetite for inefficient or ineffective or prolonged failure of, governance and control processes, critical financial reporting processes, critical supply chain and business continuity processes.

2.2. Policy Framework

This policy forms part of the Information Protection and Assurance (IPA) and IT Security Policy Set which is located here:

https://poluk.sharepoint.com/sites/postoffice/inside/Pages/Information-security.aspx

DRAFT

POL00401626

2.3. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

At Document/System Creation

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Product or service entity	Systems may not adequately support implementation of retention schedules and timely destruction of data. It may not be technically possible to permanently delete data or it may require a manual process.	As part of the design of a new product or service, or where a product or service is being updated, product or service risks must be considered, mitigated and documented before completion of design phase. This must include updating of any related Document Retention Schedules. The integrity and accuracy of data must be ensured at the point of collection.	Product manager Product manager/Data Owner	During design phase/ annually/ anytime there is a change During design phase/ annually/ anytime there is a change
Data Flows	Systems further down the process chain may not understand or implement the correct retention schedules.	As part of the design of projects or implementation of systems like new products or services, or where a product or service is being updated, product or service risks must be considered, mitigated and documented before completion of design phase. Understand what entities are within the system for which they are Data Owner and	Product Manager Data Owner	During design phase/ annually/ anytime there is a change Ongoing

POL00401626

		how these flow to other system or product entities. Ensure Departmental Data Stewards and Line Managers understand the full implications of implementing change within the systems for which they are designated Data Owner.	Data Owner/Departmental Data Steward	As part of sign-off of new or updated product sets.
Retention Schedules	Lack of creation or updating of retention schedules means that colleagues may not be aware of their obligations leading to inappropriate usage or retention of documents. This can cause Post Office to be fined or suffer reputational damage.	All Data Owners and Line Managers must ensure that the retention schedules for their area are up to date. This is especially important when changes are being implemented to business processes.	Data Owner/Line Manager	Ongoing

During Use of a document or system

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Risks to Information	Lack of understanding of the importance or sensitivity of the information flowing through a department could mean that employees do not perform the required actions on it.	Data Owners must ensure that all employees who view or process the information within their sphere of control understand the importance of that data.	Data Owners	Every 6 months in the Director assertions.
		Data Owners need to understand the designs of systems or products such that they can fully understand the scope of their entity. Data Owners may pass this to Departmental Data Stewards, but they retain accountability.	Data Owners	Ongoing
		Data Owners must ensure evidence of any decisions are retained.	Data Owners	Ongoing
		Data Owners must understand the complete information lifecycle (creation, capture, index, manage, access, retrieve, administer, repurpose, share, retain, dispose, preserve) for all data within their sphere of control.	Data Owners	Ongoing

POL00401626

Information Security	Inadequate access controls may lead to unauthorised deletion of information including sensitive or business critical information.	Line Managers must assess and assure risks relating to employee access to systems and files, especially those containing sensitive or business critical data. Data Owners must ensure that extra training on information security and data protection is provided to their Departmental Data Stewards.	Line Managers/ IT Data Owners	Ongoing Annually
Personal Data	Due to inadequate training, there is a risk of unintentional misuse of Personal Data, resulting in punitive penalties, reputational damage and a loss of licence to process personal data.	Data Owners must ensure all employees within their areas understand their responsibilities in regard to the protection of personal data. IPA must ensure that suitable training is made available to Data Owners and employees.	Data Owners IPA	Ongoing Annually
Employees	Due to inadequate training, there is a risk of under, or over, retention of information and failure to follow retention schedules, leading to punitive penalties or reputational damage.	All employees must undertake the annual Information Security and Data Protection training. They must also read and understand the Acceptable Use Policy, the Information Classification Standard and this document. 3rd party suppliers must ensure that all employees with access to Post Office data and information undertake Post Office agreed information management training. Ensure annual training contains adequate information on information management Ensure the IPA and IT Security Policy Set contains adequate information on Information management.	All employees 3rd party suppliers IPA IPA & IT Security	Annually/ within 3 weeks of starting Annually/ within 3 weeks of starting Annually Annually
Document Management	Failure to keep information evidencing appropriate destruction will increase time spent handling public access requests and will fail to protect Post Office in disputes around	Data Owners must ensure that they have defined the storage requirements for the data under their sphere of control, and that this has been documented and agreed. This particularly applies where encryption is	Data Owners	Annually/when a change occurs

POL00401626

	information rights regulations (such as Freedom of Information Act and Data Protection Act).	required. This is a field within the retention schedule.		
Retention Schedules	Lack of communication of required retention schedules may mean that incorrect decisions are made by employees regarding information which could lead to regulatory fines or inability to answer a request to find or correct data.	Data Owners must ensure that correct retention schedules are in place for the systems or product entities within their sphere of control. These are required to be created at project initiation. Line managers must ensure that they and all their employees are aware of the retention schedules in place for the data/information they process. Line Managers s must remain aware of relevant regulatory and legislative requirements for document retention and must regularly review and update retention schedules in line with these as well as functional changes to their area.	Data Owners Line Managers Line Managers	Annually/ when a need is identified Annually/ when a need is identified Annually/ when a need is identified
Incident Management	Failure to understand the implications of an incident can lead to poor decision making or regulatory sanctions	Data Owners must ensure that they are aware of any incidents to their data, and are satisfied with the resolutions	Data Owners	During an incident
Processes and Procedures	Incorrect processes and procedures can lead to employees incorrectly using data.	Data Owners / Departmental Data Stewards are responsible for ensuring all processes which access the information within their sphere of control are adequate and appropriate.	Data Owners & Departmental Data Stewards	Annually / when a new process or procedure is written
Governance	Lack of governance over documents could lead to incorrect usage of data and thus result in fines or reputational damage to Post Office.	All employees implementing document management practices consistent with this Policy. Preserving documents as required under this Policy. Properly disposing of information at the end of its retention period. Monitoring compliance with this Policy.	All employees All employees All employees	Ongoing Ongoing Ongoing

POL00401626

		Educating employees in document management practices. Maintaining the repository of retention schedules.	Head of MI, Analytics and Data Strategy IPA Company Secretariat	Ongoing Annually Ongoing
Legal/ Regulatory Framework	Failure to understand the requirements of any legal or regulatory issues by the Data Owner may lead to Post Office receiving sanctions where documents or entities have not been controlled appropriately	Ensure when creating their Document Retention Schedules all regulatory or legal requirements have been considered.	Data Owners	Annually

During Document/System Disposal

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Risks to Information	Incorrectly disposing of information could mean that, through lack of continued controls being implemented for a defunct system/document, Post Office may suffer a data breach.	Data Owners must ensure that they enforce the clauses within a contract at the end of its term. Data Owners must ensure that all users of the entities or documents under their sphere of control understand what actions are to be taken at the end of a retention period. All employees must ensure they understand what needs to be done with a document or system at the end of its retention period.	Data Owners Data Owners All Employees	When a contract closes Ongoing Ongoing
Document Management	Failure to keep information evidencing appropriate destruction will increase time spent handling public access requests and will fail to protect Post Office in disputes around information rights regulations (such as Freedom of Information Act and Data Protection Act).	The Destruction or transfer of information must be authorised by the Data Owner or Departmental Data Steward and documented so that an audit trail exists.	All employees/Data Owners/ Departmental Data Steward	Ongoing

POL00401626

DRAFT

POL00401626

3. Tools – Retention Schedules

Retention schedules will ensure that retention of information is considered prior to its creation. Some record types can be identified as having definite long-term business or historical value due to the activities they arise from. For others, their value may change over time, or an event (such as an audit or legal action) may require that their scheduled disposal is put on hold. All disposal of information must therefore be approved by the Data Owner before it is actioned and records must be reviewed where this is necessary to make a decision.

Disposal of information at the end of its assigned retention period means either destruction or transfer. Destruction of information must follow Post Office procedures as defined by the Data Owner / Departmental Data Steward in order to prevent a data breach (procedures apply to destruction of hard copy documents, electronic information and hardware). Where documents have been identified as suitable for transfer to The Postal Museum archive Departmental Data Stewards must ensure they comply. This should not be confused with transfer of semi-current or inactive documents to off-site storage facilities. Documents at the end of their retention period must not be transferred to off-site storage facilities unless they are subject to a hold on disposal.

Duplicate documents should be destroyed as soon as possible. Where information has been regularly shared between business units, only the original documents should be retained. Care should be taken that seemingly duplicate documents have not been annotated. Where Post Office shares information with other bodies, Post Office must ensure that they have adequate procedures in place so that the information is managed in accordance with the relevant legislation and regulatory guidance.

3.1. Functional Retention Schedules

Retention schedules set out the groups of documents that Post Office functions will maintain and when these are due for review, transfer to The Postal Museum or secure destruction.

Information on retention schedules will fall into three main categories:

1. Destroy after an agreed period – where the useful life of a group of documents can be easily pre-determined (for example, destroy 3 years after creation; destroy 6 years after the end of the financial year).

2. Automatically select for permanent preservation – where certain groups of documents can be readily defined as worthy of permanent preservation and transferred to The Postal Museum.

3. Review – examine documents to determine whether they should be destroyed, retained for a further period or transferred to The Postal Museum for permanent

POL00401626

preservation. Documents which fall under category 1 may need to be reviewed for potential legal hold if they pertain to an active case.

Retention periods and actions are based on informational value, evidential value, legal or regulatory requirements, and historical value.

DRAFT

POL00401626

4. Where to go for help

4.1. Additional Policies

This policy is one of a set of policies. The full set of IPA and IT Security policies can be found at:

https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx

The full set of Post Office Policies can be found at:

https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx

4.2. How to raise a concern

Any Post Office employee who suspects dishonest or fraudulent activity has a duty to:

- Discuss the matter fully with their Line Manager; or,
- Report their suspicions by telephoning Grapevine on GRO
- If either or both are not available, staff can contact the Post Office's General Counsel, who can be contacted by email at: whistleblowing GRO or by telephone on: GRO
- Alternatively staff can use the Speak Up service available on GRO
- or via a secure on-line web portal: http://www.intouchfeedback.com/postoffice

Post Office encourages members of the public or people not employed by us who suspect [*activity in breach of policy*] to write, in confidence, to the **Chief Executive's Office, Finsbury Dials, 20 Finsbury St, London EC2 9AQ**.

4.3. Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact Information Protection and Assurance via GRO or IT Security via GRO

4.4. How to request an exception

If there is anything within this policy that causes business impact, please contact IPA via GRO and we will process an exception. Any exceptions are presented to the Information Security governance body for ratification.

POL00401626

Appendix A – Legislation details

Postal Services Act 2000

The Postal Services Act requires postal companies operating in the UK to be licensed. The Licence sets out quality standards and the rules by which licensees are permitted to operate. Postcomm has strong powers to investigate compliance and Licence Condition 17 obliges Post Office to furnish any information that the regulator requires to fulfil its function. Therefore, it is in Post Office's interest to retain and dispose of information systematically in order to provide evidence of compliance.

Data Protection Act (1998) [General Data Protection Regulations (Regulation (EU) 2016/679)]

The Data Protection Act governs how personal details must be handled and gives individuals rights over their personal information including access and processing. There is an explicit obligation under the Act that personal data processed for any purpose shall not be kept for longer than is necessary for that purpose. Therefore, documents containing personal data must always be allocated a retention period, and must never be held indefinitely.

