POL00401625

Post Office Risk and Compliance Committee Agenda

Date	
20 July 2017	
Start Time	**Finish Time**
13.00	16.00
Location	
Room 0.03 Moorgate	

Present	In Attendance		Apologies
Jane MacLeod(Chair)	Elena Nistor	Tim Armit	Kevin Gilliland
Paula Vennells	Richard Williams	Martin Hopcroft	Johann Appel
Al Cameron	Amanda Radford	Sally Smith	
Martin Kirke	Georgina Blair	James Dingwall	
Alwen Lyons	Adnan Killedar	Chris Russell	
Rob Houghton	Deana Herley	Mick Mitchell	
Nick Kennett	Jonathan Hill	Rebecca Barker	
Martin Edwards	Jenny Ellwood		
Mark Davies	Roger Gale		

Agenda Item		Action Needed	For ARC	Purpose	Lead	Time
1.	**Welcome, introduction & 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 4th May and update on actions inc. i. JML update ii. Update on previous IA report on JML iii. Update on data cleanse activities to underpin regulatory training	Chair	
3.	**Key Operational Risks**	Discussion & approval	✓	To review the management of key operational risks.		13.05 – 14.55 (110 minutes)
	3.1 FS Conduct Risk				Jono Hill	
	3.2 Change Risk				Jenny Ellwood	
	3.3 Financial Crime				Sally Smith	
	3.4 Annual Gifts & Hospitality Report				Sally Smith	
	3.5 IT Controls & IT Tube Map				Rob Houghton	
	3.6 Finance Controls				Amanda Radford	

Post Office Audit, Risk and Compliance Committee Agenda (cont.)

Agenda Item		Action Needed	For ARC	Purpose	Lead	Time
3. cont .	**3.7** Health and Safety **3.8** Business Continuity **3.9** DR Testing of IT systems	Discussion & approval	✓	To review the management of key operational risks.	Martin Hopcroft Tim Armit Mick Mitchell	13.05 – 14.55 (110 minutes)
	BREAK					14.55 – 15.05 (10 minutes)
4.	**Risk** **4.1** LRG Placemat **4.2** Risk Incidents	Questions & Noting	✓	To note LRG placemat, progress to date with the Finance and Operations Placemat and recommendation for further rollout of placemat.	Deana Herley/ Richard Williams	15.05 – 15.25 (20 minutes)
5.	**Audit** **5.1** Internal audit report	Questions & noting	✓	To note the Internal Audit Report and lessons learned	Elena Nistor	15.25 – 15.35 (10 minutes)
6.	**Policies** **6.1** Vulnerable Customers **6.2** Financial Crime **6.3** Anti-Bribery and Corruption **6.4** Protecting Personal Data **6.5** Code of Business Standards	Approval	✓	To approve new and updated policies	Jono Hill Sally Smith Sally Smith Chris Russell Martin Kirke	15.35 – 15.55 (20 minutes)
7.	**Noting papers** **7.1** Horizon Scan **7.2** POMS RCC minutes	Noting	✓		Chair Nick Kennett	15.55 – 16.00 (5 minutes)
8.	**Any Other Business**					
	CLOSE					16.00

Post Office Ltd – Confidential

Risk and Compliance Committee (R&CC)		**Reference: R&CC May 2017**
Date: 04 May 2017	**Venue: Boardroom, Finsbury Dials**	**Time: 13:00 – 16:00**
Members:		
Jane MacLeod (JM)	Group Legal, Risk & Governance Director	Chair
Al Cameron (AC)	Chief Finance & Operations Officer	Member
Alwen Lyons (AL)	Company Secretary	Member
Kevin Gilliland (KG)	Chief Executive - Retail	Member
Martin Kirke (MK)	HR Director	Member
Nick Kennett (NK)	Chief Executive – Financial Services & Telecoms	Member
Rob Houghton (Rob H)	Group Chief Information Officer	Member
Attendees:		
Richard Williams (RW)	Senior Risk Manager	Report (Paper 3.1)
Johann Appel (JA)	Senior Audit Manager	Report (Paper 5)
Deana Herley (DH)	Senior Assurance Manager	Report (Paper 3.2)
Georgina Blair	Risk Business Partner	Secretariat
Jonathan Hill (JH)	Head of Risk, Banking Regulation and Strategy	On behalf of Chief Executive – Financial Services and Telecoms (Paper 5.4)
Jenny Ellwood (JE)	Head of Transformation Risk and Assurance	Report (Paper 5.6)
Amanda Radford (AR)	Financial Controller	Report (Paper 5.2)
Martin Hopcroft (MH)	Head of Health and Safety	Report (Paper 5.5)
Sally Smith (SS)	Head of Financial Crime	Report (Paper 5.3)
James Dingwall (JD)	Interim MLRO	Report (Paper 5.3)
Angela Van Den Bogerd (AVB)	People & Change Director	Report (Papers 5.5 & 5.6)
Russell Hancock (RH)	Supply Chain Director	Report (Paper 4.1)
Sharon Gilkes (SG)	Business Performance and IT Transformation Director	Report (Paper 3.2)
James Carter (JC)	HR Projects Manager	Report (Paper 7.1)
Kelly Taylor (KT)	Employee Relations Manager	Report (Paper 7.1)
Apologies:		
Paula Vennells	Group Chief Executive	Member
The meeting began at 13.00		
Agenda Item 1, Welcome, introduction & conflicts of interest		
The Chair declared the committee quorate and opened the meeting. The Chair asked for any conflicts of interest to be declared. Standing conflicts of interest were acknowledged and no other conflicts were raised.		

Agenda Item 2, RCC minutes and actions

The Committee agreed the minutes of the previous meeting and reviewed the open actions.

AP 1771 (Vulnerable Customers) – The Chair noted that a partner bank had recently asked whether POL had a Vulnerable Customer Policy. JH explained that there is a standard procedure for responding to such queries, and noted that there is an increasing focus on vulnerable customers by the FCA. An update on the policy is expected at the next RCC meeting.

AP1770 (GE accountabilities) – The Chair reported that she would speak to Ben Gray about work he might be doing in this area, and update the action.

AP1768 (Fraud Reporting) – AC noted that there was a need to confirm accountabilities in this area given the recent reorganisation. NK explained that Bank of Ireland will start providing fraud data to POL, and that FRES already provides data. AC and JM agreed to meet to discuss accountabilities and to report back to the Committee (AP 1774).

AP1767 (Tax Governance) – AR explained that a paper was being prepared for May ARC giving the context of current tax governance arrangements, the background to the HMRC report and how POL is addressing HMRC's findings. A strategy paper will follow later in the year. AR confirmed she would circulate the ARC paper to RCC Committee members prior to the ARC meeting.

Agenda Item 3, Risk Submission & Supporting Papers for the Annual Report and Accounts

3.2 Executive Declarations

DH introduced the paper and explained the categorisation of declarations, and asked the Committee to consider which declarations should be reported in the