The Law provides that, apart from any statutory and regulatory retention periods, employers should adopt a risk analysis approach to deciding the retention period appropriate for employee's personal information. Employee files should be reviewed on a regular basis to clear out irrelevant, excessive and/or out of date information. Once the employment relationship has ended, employers should destroy information which is no relevant.

Freedom of Information Act (2000)

The main purpose of the Freedom of Information Act (FOI) is to open the actions and decisions of Post Office up to legitimate public scrutiny. The Act gives anyone the right to ask for information, be told whether or not Post Office have it and, if so, to be given the information unless covered by a relevant exemption. It applies to all recorded information (including email correspondence) held by or on behalf of Post Office, regardless of when, where or why it was created.

FOI does not itself change the length of time that documents are kept. However, being able to demonstrate a clear and coherent document retention policy assists compliance, and the systematic and timely disposal of information is also important in preventing the release of confidential information.

The Freedom of Information Act extends the definition of personal data to include any unstructured personal information. Individuals, and sometimes third parties, may therefore have a right to see any data held about them irrespective of where it is stored.

Companies Acts (1985, 2004, 2006)

The Companies Act requires public companies to keep accounting details for a minimum of 6 years from the date they were made. The Act also requires companies to keep statutory registers (e.g. of Directors' interests) and to file statutory returns at Companies House.

The Companies (Audit, Investigations and Community Enterprise) Act 2004 requires that documents relating to transactions and accounting practices is auditable, and permits auditors and the Secretary of State to request company information from any employee.

POL00401626

Limitation Act (1980)

The Limitation Act sets out the time periods within which various kinds of legal proceedings must be brought. The risk of claims and their limitation period must be taken into account when deciding how long documents should be kept.

Public Records Acts (1958, 1967)

Post Office is subject to obligations under the Public Records Acts (PRA) which require public bodies to select documents of historical interest for permanent preservation. Under PRA, documents of historical value must be identified and transferred to The Postal Museum archive for permanent retention no later than 20 years after they were created.

Financial Services and Markets Act (2000)

The key statute that regulates the financial services industry in the UK

DRAFT

POL00401626

Appendix B – Example Retention Schedule

Retention Schedules should be stored in the Data Retention Schedule area as a spreadsheet. The example below is a small portion of the Company Secretariat one to show fields and suggested usage.

	Record Category	Record Type	Local Record Name	Record Format	Record Location	Retention Period	Authority	Information Asset Owner	Storage Instructions	End of Period Action	Record of Historical Value?	Notes
1	**ACTIVITY: Corporate Governance** Records related to incorporation and organisation of POL and its subsidiaries, ownership, boards and committees, shareholders, strategy, planning and policy.											
1.1	Board of Directors and Senior Committee Meetings	Records related to proceedings of the board of directors, board committees and shareholders. Includes meeting minutes and meeting notices, shareholder decisions.				Ten years from date of meeting.	S.248(2) CA 2006			Transfer to Postal Museum Archive.	Y	
1.2	Business Organisation and Incorporation	Records related to the creation, structure, and governance of POL and its subsidiaries. Includes incorporation documention, articles and memorandum of association, and name change certificates.				Permanent.	S.32 CA 2006			Transfer to Postal Museum Archive.	Y	
		Copies of forms filed at Companies House.				No requirement to retain, Good practice to retain copies for two years.	CA 2006			Destroy	N	
		Statutory registers.	Register of members	Electronic	Blueprint	Permanent. Entries for former members must be retained for at least ten years from the date when they ceased to be members.	S.114 CA 2006			Transfer to Postal Museum Archive.	Y	
			Register of Directors and Secretaries	Electronic	Blueprint	Permanent.	S.162 CA 2006					

DRAFT

POL00401626

5. Control

5.1. Policy Version

Date	Version	Updated by	Change Details
26/02/2018	0.1	IPA & CoSec	First draft Version
04/03/2018	0.2	IPA & Head of MI, Analytics and Data Strategy	Edits following peer review.
07/03/2018	1.0	General Counsel	First Final Version

5.2. Policy Approval

Group Oversight Committee: Risk and Compliance Committee (RCC)
Sign-off Authority: Risk and Compliance Committee (RCC)
Policy Sponsor: Jane MacLeod, Group Director of Legal, Risk & governance
Policy Owner: Head of Information Protection and Assurance
Policy Author: Jules Harris
Approved by: Post Office Management Services Limited RCC
Post Office Ltd RCC

Approved: Xx xxx 18
Next review: Xx xxx 19

DRAFT

POL00401626

IT Security Policy

Author: Hazel Freeman | Sponsor: Jane MacLeod | Meeting Date: 13 March 2018

Executive Summary

Context

1. To support the GDPR project a new policy is being presented for review. This is titled 'IT Security Policy' and replaces the Business Information Systems policy and Business Information Systems Framework. The policy has been aligned to the COBIT5 project and the IT Risk register maintained by Financial Control.

Questions addressed in this paper

1. Why is the policy required?
2. Changes to the policy and the value of those changes
3. Stakeholder inclusion in developing the policies
4. How we will communicate the policies to third parties?
5. Implications of the policy changes to our staff and the wider business
6. Impact of delaying approval

Conclusion

2. The IT Security Policy has been created to provide a set of minimum controls needed to mitigate the following risks to Post Office data;
   - Poor design of business applications or lack of consideration regarding security requirements during the design process can lead to the introduction of security vulnerabilities and subsequently result in breaches of data, loss of integrity or data being accessed by unauthorised individuals.
   - Having inappropriate access controls to data owned or processed by Post Office could lead to inappropriate access by unauthorised individuals.
   - If the design of systems supporting or running security services for Post Office are not securely designed to the highest standards, those functions cannot be assured and Post Office systems and data may be open to attack, causing data breach or loss of confidentiality, integrity and availability.
   - If networks supporting the flow of Post Office information are not designed with security in mind, then those networks themselves may contain vulnerabilities causing a loss of confidentiality, integrity or availability of systems and or data.
   - Poorly controlled mobile and removable devices may lead to a data breach causing a loss of confidentiality, integrity or availability, reputational damage and/or fines from the regulator.

POL00401626

- If Post Offices devices (laptops, mobiles, network devices, servers etc) are poorly configured or maintained and those vulnerabilities are exploited then this could lead to a loss of confidentiality, integrity or availability, reputational damage and/or fines from the regulator
- Post Office's environment is compromised due to lack of, or poorly configured cyber threat protection solutions which could lead to a loss of confidentiality, integrity or availability, reputational damage and/or fines from the regulator.

Input Sought

The RCC is asked to approve the new IT Security Policy

POL00401626

The Report

Why is the policy required?

3. This is a new policy that is required to support the GDPR program. It supports section (f) of Article 5 of the regulation:

   GDPR requires that personal data shall be:

   "f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Changes to the policy and the value of those changes.

4. The policy has been created using the new template, the controls are clearly linked to the risks that they are mitigating.
5. The policy is supported by a number of standards that are currently under review, these include:
   - Access control Standard
   - Network Security Standard
   - BYOD Standard
   - Wireless Standard
   - Cloud Computing Standard
   - Portable Device Standard
   - Remote Access Standard
   - Logging and Monitoring Standard
   - SDLC standard
   - Encryption Standard
   - Anti Malware Standard
   - Patch Management Standard
   - Configuration Standard
   - Cyber Incident Response Standard
   - Threat Management Standards
   - IT Security Standard

Stakeholder involvement in developing the policies

6. The policies have been developed by - Information Protection and Assurance (IPA), IT Security; in conjunction with - Legal, Risk and Governance. Data Protection Officer, and Financial control (COBIT5 project).

How we will communicate the policies to third parties?

POL00401626

7. IT Security will:
   - update the policies on the SharePoint site for staff reference
   - engage with suppliers to inform them of the new policy set
   - perform workshops with suppliers so they understand what is required of them
   - perform a gap analysis with the suppliers to understand where we have gaps
   - work with the suppliers to create a remediation plan
   - communicate the existence of the new policies in the all-staff Monthly Information Security Update publication

Implications of the policy changes on our staff and the wider business

8. This policy is mainly directed at suppliers of IT Services to Post Office, and not colleagues. Within IT colleagues in the architecture space are required to ensure that these policies have been adhered to as part of any designs received from our third party suppliers.
9. Over the next 12 months, IT security will work with our suppliers to understand where our gaps are and remediate them.
10. The introduction of the Minimal Control Requirements supports third parties in understanding what is required of them.

Impact of delaying approval

11. The GDPR deadline is fast approaching (May 2018), we have already updated Schedule 16 of the standard contract to include the IT Security Policy as a requirement.

POL00401626

GROUP POLICIES

IT Security Policy

Version – V0.3

POL00401626



1. Overview 3
1.1. Introduction by the Policy Owner 3
1.2. Risk Appetite 3
1.3. Purpose 3
1.4. Core Principles 3
1.5. Application 4
1.6. Legislation 4
1.7. Industry Guidance 5
1.8. Policy Framework 5
1.9. Who must comply? 5
2. Minimum Controls 6
3. Where to go for help 10
Additional Policies 10
3.1. How to raise a concern 10
3.2. Who to contact for more information 10
4. Control 11
4.1. Policy Version 11
4.2. Document Control 11

POL00401626

1. Overview

1.1. Introduction by the Policy Owner

Post Office is committed to protecting its employees, customers, Third Party Supply Chain and information assets from damaging or illegal actions by individuals, either knowingly or unknowingly. Post Office enables this through the development and deployment of policies, standards and guidelines which are aligned to international best practices. Effective cyber and information security is a team effort involving everyone in Post Office.

1.2. Risk Appetite

There follows a list of applicable Risk Appetite statements for this policy:

- **Averse risk appetite** in relation to not complying with law and regulations or deviation from its business conduct standards, of which this standard forms part.
- **Averse risk appetite** in relation to any serious impact to the confidentiality, integrity and availability of information, leading to financial loss, business disruption, public embarrassment or legal consequences in line with risk impacts.
- **Tolerant risk appetite** for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality.
- **Averse risk appetite** for litigation in relation to high profile cases / issues.
- **Averse risk appetite** for unethical behaviour including staff misfeasance.
- **Averse risk appetite** for data loss/leakage that can lead to customer, commercial or reputational damage
- **Neutral risk appetite** for operational IT services.
- **Averse appetite** for inaccurate and unreliable processing of data.
- **Averse risk appetite** for inefficient or ineffective or prolonged failure of, governance and control processes, critical financial reporting processes, critical supply chain and business continuity processes.

Post Office acknowledges however that in certain scenarios even after extensive controls have been implemented a risk may still sit outside the agreed Risk Appetite. In exceptional circumstances a Risk Exemption waiver may be granted

1.3. Purpose

The purpose of this document is to detail the minimum IT controls required to reduce the Post Offices exposure to information security threats such as:

- threats from the internet (cyber threat)
- threats from internal staff (either malicious or accidental)
- threats from third parties (either malicious or accidental)

1.4. Core Principles

Compliance with this policy will ensure that the following principles are met:

POL00401626

- External suppliers to be identified and categorised such that a risk based approach can be facilitated in assessing the suppliers security controls.
- Security arrangements can be agreed and embedded into service agreements and contracts.
- Security controls can be validated prior to services commencing and on an ongoing basis.
- Termination of third party relationships can be effectively managed so as not to expose Post Office to additional Risks.

1.5. Application

This policy relates to all Post Office information assets, including critical business information systems, as defined by Post Office, and as amended from time to time, and applies to all employees[1]

Post Office information assets and systems include, but are not limited to:

- Business environments;
- Business processes;
- Business applications (including those under development);
- Information systems; and
- Networks

1.6. Legislation

Post Office seek to comply withall relevant UK legislation and regulatory requirements including (but not limited to):

- General Data Protection Regulation (2017)
- Data Protection Act (1998 and 2017).
- Freedom of Information Act (2000).
- Privacy and Electronic Communication Act (2003).
- Regulation of Investigatory Powers Act (RIPA) (2000).
- Copyright, Designs and Patents Act (1988).
- Computer Misuse Act (1990).
- Human Rights Act (1998).
- Terrorism Act (2006).
- Limitation Act (1980).
- Malicious Communication Act 1988).
- Digital Economy Act (2010).
- Privacy and Electronic Communications (EC Directive) (Amendment) Regulations (2011).
- Counter-Terrorism and Security Act (2015).

[1] In this policy employee means employees permanent employees, temporary including agency employees, contractors, consultants and anyone else working on behalf of Post Office.

POL00401626

1.7. Industry Guidance

Post Office is a member of the Information Security Forum (ISF) which is used to provide input to Information Protection and Assurance (IPA) and IT Security developments.

1.8. Policy Framework

This policy forms part of the IPA and IT Security Policy Set which is located here:

https://poluk.sharepoint.com/sites/postoffice/inside/Pages/Information-security.aspx

1.9. Who must comply?

Compliance with this policy is mandatory for all Post Office services. All third parties who do business with Post Office, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this standard or have their own equivalent policy.

POL00401626

Post Office Limited Risk and Compliance Committee-13/03/18

2. Minimum Controls

A minimum control is an activity which must be in place in order to manage the risks within the defined Risk Appetite statements contained within the table below. To comply with this, mechanisms must be in place within each business unit or product to demonstrate compliance. The minimum controls can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk, and the required minimum controls. The subsequent page defines in greater detail terms used:

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Secure Development of business applications	Poor design of Business applications or lack of consideration regarding security requirements during the design process can lead to the introduction of security vulnerabilities and subsequently result in breaches of data, loss of integrity or data being accessed by unauthorised individuals.	All projects and programmes must liaise with IT Security and the IT Architecture teams for advice and guidance on the security aspects of their designs. All development must comply with SDLC and Secure Coding and Testing standards (e.g All data used in testing must be cleansed).	Business Unit CIOs, Project & Programme Managers, and procurement.	At project design phase and during change.

POL00401626

Supplementary Documents

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Identity and Access Management	Having inappropriate access controls to data owned or processed by Post Office could lead to inappropriate access by unauthorised individuals	All systems must comply with the Access Control Standard.	Data Owners, Line Managers, Business Unit CIOs, Project and Programme managers, and procurement	Whenever a new system is being designed or procured, or when significant change is being applied.
Security Infrastructure	If the design of systems supporting or running security services for Post Office are not securely designed to the highest standards, those functions cannot be assured and Post Office systems and data may be open to attack, causing data breach or loss of confidentiality, integrity and availability.	All projects and programmes must liaise with IT Security and the IT Architecture teams for advice and guidance on the security aspects of their designs. All infrastructure must comply with the Platform Security standard	Business Unit CIOs, Third party supply chain of IT Services where systems are hosting or processing Post Office Data	All the time, and evolving with new best practice.

Post Office Limited Risk and Compliance Committee-13/03/18

POL00401626

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Network Management	If networks supporting the flow of Post Office information are not designed with security in mind, then those networks themselves may contain vulnerabilities causing a loss of confidentiality, integrity or availability of systems and or data.	All network designs must adhere to the Network Security standard.	Business Unit CIOs, Third party supply chain of IT Services where systems are hosting or processing Post Office Data	All the time, and evolving with new best practice.
Mobile and removable devices	Poorly controlled mobile and removable devices may lead to a data breach causing a loss of confidentiality, integrity or availability, reputational damage and/or fines from the regulator.	All mobile and removable devices must adhere to the BYOD and Portable device standards.	All staff	All the time

POL00401626

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Vulnerability Management	If Post Offices devices (laptops, mobiles, network devices, servers etc) are poorly configured or maintained and those vulnerabilities are exploited then this could lead to a loss of confidentiality, integrity or availability, reputational damage and/or fines from the regulator	All devices must adhere to the patch management and configuration management standards, and also any hardening documentation. All devices must comply with the Vulnerability Management Standards	IT Security and IT Architecture, Third party supply chain of IT Services where systems are hosting or processing Post Office Data	All the time
Cyber Threat Protection	Post Office's environment is compromised due to lack of, or poorly configured cyber threat protection solutions which could lead to a loss of confidentiality, integrity or availability, reputational damage and/or fines from the regulator	All of Post Office's cyber security protection solutions must adhere to the Threat Protection Standards	IT Security and IT Architecture, Third party supply chain of IT Services where systems are hosting or processing Post Office Data	All the time

POL00401626

3. Where to go for help

Additional Policies

This Policy is one of a set of policies and standards. The full set of policies and standards can be found at:

https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx

3.1. How to raise a concern

Any Post Office employee who suspects dishonest or fraudulent activity has a duty to:

- Discuss the matter fully with their Line Manager; or,
- Report their suspicions by telephoning Grapevine on GRO.
- If either or both are not available, staff can contact the Post Office's General Counsel, who can be contacted by email at: whistleblowing GRO or by telephone on: GRO.
- Alternatively staff can use the Speak Up service available on GRO
- or via a secure on-line web portal: http://www.intouchfeedback.com/postoffice

Post Office encourages members of the public or people not employed by us who suspect [*activity in breach of policy*] to write, in confidence, to the **Chief Executive's Office, Finsbury Dials, 20 Finsbury St, London EC2 9AQ**.

3.2. Who to contact for more information

If you need further information about this standard or wish to report an issue in relation to this standard, please contact Information Protection and Assurance via GRO or IT Security via GRO

POL00401626

4. Control

4.1. Policy Version

Date	Version	Updated by	Change Details
06/02/2018	0.1	IT Security	First draft for review
05/03/2018	0.2	IT Security & IPA	Updated post JH Comments
09/03/18	0.3	IT Security	Updated post peer review

4.2. Document Control

Group Oversight Committee: Risk and Compliance Committee (RCC)
Sign-off Authority: Risk and Compliance Committee (RCC)
Policy Sponsor: Rob Houghton, Group CIO
Policy Owner: Head of IT Security
Policy Author: Hazel Freeman
Approved by: Post Office Ltd RCC

Approved: Xx xxx 18
Next review: Xx xxx 19

POL00401626

IT POLICIES

IT Disaster Recovery Policy

Version – V0.1

POL00401626

Group Oversight Committee:	Risk and Compliance Committee (RCC)
Sign-off Authority:	Risk and Compliance Committee (RCC)
Policy Sponsor:	Rob Houghton Group CIO
Policy Owner:	IT Security and Service Director
Policy Author:	Head of IT Risk & Compliance
Approved by:	Post Office Management Services Limited RCC Post Office Ltd RCC
Approved:	
Next review:	

POL00401626

1. Overview 4
1.1. Introduction by the Policy Owner 4
1.2. Purpose 4
1.3. Core Principles 4
1.4. Application 5
1.5. Impact of loss of service 5
1.6. Legislation 5
2. Risk Appetite and Minimum Control Standards 6
2.1. Risk Appetite 6
2.2. Policy Framework 6
2.3. Who must comply? 6
2.4. Minimum Control Standards 7
3. Where to go for help 10
3.1. Additional Policies 10
3.2. How to raise a concern 10
3.3. Who to contact for more information 10
3.4. How to request an exception 10
4. Version Control 11

POL00401626

1. Overview

1.1. Introduction by the Policy Owner

Post Office's Board and Group Executive (GE) recognise that with the ever increasing threat landscape, the possibility and the impact of events caused by human action or natural disasters must be planned for.

The GE are committed to developing a strategic response to current and emerging threats to enable Post Office to achieve its objectives, whilst preserving the Post Office brand, commercial image, reputation, competitive advantage, revenues, profitability, legal, regulatory and contractual compliance.

Employees have a responsibility to understand the requirements set out in this policy, if there is any misunderstanding, the employee must gain clarification from the IT Service Performance team.

1.2. Purpose

The purpose of this document is to detail the IT controls required to reduce exposure to the Post Office brand in the event of Disaster Recovery incident occurring within the Post Office estate.

Disaster recovery focuses on the IT or technology systems supporting critical business functions, as opposed to business continuity, which involves keeping all essential aspects of a business functioning despite significant disruptive events. Disaster recovery is therefore a subset of business continuity.

Disaster Recovery is where our catastrophic loss over services hosting site occurs and invocation and recovery is needed from an alternate location, this is different from resilience which is the mechanism that is designed in to keep systems available in the event of component failure loss at the same location.

Resilience should be measured in no loss to the system disaster recovery is where a recovery exercise needs to occur to invoke and set up a system post a catastrophic host location loss.

1.3. Core Principles

Compliance with this policy will aid in adhering to the following principles:

- Maintain and enhance shareholder/stakeholder value.
- Protect revenue streams and business profitability.
- Improve governance.
- Ensure that IT DR postponement is managed by exception.
- Compliance with Legal and Regulatory requirements.

POL00401626

1.4. Application

This policy applies to employees[1]and, Third Party Supply Chain.

1.5. Impact of Loss of Service

The inability to recover service will result in a Loss of Service to our customers.

Data loss can lead to financial loss through fines from regulators, damage the reputation of Post Office though negative coverage in the media and result in loss of trust by our customers and suppliers.

1.6. Legislation

Post Office seek to comply with all relevant UK legislation and regulatory requirements.

ISO/IEC 27031:2011

ISO 22301

ISO/IEC 24762:2008

[1] In this policy employee means employees permanent employees, temporary including agency employees, contractors, consultants and anyone else working on behalf of Post Office.

POL00401626

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

There follows a list of applicable Risk Appetite statements for this policy:

- **Averse risk appetite** for inefficient or ineffective prolonged failure of governance and control processes, critical supply chain and business continuity processes.
- **Averse risk appetite** for any serious impact to the confidentiality, integrity and availability of information which may result in financial loss, business disruption, public embarrassment or legal consequences.
- **Averse risk appetite** for data loss/leakage that can lead to customer, commercial or reputational damage

Post Office acknowledges that in certain scenarios, even after extensive controls have been implemented, a risk may still sit outside the agreed Risk Appetite. In exceptional circumstances a Risk Exemption waiver may be granted.

2.2. Policy Framework

This policy forms part of the IT Policy Set. IT Policies are currently under review.

2.3. Who must comply?

Compliance with this policy is mandatory for all Post Office employees and applies wherever in the world Post Office business is undertaken.

All IT Services, Systems and Infrastructures will have IT Disaster Recovery criteria agreed, that conforms to the business needs and the IT Disaster Recovery Framework.

All new IT services must have an agreed IT Disaster Recovery criteria with the IT Security and Service Director prior to transition to the live service.

POL00401626

2.4. Control Standards

The control standards described below are derived from the IT Controls Framework (COBIT 5). The controls are in place to manage the risks within the defined Risk Appetite statements, as contained within the table below. To comply with this, mechanisms are in place within IT to demonstrate compliance.

The table below sets out the relationships between identified risk, and the required minimum control standards.

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Identify areas of continuity that need addressing	Failure to define an IT business continuity plan may result in inability to restore critical applications within defined timelines in line with business need.	• Disaster Recovery Framework in place. • (BIA) is performed on a periodic basis which considers the impact of a disruption to critical business functions. • ITSCM Monthly reviews are in place, outputs of DR to be discussed and manage any escalations. • Obtain the defined RTOs and RPOs for key PO applications and understand if both the business and IT have agreed the recovery timeframe.	IT Service & Performance. SISD IT Service Continuity Manager	Annual
Develop and implement a business continuity response	Failure to define a PO IT business continuity plan may result in inability to restore critical applications within defined timelines in line with business need.	• The DR Framework will show the last test date/scheduled tests. • ITSCM Monthly reviews are in place, outputs of DR to be discussed and manage any escalations. • Exception process in place in place to prevent cancellation/postponement of DR tests without authorisation. • Forward Schedules to be provided by third-parties to prevent any failover tests clashing with other suppliers.	IT Service & Performance. SISD IT Service Continuity Manager. Head of IT Risk & Compliance	Monthly
Exercise, test and review	Failure to exercise and test the business continuity plan	• Third-party suppliers ensure regular test occur in accordance to their contracts.	IT Service & Performance.	Annual

POL00401626

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
the DR Framework	in line with the PO IT business continuity strategy may result in inability to restore critical applications within defined timelines in line with business need.	• Any conflicting dates to be rearranged and scheduled.	SISD IT Service Continuity Manager Third party suppliers	
Develop and implement a business continuity response	Absence of a defined and communicated training strategy for business continuity response may result in: a) Business interruption and delays in recovery of business operations which fail to meet business needs. b) Misalignment of priorities for recovery of services.	• DR Framework to be communicated to Business Stakeholders. • Any misalignment of priorities for recovery of services will be reviewed at the Monthly ITSCM.	Head of IT Services. IT Service & Performance. SISD IT Service Continuity Manager. Head of IT Risk & Compliance	Quarterly
Manage backup arrangements	Absence of a defined process for review of backup schedules and compliance with PO IT policy may result in non-compliance with policy and failure to identify backup schedules not being setup to business requirements.	• Recovery point objectives in place where applicable. • DR Framework includes high level contractual requirements of suppliers. • Stakeholder reviews in place and confirm if the requirements for recovery are correct. • Monitored at the monthly ITSCM.	Head of IT Services. IT Service & Performance. SISD IT Service Continuity Manager.	Monthly
Conduct post-resumption review	Absence of a defined process to test and review restoration of backup and archived data may result in: a) Failure to restore from backups resulting in loss of business critical information when a disaster has occurred.	• Continuity test, understand the effectiveness of the plan, continuity capabilities, roles and responsibilities, skills and competencies. • Understand the steps required for improvement and validate if remediation plans have been put in place. • Obtain evidence that these changes were processed via the enterprise change control process.	IT Service & Performance. Change Management.	As appropriate

Post Office Limited Risk and Compliance Committee-13/03/18

POL00401626

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
	b) Failure to recover applications in line with business need when a disaster has occurred.			

POL00401626

3. Where to go for help

3.1. Additional Policies

This policy is one of a set of policies.

3.2. How to raise a concern

Any Post Office employee who suspects that a serious event is taking place is required to:

- Report this to the IT Service Desk.

3.3. Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact IT Security & Service Director.

3.4. How to request an exception

If there is anything within this policy that causes business impact, please contact Head of IT Risk & Compliance who will process the exception. Any exceptions are presented to the Information Security governance body for ratification.

POL00401626

4. Version Control

Date	Version	Updated by	Change Details
13/03/2018	V0.1		Sign off required at RCC

POL00401626

Disaster Recovery Framework

	Fujitsu	Network Banking Service (POCA/Vocalink/Santander)	Network	Debit Card System	On-line Transaction processing Service (Horizon POS)	Automated Payments Outpay (APOP)	Bureau Service	Web Services including Moneygram	Logistic Feeder Service (LFS)	Automated Payments Service (APS)	Department of Vehicle Licensing Authority - Post Office MOT Enquiry	Electronic Top-ups Service	Postal Address File (PAF) service	Transaction Enquiry Service (TES)	Track and Trace	PODG	Collect & Return Web Service
Gold Service (recovery within 5 hours)		✓	✓	✓	✓											✓	
Silver Service (recovery within 24 hours)						✓		✓		✓							✓
Bronze Service (recovery time within 96 hours)							✓		✓		✓	✓	✓	✓	✓		
Busines Impact Analysis		✓	✓	✓	✓	✓	✓				✓					✓	
Contracted Recovery Time Objective (RTO)		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Recovery Time		2 hours	2 hours	2 hours	2 hours	2-5 hours	2 hours	2 hours	2 hours	2-5 hours	2-5 hours	2-5 hours	2-5 hours	2-5 hours	2-5 hours	2-5 hours	2-5 hours
Contracted Recovery Point Objective (RPO)		n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a		n/a
Recovery Point		n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a		n/a
Managed By Atos		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DR Test frequency confirmed		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DR Tests up to date		✓	✓								✓			✓		✓	
Last Tested		Oct-17	Oct-17	May-13	May-13	May-13	May-13	May-13	May-13	May-13	May-16	May-13	May-13	May-13	May-13	Jun-17	May-13
Scheduled Test		Jul-18	Jan-18														

Key

Red box denotes risk/gap

* Verizon dates have been received and are currently being re-aligned to avoid tests already scheduled from other Suppliers.

POL00401626

Disaster Recovery Framework

	MDM (production environment)	Credence (production environment)	POLSAP (production environment)	Gemalto	Biometric Application, Enrolment and	Fres	Travel Money Card	Bureau Service	Computacenter	DHCP	Active Directory	Email	OneDrive	Sharepoint	Skype	Ricoh Printer Server	Admin LAN
Gold Service (recovery within 5 hours)	✓	✓	✓		✓					✓	✓	✓	✓	✓	✓	✓	✓
Silver Service (recovery within 24 hours)							✓										
Bronze Service (recovery time within 96 hours)								✓									
Busines Impact Analysis	✓	✓	✓				✓	✓									
Contracted Recovery Time Objective (RTO)	✓	✓	✓		✓					×	✓	×	×	×	×	×	×
Recovery Time	2-5 hours	2-5 hours	2-5 hours		4 hours					n/a	4 hours	n/a	n/a	n/a	n/a	n/a	n/a
Contracted Recovery Point Objective (RPO)					n/a					×	✓	×	×	×	×	×	×
Recovery Point					n/a					n/a	15 mins	n/a	n/a	n/a	n/a	n/a	n/a
Managed By Atos	✓	✓	✓		✓		×	×		✓	✓	✓	✓	✓	✓	✓	✓
DR Test frequency confirmed	✓	✓	✓		✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
DR Tests up to date		✓	✓		✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Last Tested	May-13	Jun-17	##		###		May-17	###		Jun-17	Jun-17	Jun-17	Jun-17	Jun-17	Jun-17	Jun-17	Jun-17
Scheduled Test					###					Jul-18	Jul-18	Jul-18	Jul-18	Jul-18	Jul-18	Jul-18	Jul-18

POL00401626

Disaster Recovery Framework

	Firewall and DDoS	Core network	Wifi	VPN	**Accenture Back Office**	Credence (software)	Core Finance	Financial Management Information	MDM	SAPHR	TransTrack	Automated	POLSAP (Software)	**Accenture CDP**	CDP Web platform	**Atos**	Service Desk	SDM12 (management tool)	**NCR**	Self Service Kiosk
Gold Service (recovery within 5 hours)	✓	✓	✓	✓		✓							✓		✓		✓			
Silver Service (recovery within 24 hours)																		✓		✓
Bronze Service (recovery time within 96 hours)																				
Busines Impact Analysis						✓							✓							
Contracted Recovery Time Objective (RTO)	×	×	×	×		✓	✓	✓	✓	✓	✓	✓	✓		✓		×	×		
Recovery Time	n/a	n/a	n/a	n/a		4 hours	4 hours	4 hours	4 hours	4 hours	4 hours	48 h	4 hours		21.4 hou		n/a	n/a		
Contracted Recovery Point Objective (RPO)	×	×	×	×		✓	✓	✓	✓	✓	✓	✓	✓				×	×		
Recovery Point	n/a	n/a	n/a	n/a		1 hour	1 hour	1 hour	1 hour	1 hour	1 hour	1 ho	1 hour		n/a		n/a	n/a		
Managed By Atos	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓		×
DR Test frequency confirmed	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓					
DR Tests up to date	✓	✓	✓	✓		×	✓	✓	×	×	×	✓	✓		✓					
Last Tested	Jun-17	Jun-17	###	Jun-17			May-17	May-17				###			###					
Scheduled Test	Jul-18	Jul-18	###	Jul-18		Oct 18 (p)	Oct 18 (p)	Oct 18 (p	Oct 18 (	Oct 18 (p)	Oct 18 (p)	Oct	Oct 18 (p)		###					

POL00401626

Disaster Recovery Framework

	Verizon	Branch Network	Voice Services	Mobiles Phones	WAN Service between Data Ce	WAN Service to all Administratio	WAN Service to all Branch Sites	LAN Service for all Administratio	LAN Service for all Branch Sites	Wireless LAN Service for Admin	Gateway Service including Perim	Third Party and business-to-bus	Branch Firewall service	Remote Access Service	Network Access Control	Threat Detection Service
Gold Service (recovery within 5 hours)		✓														
Silver Service (recovery within 24 hours)																
Bronze Service (recovery time within 96 hours)			✓	✓												
Busines Impact Analysis																
Contracted Recovery Time Objective (RTO)		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Recovery Time					1 hour	12 hours	12 hours	12 hours	12 hours	12 hours	1 hour	1 hour	12 hours	4 hours	12 hours	12 hours
Contracted Recovery Point Objective (RPO)		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Recovery Point					15 mins	15 mins	15 mins	15 mins	15 mins	15 mins	15 mins	15 mins	15 mins	15 mins	15 mins	15 mins
Managed By Atos		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DR Test frequency confirmed		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DR Tests up to date		✓	✓													
Last Tested		Feb-17	Feb-17													
Scheduled Test		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*

WAN Service between Data Centres
WAN Service to all Administration Sites
WAN Service to all Branch Sites
LAN Service for all Administration Sites
LAN Service for all Branch Sites
Wireless LAN Service for Administration Sites
Gateway Service including Perimeter security
Third Party and business-to-business Gateway Service including Perimeter security
Branch Firewall service
Remote Access Service
Network Access Control
Threat Detection Service
Voice Service for business Users
Voicemail Service for Corporate Users
Audio Conferencing Service for Corporate Users
Mobile Service for Corporate Users
IVR Service for Contact Centres
Call Routing and ACD Service for Contact Centres
Historic Reporting Service for Contact Centres
Voice Recording Service for Contact Centres
Workforce Management for Contact Centres
Outbound Dialling Service for Contact Centres

POL00401626

Disaster Recovery Framework

	Voice Service for business User	Voicemail Service for Corporate	Audio Conferencing Service for	Mobile Service for Corporate Us	IVR Service for Contact Centres	Call Routing and ACD Service fo	Historic Reporting Service for C	Voice Recording Service for Cor	Workforce Management for Con	Outbound Dialling Service for Co	**Ingenico**	Paystation	**Itron**	Paystation Support	**Moneygram**	Moneygram service	**Qmatic**	Branch Queue System	**Vocalink**	Link Network Switch	**POCA**	Post Office Card Account services Contact centre	Post Office Card Account services Cheque Printing	Post Office Card Account services Banking Engine
Gold Service (recovery within 5 hours)																				✓			✓	✓
Silver Service (recovery within 24 hours)																✓						✓		
Bronze Service (recovery time within 96 hours)												✓		✓				✓						
Busines Impact Analysis																								
Contracted Recovery Time Objective (RTO)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		×						✓		✓		✓	✓	✓
Recovery Time	12 hours	12 hours	12 hours	12 hours	1 hour	1 hour	12 h	12 hours	12 h	12 hours		n/a						4 hours		4 hours		50% 4 hours	2 hours	3 hours
Contracted Recovery Point Objective (RPO)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		×						✓		×				
Recovery Point	15 mins	15 mins	15 mins	15 mins	15 mins	15 mins	15 n	15 mins	15 m	15 mins		n/a						2 hours		n/a				
Managed By Atos	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		×		×		✓		✓		×	×	×
DR Test frequency confirmed	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓						✓		✓		✓	✓	✓
DR Tests up to date												✓								✓		✓	✓	✓
Last Tested												###						Aug-16		Jun-17		Jul-17	Jul-17	Jul-17
Scheduled Test	*	*	*	*	*	*	*	*	*	*		###						Feb-18				May-18	May-18	May-18

POL00401626

Disaster Recovery Framework

	Post Office Card Account services Document Processing
Gold Service (recovery within 5 hours)	
Silver Service (recovery within 24 hours)	
Bronze Service (recovery time within 96 hours)	✓
Busines Impact Analysis	
Contracted Recovery Time Objective (RTO)	✓
Recovery Time	24 hours
Contracted Recovery Point Objective (RPO)	
Recovery Point	
Managed By Atos	✗
DR Test frequency confirmed	✓
DR Tests up to date	✓
Last Tested	Jul-17
Scheduled Test	May-18

POL00401626

Business Continuity & Crisis Management Update

Author: Tim Armit Sponsor: Jane MacLeod Meeting date: 13 March 2018

Executive Summary

Context

Business Continuity capability continues to improve across Post Office. There are gaps across all areas but awareness and levels of ability to respond to incidents is increasing. Levels of resilience and recovery capability is improving in Bolton, Chesterfield, Supply Chain and the Banking Framework.

Questions this paper addresses

- Can the new Business Continuity Policy be approved?
- What is the capability to recover of Post Office key sites?
- How have recent incidents been managed?

Input Sought

The Committee is requested to note the report.

POL00401626

Conclusion

Approval of the updated Business Continuity Policy

1. Attached is a revised Business Continuity Policy, this is primarily a reformatting of the Policy approved last year with a few minor changes. As part of the policy, The Policy should be reviewed and approved annually.
2. The committee is asked to approve the Policy.

What is the current capability of key locations to recover?

1. Post Office has had a contract with SunGard for the provision of work space recovery solutions for a number of years. This contract provides desks, PC's, telephones, network connections, meeting rooms and facilities to Post Office within 3 hours of a major incident and this can be used for up to 3 months. This contract was set to only support Chesterfield and was scaled to lower numbers of staff.
2. The contract is now being upgraded to include doubling the number of desks available for Chesterfield (120 positions) and providing Bolton (50 positions), Bristol (20 positions) and London (20 positions).
3. The SunGard solution requires a fixed VPN link to Post Office systems. This is being implemented in March 2018 and will enable all offices at all SunGard locations to be able to access Post Office systems.
4. Chesterfield will test this solution on March 23rd with staff relocating from the Post Office to the SunGard site to work in a normal manner for a day.
5. Bolton has identified the impacts it could suffer if unable to work and is implementing team based recovery plans. Initial reports show that a 2 day down time would have minimal operational impact, this is to be robustly challenged across the business. Payroll is key but can be mitigated by using last months data at BACS. The SunGard solution for this will be tested by the end of April 2018.
6. Bristol Inventory call centre supports branch orders of cash into Supply Chain. A recovery solution to support this is being implemented in the new contract and will enable the team to relocate and continue to operate.
7. London relies upon home working as its primary recovery solution and this was tested in 2017 and during the recent snow. The 20 positions are to enable crisis management to be controlled and to bring together teams over the following weeks after an incident where groups need to work together.
8. Supply Chain review has been completed and the report is with management for presentation and agreement in April 2018. This has identified a number (154) of challenges and requirements to ensure resilience is in place across the depots. Supply Chain and Business Continuity are now reviewing these to prioritise, assess impact and agree solutions.
9. Banking Framework has worked with Business Continuity to identify risks and impacts of failures in the processes. The cycle of a cheque or cash from customer to reconciliation relies on a number of third party suppliers and now this flow has been captured and detailed the risk in this supply chain can be challenged and the plans in place with third parties confirmed. This report will be reviewed and the next steps to ensure supplier plans are in place will be undertaken by May 2018.

POL00401626

10. The Grapevine invocation of the Post Office crisis management system, called the Business Protection Team continues to improve. This was used quickly during the Verizon call centre failure and regularly across the adverse weather conditions once it was clear there was a significant impact to operations. The calls are focussed, short and effective. The system was not invoked during the explosion in Farnham and the lock out from the London cash centre as the decision was to manage these as operational issues and the impact was at a local level and not across multiple Post Office business areas. This system has now been fully rolled out to POMS and is being implemented across all of Supply Chain.

11. There still remains key IT systems that are vulnerable to being lost in a major incident and IT are aware of these. They include the Swindon based systems to support all warehouse activity and the APOP system in Chesterfield to manage all Payments Out. The data is not secured on these systems and there is no recovery capability. The business owners are aware and are working with IT to develop solutions. This risk has been reported in many forums for over a year and progress to secure the data and implement a recovery solution is critical.

How successful was the management of significant incidents?

12. The adverse weather between February 27th and March 3rd impacted operations across all parts of Post Office. The response from staff was exceptional and the BPT met multiple times each day to report on the situation and manage any areas of risk. Across the period a number of Supply Chain depots were impacted either being closed or having to deliver to only local urban areas. Branches did a tremendous job with only around 200 being closed from 11,500 at the worst periods. Chesterfield call centre and Bristol had to close early on a couple of days but with no visible signs of impact. Mail and Cheques were not collected regularly from many branches, Royal Mail suspended guarantees on Special Delivery and ParcelForce did the same. No POCA issues were reported and no cash outs happened. All staff were reported safe at all times.

13. Verizon Puzzel system failed on February 22nd across the UK failing all Post Office call centres and all other Verizon UK customers. This was down for over 2 hours and Verizon could not determine the root cause. As this happened later in the day the impact was minimal but the failure of operations was total. The BPT worked well to support communications and liaison with IT. IT are working with Verizon to determine how this could happen and why their recovery capability was so poor.

14. There was an explosion in the Farnham branch on March 4th which is believed to be related to appliances in the kitchen. No one was hurt, there was a significant police and media immediate response but once it was found to be an accident this went away very quickly. The branch opened the next day.

15. The London Cash Centre could not be opened on March 5th. A power failure locally defaulted the doors to the site to locked and the manual over ride and generator support did not work. Entry was delayed for a number of hours impacted the delivery to branches on that day. This has happened before and Facilities and Supply Chain are now working urgently with CBRE on a solution.

POL00401626

Appendix 1

Status of progress

Action	*Update*	*Owner*	*Target Date*
Further training and education for the Business Protection Team including improvement of the procedure to invoke the Business Protection Team	Initial changes made to invocation in place. Second workshop planned for April	Tim Armit	4/18
Development and implementation of a recovery strategy for Bolton	Cost for Sungard solution agreed and budget, meeting with Bolton lead team to agree solution being planned for March with a test in April.	Joe Connor / Tim Armit	4/18
Stay Calm manual needs to be simplified and training provided as to its use	Training across Supply Chain depots underway. Agreement to restructure Stay Calm is in place with key users within Supply Chain. Review of documentation complete. Draft new approach out for pilot now, once approach agreed new approach to be rolled out in April. Restructured document in place by year end.	Tim Armit / Marcia Bourne	4/18
Resilience levels across all key locations and facilities needs to be tested, improvements identified and implemented.	Chesterfield solution in place and approach to PC's being reviewed for improvement by IT. Finsbury Dial home working proven in a controlled manner in August 2017 and more realistic exercises will develop from this in the summer of 2018. Supply Chain solutions being reviewed. The levels of resilience will continue to be reviewed whilst plans and strategies are developed across all areas led by Tim Armit but owned by each business lead. This will take until June 2018	Paula Jenner / Tim Armit / Russell Hancock	6/18

Detailed plans across all sites and business areas are in place and can be presented during a deep dive into business continuity capability and status.

POL00401626

Business Continuity Management Policy Review

Approval Sought

Please find attached an updated version of the Business Continuity Policy. This has been approved and implemented in previous year and should be reviewed and re-approved annually, this is what is required.

The policy has been transferred to the new Post Office policy template and slightly simplified but with no other material changes.

The key approach steps are taken directly from the ISO Standard and ensures we are working to best practice and that when challenged by customers or suppliers we can demonstrate an approach which meets their expectations.

Within Post Office at this time the current status against the policy is shown at a high level below:

- The impact on the business areas of IT systems failing has been completed.
- Impact analysis of Bolton operations has been completed for a first review.
- Impact analysis on Chesterfield has been completed for a first review.
- Impact analysis on LRG operations has been completed for a first review.
- Banking Framework processes impact on supplier failure has been completed for first review. Suppliers must now be challenged by Banking to prove their recovery capability meets Post Office requirements.
- Risk analysis on all key locations has been completed by CBRE
- Current status of recovery strategies and recovery capability for Supply Chain has been completed for first review. Key risks in terms of Swindon and contingency strategies for depots are to be worked through.
- Incident management processes are in place and proven within the BPT approach.
- BPT training has been completed.
- Initial Gold Team training has been completed.
- Testing of Chesterfield has been completed and is planned again for March 2018
- Testing for Bolton is planned for April
- Working from home test for Finsbury Dials has been undertaken
- A recovery capability for Bristol, Chesterfield, Bolton and London is being implemented with Sungard

All work is being managed against the Policy approach. A wide scope has been undertaken to run multiple stream projects across many areas of Post Office simultaneously to reduce the risk many areas are exposed to.

The aim is for you to please approve the attached policy.

Tim Armit

Business Continuity Manager

POL00401626



Business Continuity Management Policy

Version – V2.2

DRAFT

POL00401626

1 Overview 3
1.1 Introduction by the Policy Owner 3
1.2 Purpose 3
1.3 Core Principles 3
1.4 Business Continuity Objectives 4
1.5 Application 4
1.6 The Risk 4
1.7 Legislation 5
1.8 Industry Guidance 5
2 Risk Appetite and Minimum Control Standards 6
2.1 Risk Appetite 6
2.2 Policy Framework 7
2.3 Who must comply? 7
2.4 Minimum Control Standards 8
2.4.1 Threats 11
2.4.2 Approach 11
2.5 Implementation 12
2.5.1 Satisfying BCMS Requirements 12
3 Tools & Definitions 14
3.1 Tools 14
3.2 Definitions 14
4 Where to go for help 15
4.1 Additional Policies 15
4.2 How to raise a concern 15
4.3 Who to contact for more information 15
5 Governance 16
5.1 Governance Responsibilities 16
6 Control 17
6.1 Policy Version 17
6.2 Policy Approval 17

DRAFT

POL00401626

1 Overview

1.1 Introduction by the Policy Owner

The Business Continuity Manager has overall accountability to the Board of Directors for the design and implementation of controls to prevent or deter failures in normal operations. The Business Continuity Management Policy details the approach to implementing strategies and plans to minimise the impact to operations and restore operations in a time to meet business requirements. This approach ensures the risks to operations are known, the impact to operations of failure are understood and recovery priorities are based upon the tolerance to impact. The Policy is an agenda item for the Audit and Risk Committee and the Post Office board is updated as required.

1.2 Purpose

This Policy has been established to set the minimum operating standards relating to the management of the Business Continuity risks. It is one of a set of policies which provide a clear risk and governance framework and an effective system of internal control for the management of risk and continuity of operations across the group. Compliance with these policies supports the Group in meeting its business objectives and to balance the needs of shareholders, employees and other stakeholders.

1.3 Core Principles

Post Office adopts the Business Continuity Institute's Good Practice Guidelines definition of business continuity as: "A holistic management process that identifies potential threats to an organisation, and the impacts to business operation those threats, if realised, might cause, and provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities."

This Policy is consistent with "ISO22301", which is the Business Continuity International Standard. The purpose is to define the Group's policy with regard to business continuity management that is appropriate to its aims and objectives. This includes a framework for:

- setting business continuity objectives;
- satisfying appropriate legal, regulatory and contractual requirements;
- continual improvement of the Business Continuity Management System ('BCMS'); and
- key controls in respect of business continuity.

This policy should also be read in conjunction with other Post Office resilience, health & safety, and physical security related policies and procedures.

DRAFT

POL00401626

The following areas of Post Office's business are within the scope of the policy:

- All customer support centres including but not limited to, Finsbury Dials, Chesterfield and Bolton office
- All Supply Chain Locations
- All Directly Managed Branches
- All other Post Office Operational centres
- All external/outsourced Supply Chain Capability.

Out of Scope of this Policy:

- All IT systems – these are covered within the ITDR Policy

This policy's effective date will be determined by the date on which final approval is given by the appropriate governance forum

1.4 Business Continuity Objectives

Based on the requirements and factors set out in this document, the following major objectives are set for business continuity:

- Objective 1 - Comply with health and safety legislation at all times
- Objective 2 – Maintain stakeholder confidence
- Objective 3 – Maintain customer service levels
- Objective 4 – Minimise loss of revenue

The success of the BCMS will be judged on its ability to meet these overall objectives.

1.5 Application

This Policy is applicable to all areas within the Group and defines the minimum standards to control financial loss, customer impact, regulatory breaches and reputational damage in line with the Group's Risk Appetite.

The risk to the Group from Business Continuity is reviewed by the board annually.

1.6 The Risk

The Business Continuity Policy is designed to help mitigate the risk that normal operations are interrupted and not restored in a controlled and timely manner with the consequence that:

- staff and Customers safety is at risk;
- customers are unable to be served;
- regulatory requirements are not met;
- legal and contractual breaches occur;
- income is affected; and
- confidence in the Post Office's reputation is harmed.

POL00401626

1.7 Legislation

The Group is subject to a variety of legal and regulatory requirements which either apply directly or are imposed through contractual arrangements with key clients. These include, but are not limited to:

- Health and Safety legislation;
- Payment Card Industry – Data Security Standard compliance;
- Financial Services legislation;
- National and international standards e.g. ISO9001; ISO270001; and
- Consumer protection legislation.

1.8 Industry Guidance

ISO22301 is the accepted International Standard for Business Continuity. There are other Standards on Operational Risk, Information Security, Crisis Management and IT Disaster Recovery.

The Business Continuity Institute issues good practice guidelines

The FCA issues best practice guidelines

DRAFT

POL00401626

2 Risk Appetite and Minimum Control Standards

2.1 Risk Appetite

The following risk appetite statements are relevant to Business Continuity:

> ***Averse*** appetite for taking risks which might result in failure to maintain the service commitment in respect of customers in line with our social purpose and Government's policy on subsidy**.**
>
> ***Neutral*** risk appetite for dissatisfaction related to BAU services recognising that in a complex business there will be a level of dissatisfaction as part of the normal course of business of achieving our commercial objectives.
>
> ***Averse*** appetite for risk taking which would alienate or lose significant groups of profitable customers
>
> ***Tolerant*** risk appetite for customer dissatisfaction caused by transformation, innovation and customer selection/profitability decisions.
>
> ***Neutral*** appetite for risk taking which would have a detrimental impact on vulnerable customers. Post Office will take a balanced view, reflecting commercial implications of introducing safeguards and controls to protect vulnerable customers and the needs of those customers.

Post Office takes its legal and regulatory responsibilities seriously and consequently has:

> ***Tolerant*** risk appetite for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality
>
> ***Averse*** risk appetite for not complying with law and regulations or deviation from business' conduct standards
>
> ***Averse*** risk appetite for unethical behaviour including staff Misfeasance, failure of, governance and control processes, critical financial reporting processes, critical supply chain and business continuity processes.

Post Office is committed to safeguarding the wellbeing of its people and therefore has:

> ***Averse*** risk appetite associated to the health, safety and wellbeing of POL customers and colleagues in everything we do. This is paramount to every aspect of POL operation. This includes; loss of life, serious injury and non-compliance to regulation and policy

DRAFT

POL00401626

Post Office is committed to exploiting technological benefits to achieve market advantage. In recognition of this, Post Office has:

> ***Averse*** appetite for data loss/leakage that can lead to customer, commercial or reputational damage
>
> ***Neutral*** appetite for operational IT services
>
> ***Averse*** risk appetite for any serious impact to the confidentiality, integrity and availability of information, leading to financial loss, business disruption, public embarrassment or legal consequences.

Post Office recognises that it cannot completely eliminate business continuity risks. However, this policy sets out controls to reduce and/ or mitigate such risks.

This level of risk appetite will be applied to the risk assessments that are carried out as part of the BCMS and will determine the actions that need to be taken to mitigate risk to an acceptable degree.

2.2 Policy Framework

Post Office has established a suite of resilience and risk policies, on a risk sensitive approach which are subject to regular review. Other policies which may be relevant to business continuity include the following:

- IT Disaster Recovery
- Information Security
- Data protection

2.3 Who must comply?

Compliance with this Policy is mandatory for all Post Office employees and applies wherever the Group's business is undertaken. All third parties who do business with the Group, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this Policy with their own equivalent Policy.

Where non-compliance is identified the matter must be referred to the Director of Risk and Compliance and the Group Legal Director. Any investigations will be carried out in accordance with the Investigations Policy. Where is it identified that that an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary offence.

The next page sets out the minimum control standards that the Group has implemented to control these risks.

DRAFT

POL00401626

2.4 Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
All	BCMS is not fit for purpose.	Annual review of the BCMS content and effectiveness. Internal Audit review	Business Continuity Manager Audit Manager	Annually
All	Risks the business and locations are exposed to are not known or are inadequately mitigated.	ISO22301 defines managing Business Continuity risks to include an assessment of : • Threats; • Vulnerabilities; • Impact & likelihood before risk treatment; • Risk treatment (e.g. reduction, removal, transfer); • Function responsible/ owner; and • Timescale and review frequency.	Business Continuity Manager. IT DR Manager. Facilities Manager. Location PICS. Business Leads.	Annually
All	The impact on operations of a business continuity incident is not clearly understood.	Impact is measured against agreed metrics and agreed times to ensure business areas can be compared and strategies implemented which are compatible with the risk and impact the operational area is exposed to.	Business Continuity Manager. Business Leads	Every two years or on change.

DRAFT

Post Office Limited Risk and Compliance Committee-13/03/18

POL00401626

All	Recovery strategies do not meet business needs	Annual tests of strategies in place to ensure business has confidence and understanding in the capability	Business Continuity Manager All business leads	Annually
All	Contingency plans are not in place or available.	Plans in place must be assessed by internal audit and annually the status presented to the RCC. Plans must be held by all managers and available in a single accessible repository.	All business leads Business Continuity Manager	Annually
BPT	BPT does not know the process to respond to a crisis	All BPT members are contacted and involved in crisis conference calls and undergo training.	Business Continuity Manager BPT members	Twice yearly
All	Staff are unaware of how to respond to a crisis	All staff are briefed and made aware of their responsibilities	Business Continuity Manager All business leads	Ongoing
Building unavailable	Any key operational site may become unavailable for its purpose.	Risk assessments of sites are carried out annually by CBRE and POL. Strategies for the recovery of key operations per site are in place and annually tested.	Business Lead. Facilities Manager. Business Continuity Manager.	Annually. Upon moving in.
IT system failure	Any IT system can fail at any time.	This is managed under the IT DR policy and the IT COBIT process. All systems are documented and the impact of them failing documented. Resilient and DR capability is in place and managed by IT. This is tested annually.	CIO IT DR lead Business Leads Business Continuity Manager	Annually. Upon Change. Upon implementation
Supply Chain distribution failures	Depots, Vans and operations may fail leading to routes and deliveries and collections not meeting business needs.	Plans and strategies to mitigate failures are in place and tested. Contingency planning for the loss of all forms of assets are tested.	Supply Chain lead Depot Leads Business Continuity Manager	Annually
Outsourced or supplier failure	Post Office relies heavily on suppliers and outsourcing to achieve its day to day operations. Any of these could fail or go out of business.	Part of the contract allocation and contract management covers business continuity. All suppliers commit to meet business continuity requirements and to test these. Contracts must contain appropriate BC and DR capability statements. Suppliers should demonstrate their recovery capability before a contract is signed, on review of the contract and if necessarily post any incident that	Contract owner. Area dependent on contract. Business Continuity Manager. IT DR manager	Annually

POL00401626

		affects them. Capability to restore operations in stated timeframes must be tested annually by all key suppliers. Suppliers to be categorised according to the risk their failure presents to Post Office. Many key suppliers will be within IT and the business consequence of an IT supplier failing must be shown to be mitigated by IT DR tests within these suppliers.		
Staff unavailable	Post Office staff are the key to the success of operations. At any time due to weather, health or any scenario staff may be unable to work.	Identification of single point of failure staff is undertaken within the contingency planning. Key roles must be documented and where possible dual role training undertaken. As a working example the dependency on skilled drivers is key to supply chain and this is mitigated by the Rapid Response Team when required.	All business leads. HR leads Business Continuity Manager.	Ongoing.

DRAFT

POL00401626

2.4.1 Threats

Post Office plans for the worst case scenario and does not work to specific threats unless they are beyond the scope of the risks planned for. Threats continue to vary and these will be used to define scenarios for exercises. Threats include:

- Weather related events
- Infrastructure failure
- Pandemic
- Cybercrime
- Environmental disasters
- Terrorism
- Industrial Action

2.4.2 Approach

In the approach to implementing, managing and reviewing business continuity capability the Post Office will:

- Create a Business Continuity Management System in line with ISO Standards showing the detailed approach to implementing and managing business continuity;
- Complete Risk and Impact assessments of tangible and intangible losses. To include an understanding of contractual and regulatory obligations, potential causes of risks, and impact of events both in terms of direct financial loss, cash flow interruption, customer impact, operational consequences, reputational impact and legal/regulatory impact. These assessments allow prioritisation of time and resource to implement recovery solutions;
- Develop and document strategies and plans to address key risks;
- Implement plans and recovery strategies (eg resilient IT, offsite recovery locations etc);
- Manage the central and local storage of plans;
- Annually (or more frequently) review plans;
- Consider impact of change activity on plans as part of major change activity;
- Create, manage and facilitate Post Office crisis response;
- Report all incidents and their impact;
- Test all strategies to ensure they meet business requirements;
- Integrate with IT recovery capability to ensure it meets business requirements;
- Train staff in the contingency plans and their roles and responsibilities;
- Complete root cause analysis when there is a (material) incident and review the control framework to include 'lessons learned';
- Embed appropriate and proportionate contractual requirements in contracts with suppliers and outsourcers including reporting, audit and rectification rights;
- Ensure there is regular oversight/testing of supplier and outsourcer obligations;
- Report twice yearly on progress against these approach steps.

DRAFT

POL00401626

2.5 Implementation

The approach to implement business continuity within Post Office are defined within this Policy. These are the fundamental steps required which are led by business areas, facilitated by the Business Continuity Manager and are not subject to frequent change. The Post Office GE will ensure that adequate funding is available for activities identified in the implementation and ongoing support of the business continuity process.

Amendments to the Business Continuity objectives will be managed through the standard Post Office change management process if required.

2.5.1 Satisfying BCMS Requirements

Senior Managers commit to the provision of the appropriate resources to establish and maintain the BCMS and its outputs.

Regular review of the BCMS. This is conducted by the Business Continuity Manager on an annual basis, ensuring that objectives are being met. Evaluation of the current capability is undertaken and any issues identified through this audit programme and management processes are reported to the RCC. Management review includes departmental and other management meetings and document review.

Role definition and responsibilities are defined in the BCMS and reviewed by the Business Continuity Manager to ensure that colleagues understand the roles they are required to fulfil, and that they have the appropriate skills and competences to do so. These controls are necessary to ensure the continued BCMP success and to mitigate risk. Training will be provided where gaps in competency are identified and regular reviews of staff capability will be undertaken within departmental exercises.

Use of third parties. Post Office uses third parties, both internal and external, in the delivery of products and services. The ability to continue to provide these services or restore them should a supplier fail is key to Post Office operations and part of all contracts. This supplier capability will be evidenced by documentation and records, including contracts, meeting minutes and IT DR and BC test reports.

Continual improvement:

To ensure the approach to implementing and managing the BCMS is enhanced in an ongoing manner Post Office will:

- Consider effectiveness of the BCMS across all business areas and end to end systems, processes within scope;
- Enhance current processes to bring them in to line with best practice (as defined within ISO 22301);
- Increase the level of proactive continuity planning across Post Office;

POL00401626

- Achieve an enhanced understanding of and relationship with the business units to which the BCMS applies;
- Review relevant metrics (impacts, risk etc) on an annual basis to assess their appropriateness, or to make changes to them based on collected historical data and feedback or in response to incidents;
- Obtain ideas for improvement via regular review meetings with stakeholders.

Ideas for improvement may be obtained from any source, including but not restricted to: Customers; Suppliers; Colleagues; Risk Assessments & Audits.

In order to evaluate any proposed improvements to the BCMP, the following criteria would be applied:

- Cost;
- Business benefit;
- Risk;
- Implementation timescale; and
- Resource requirement.

Accepted improvement proposals will be prioritised, and planned according to standard project management principals.

DRAFT

POL00401626

3 Tools & Definitions

3.1 Tools

None in place

3.2 Definitions

Term or Acronym	Description
BCMS	Business Continuity Management System, the set of controls in line with ISO22301 to implement and manage business continuity
BC	Business Continuity
ITDR	IT Disaster Recovery, the recovery of IT systems and data
ISO 22301	The International Standard for Societal Security (Business Continuity).

DRAFT

POL00401626

4 Where to go for help

4.1 Additional Policies

This Policy is one of a set of policies. The full set of policies can be found at:

https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx

4.2 How to raise a concern

Any Post Office employee who has concerns about a failure to comply with this policy has a duty to:

- discuss the matter fully with their Line Manager; or,
- discuss it directly with their Head of Business Unit; or,
- Report their suspicions by telephoning Grapevine on GRO
- If either or both are not available, staff can contact the Post Office's General Counsel, who can be contacted by email at: whistleblowing GRO or by telephone on: GRO.
- Alternatively staff can use the Speak Up service available on GRO
- or via a secure on-line web portal: http://www.intouchfeedback.com/postoffice

Post Office encourages members of the public or people not employed by us who suspect [activity in breach of policy] to write, in confidence, to the Chief Executive's Office, Finsbury Dials, 20 Finsbury St, London EC2 9AQ.

4.3 Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact Tim Armit – Business Continuity Manager by email at GRO

DRAFT

POL00401626

5 Governance

5.1 Governance Responsibilities

Post Office's Board of Directors have overall responsibility for ensuring that Post Office has a framework to ensure compliance with legal, regulatory and contractual requirements. The Board is kept abreast of relevant matters relating to the management of business continuity by reports from its committees including its ARC Committee. The key individuals and their specific responsibilities in relation to this policy are:

- The General Counsel is a member of the Post Office Executive team and is the Group Executive Owner and Policy Sponsor, accountable to the Board.
- The Group Business Continuity Manager is the Policy Owner who is responsible for:
    - day to day implementation of and compliance with this policy and is accountable in this regard to the General Counsel;
    - ensuring that there is an annual review of this Policy and tests compliance across the Group.
    - providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee.

Post Office's internal systems of business continuity risk control ensure that controls are regularly independently assessed for effectiveness, suitability and adequacy. In addition, Internal Audit will periodically test compliance with this policy.

DRAFT

POL00401626

6 Control

6.1 Policy Version

Date	Version	Updated by	Change Details
19th May 2016	1.0	Jon Waples	First signed version
25th Feb 2018	2.0	Tim Armit	For review and signature

6.2 Policy Approval

Group Oversight Committee: Risk and Compliance Committee and Audit and Risk Committee

Committee	Date Approved
POL R&CC	
POMS R&CC	
POL ARC	
POMS ARC	

Policy Sponsor: Jane Macleod

Policy Owner: Tim Armit

Policy Author: Tim Armit

Next review: *date of next review 01 02 2019*

DRAFT

Company Details

Post Office Limited and Post Office Management Services Limited are registered in England and Wales. Registered numbers 2154540 and 08459718 respectively. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.

Post Office Management Services Limited is authorised and regulated by the Financial Conduct Authority (FCA), FRN 630318. Its Information Commissioners Office registration number is ZA090585.

Post Office Limited is authorised and regulated by Her Majesty's Revenue and Customs (HMRC), REF 12137104. Its Information Commissioners Office registration number is Z4866081.

POL00401626

Analysis of performance of RCC against requirements

Verbatim Extracts from TOR		Meeting Dates & topics of papers reviewed					
Responsibilities -		**May-17**	**July-17**	**Sep-17**	**Nov-17**	**Jan-18**	**Mar-18**
Risk Management Framework							
a. Review the effectiveness of the risk management framework and maintain oversight of the development and implementation of the components of the risk management framework.		Supply Chain pilot of the Placemat; Business Continuity and Crisis Management update;	LRG Placemat; Risk Incidents;	LRG Placemat; Finance & Operations Placemat;	Risk Placemat	Risk Update	Risk Placemat
b. Maintain oversight of the current risk exposures of Post Office and advise on future risk strategy.		Top Risks & Risk Appetite for the ARA.					
c. Review the identification and effective management of current key risks and identified mitigating actions and regular reviews of emerging risks.			JML update; DR Testing of IT systems;			EUM Update; SuccessFactors Update; Joiners, Movers and Leavers; GDPR Update;	GDPR Programme Update;

POL00401626

Verbatim Extracts from TOR		Meeting Dates & topics of papers reviewed					
Responsibilities -		**May-17**	**July-17**	**Sep-17**	**Nov-17**	**Jan-18**	**Mar-18**
d. Consider and review areas of risk, which should include, but is not limited to, sufficient coverage of: (see i. – ix. in Terms of Reference)		IT Controls; Financial Controls; Financial Crime; FS Conduct; Health and Safety; Transformation.	FS Conduct Risk; Change Risk; Financial Crime; Annual Gifts & Hospitality Report; IT Controls & IT Tube Map; Finance Controls; Health and Safety; Business Continuity; DR Testing of IT systems;	FS Conduct; Change; Financial Crime; IT Controls Framework & DR; Finance Controls; Business Continuity	FS Conduct; Change; Financial Crime (including G & H update); IT Controls Framework; Financial Reporting Controls; Business Continuity	FS Conduct; Change; Financial Crime; IT Controls Framework; Financial Reporting Controls; Business Continuity; Health and Safety; Information Protection and Assurance	Financial Reporting Controls; FS Conduct Risk Update; Change; Financial Crime Risk Update; Product Risk: Gift Card; IT Risk Management Update; IT Risk Transformation Programme Update; Cyber Security & Information Assurance Update
e. Receive and review risk reports from the following management Sub-Committees: i. Transformation ii. Information Security iii. Security iv. Business Continuity		Business Continuity and Crisis Management update; Transformation;	Change Risk; Business Continuity;	Change; Business Continuity;	Change; Business Continuity;	Change; Business Continuity; Information Protection and Assurance;	Change; Business Continuity Planning;
The Committee will receive and review the draft annual risk management plan for onward reporting to the Board Audit, Risk and Compliance Committee.							

POL00401626

Verbatim Extracts from TOR		Meeting Dates & topics of papers reviewed					
Responsibilities -		**May-17**	**July-17**	**Sep-17**	**Nov-17**	**Jan-18**	**Mar-18**
The Committee will receive and review the draft annual internal audit plan for onward reporting to the Board Audit, Risk and Compliance Committee.							Audit Plan 2018/19
Internal Controls and Assurance							
a. Consider and review the adequacy of the Company's internal controls and make recommendations for the improvement of the Company's internal controls, processes and systems.		IT Controls; Financial Controls	IT Controls & IT Tube Map; Finance Controls	Camelot lessons learned; IT Controls Framework & DR; Finance Controls;	IT Controls Framework; Financial Reporting Controls;	IT Controls Framework; Financial Reporting Controls;	Financial Reporting Controls
b. Monitor the implementation of key recommendations and management action plans.		Internal audit report;	Internal audit report;	Internal audit report;	Internal audit report;	Internal audit report;	Internal audit report;
c. Review the adequacy of policy governance and recommend changes.			Vulnerable Customers; Financial Crime; Anti-Bribery and Corruption; Protecting	AML & CTF; Whistleblowing; Data Protection; Code of Business Standards	Acceptable Use Policy; Cyber and Information Security Policy;	Supplier Relationship Management;	Business Continuity Policy; Treasury Risk Management Framework, Policies and

POL00401626

Verbatim Extracts from TOR		Meeting Dates & topics of papers reviewed					
Responsibilities -		**May-17**	**July-17**	**Sep-17**	**Nov-17**	**Jan-18**	**Mar-18**
			Personal Data; Code of Business Standards				Authorities; Document Retention and Disposal Policy; IT Security Policy
Fraud, Theft and Ethics							
a. Review with management their fraud assessment, detection measures and their investigation of illegal acts, as appropriate.		Identity Fraud Incident Report; Financial Crime;	Financial Crime;	Financial Crime;	Financial Crime;	Financial Crime;	Financial Crime;
b. Review any summary of frauds, thefts and other irregularities of any size.		Identity Fraud Incident Report;					
c. Review with the internal auditors the results of any review of the compliance with the Company's codes of ethical conduct and similar policies including whistleblowing.		Whistleblowing Report;	Annual Gifts & Hospitality Report;		Financial Crime (including G & H update);		
Compliance							

POL00401626

Verbatim Extracts from TOR		Meeting Dates & topics of papers reviewed					
Responsibilities -		**May-17**	**July-17**	**Sep-17**	**Nov-17**	**Jan-18**	**Mar-18**
The Committee will monitor compliance with legal and regulatory obligations, including any significant breaches.		Horizon Scan; Modern Slavery Act; Whistleblowing Report; Identity Fraud Incident Report.		Regulatory Framework; Procurement Compliance reporting; Criminal Finances Act; Horizon Scan	Procurement; Criminal Finances Act;	Procurement; Tax Update; Annual Legal Risk Report; Legal and Regulatory Horizon Scanning;	Legal and Regulatory Horizon Scanning; Compliance with Payment Card Industry Data Security Standards; Procurement Compliance Reporting;

POL00401626

RCC 18/1– 18/12

POST OFFICE MANAGEMENT SERVICES LIMITED (Company)
RISK, COMPLIANCE AND CONDUCT COMMITTEE (RCCC)
(A committee of the Executive)

Minutes of an RCCC meeting held at
Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ
On 31 January 2018 at 10.30am – 12.00pm

Present:	Ian Holloway (Chair)	POMS Risk and Compliance Director
	Russell Tavener (RT)	Chief Operations Officer
	Stephen Gaines (SG)	POMS Compliance Manager
	Nick McCowan (NM)	Head of General Insurance
	Sanjeeve Thakrar (ST)	Risk Manager
	Alberto Zannatta (AZ)	Audit Manager Corporate Services
	Jules Harris (JH)	Head of IPA
	Sally Smith (SS)	Head of Financial Crime
	Renata Prywerek (PK)	Legal Counsel
	Michael Brown (MB)	Deputy for Head of Commercial
	Elizabeth McMenemy (EM)	Compliance Advisor
	Dan Tremain (DT)	Senior Product Manager Life
	Ann Young (AY)	Compliance Advisor
Apologies:	Beverley Turner (BT)	Senior Product Manager GI
	Francisco Couto (FC)	Head of FS Legal
	Ryan Griffin (RG)	Head of Protection
	Gill Craig (GC)	Deputy for Head of Travel
	Paul Paddock (PP)	Head of Travel
	Ehtsham Ali (EA)	Senior Compliance Manager IPA

RCCC 18/1 **WELCOME, QUORUM AND CONFLICTS OF INTEREST**

(a) The Chairman declared the meeting quorate and open. The Chairman extended a welcome to all persons attending the RCCC meeting for the first time.

RCCC18/2 **MINUTES OF THE MEETING HELD ON 19 December 2017**

(a) The minutes of the meeting held on 19 December 2017 were approved and the Chairman was authorised to sign them as a true record of the meeting.

.

RCCC 18/3 **RISK AND INCIDENT MANAGEMENT**

(a) ST confirmed that there were no reportable incidents recorded in December.

(b) ST confirmed that there were 82 items on the EXCO risk dashboard, 5 of which were outside of appetite

- AR – IH confirmed that there was a framework now in place to address the concerns and that the AR risk is expected to be within appetite by the end of the year
- Strategy – Business plan. There is a meeting scheduled and an

POL00401626

update to be provided at the next meeting

- Duck Creek reconciliation - Finance are working with change to spec out controls re premium flows. Currently 6 new controls and reconciliations have been identified of which internal consistency (billing to policy) & understanding how network cash can be reconciled are priorities.
- Marketing lack of infrastructure - Recommendation for CVM pilot being scoped for approval including data, communications and capability.
- Marketing lack of resource -Recruitment of additional 10 POMS dedicated staff to sit within central marketing structure.

(c) GDPR project was discussed and IH confirmed that the delivery date for GDPR is 9 February. This is to ensure that relevant documentation is produced.

RCCC 18/4

1st LINE COMPLIANCE REPORT

(a) MB confirmed the overall trend for December was generally positive. The upheld rate for complaints remains high with Claims related complaints still the top category. Root cause analysis has been provided by Collinson and will be reviewed. POMS will be looking the timeline and the products

(b) The £50 promotional vouchers remain the top category for Life. Q4 Life protection marketing campaign went live on 8th January 2018 and will run to the 31 March 2018. It is anticipated that changes to the way the customer incentive is positioned will lead to a reduction in the number of complaints relating to customer incentives particularly in branches. Complaints volumes will be monitored throughout the campaign. POMS to review processes around customer eligibility and mailing of gift vouchers.

Action MB

(c) MB will provide an update/ paper for the next Committee on the actions being taken to reduce the volume of complaints being received in respect of the Life voucher offer.

2nd LINE COMPLIANCE REPORT

RCCC18/5

(a) IH provided an update on the compliance monitoring completed in the branch network. Where issues are identified at branch level via mystery shopping or branch review clear local actions are developed and tracked to completion. However processes to ensure that systemic trends are managed across the network currently require further enhancement. For example, branch based reviews often identify incomplete travel application forms and a network wide action plan is required to ensure that this issue is addressed. The need for clear, time bound actions with clear accountabilities to address systemic issues has been raised with the Network Management. A summary of current systemic issues has also been provided. A response has been requested by 15 February 2018

(b) EM provided an update on the Quality Monitoring undertaken in Webhelp and the variances found. There were five variances in which there could have been customer detriment. EM confirmed that the

POL00401626

customers had been contacted in all instances.

Action RT

(c) RT asked if the new scorecard had been introduced in Webhelp and EM confirmed that it had not. RT will arrange for a discussion with SG, Nichola Hazard and EM.

RCCC18/6

ASSURANCE ACTIVITY

(a) RT confirmed that all the queries raised from the Collinson audit had been answered.

(b) RT confirmed that a Devitts' complaints audit was currently underway.

(c) RT advised that the Assurance Calendar for supplier audits is ready to be shared.

(d) ST confirmed that the Compliance Monitoring plan will presented to the RCCC prior to submission and approval at the ARC.

(e) AZ advised that the Change Management review would be starting next week.

Action AZ

(f) AZ also confirmed that there is to be a review on the progress of the GDPR project. IH requested an early draft of the review.

RCCC 18/7

POLICIES AND PROCEDURES

(a) SG confirmed that an updated Compliance Manual is to be issued.

(b) ST is looking at all the POL and POMS procedures.

(c) SS reminded the meeting that all gifts and hospitality either given or received must be recorded including the gifts that are declined.

Action NC

(d) NC confirmed that a price change governance report is to be presented to the RCCC.

RCCC18/8

FINANCIAL CRIME

(a) SS confirmed that the annual training draft must be completed by Feb 28. SS also advised the meeting that last year 22 branches were switched off for failing to complete their training and to date 8 branches remain "switched off".

(b) SS advised that due to new fit and proper regulation, there would be a more rigid approach will be adopted and branches will be switched off if it is decided that the branch cannot demonstrate evidence that it complies with the fit and proper regulation.

(c) SS also advised that they would be looking at the training currently provided and ensuring that the questions are more appropriate.

RCCC18/9

INFORMATION PROTECTION & ASSURANCE

(a) Hexaware SMP document, JH advised that they are looking to baseline

POL00401626

this document with Hexaware over the coming days and then proceed to arranging an assessment of the controls Hexaware have in place.

(b) POMS PCI compliance are planning sign a contract with Global Pay this will bring them out of the current PCI certification with Post Office.

(c) The number of Cyber Attacks doubled in 2017* named as the worst year ever for data breaches and cyber incidents worldwide. Key points from report are:

- Ransomware led the way in terms of the form of attack
- Ransomware doubled in the last year to 160K
- 93% of the breaches could have been avoided using simple basic IT Hygiene.

* According to Online Trust Alliance

RCCC 18/10

INTERNAL AUDIT

(a) AZ confirmed that there were currently 8 internal audit actions open for POMS. 5 actions are recorded for Compliance and RT has 3 actions

(b) The internal audits in progress are as follows

- Travel insurance –Assessment of control framework – Reporting Phase
- MI Discover Phase- Fieldwork started
- Change Management Process – Starting 5th Feb
- Readiness to European GDPR – Planning phase

RCC18/11 **OUTSTANDING ACTIONS LIST**

(a) **Action 17/77 (b)** Home claim report – RT is to continue to ask for clarity on the Home Claim report produced by Junction RT confirmed that IC will produce this report **–Open**

(b) **Action 17/93 (d)** Repudiated claim on Home Insurance. BT confirmed that she has asked Junction to provide further information - **Open**

(c) **Action 17/95 (b)** TIF Audit – RT confirmed that TIF are open to POMS conducting a review but are resistant to the use of a third party to conduct the review. RT further confirmed that following the Quarterly Business review RT would be looking to instigate formal actions or sanctions if this is not resolved. RT confirmed that TIF may allow an audit but are still insisting that it is not done by a third party– **Open**

(d) **Action 17/99 (a)** IDD – IH confirmed that he will provide a fuller update in Jan 2018. A brief update was provide to the meeting. There is continued pressure on the Network to provide IDD training for the sales force. IH is reasonably confident that the deadlines will be met. There will be a greater focus on Travel insurance. There is focus on the training record keeping and there will be a manual process until EUM commences in July. The records should be electronically stores by Feb 2019. There is will an update in March 2018 **Open**

POL00401626

RCCC 18/12 **ANY OTHER BUSINESS**

(a) SG asked if there was any monitoring being completed on the new Easy Life sales. DT confirmed that all the sales will be monitored by FSRisk by FAD and will ensure that sales are completed by branches who have been trained

(b) There was no other business raised. There being no further business the meeting was closed.

(c) The next meeting of the RCC will be held on 28 February 2018 at 14.00 pm.

Chairman. **Ian Holloway** ..... Date 6/03/18

POL00401626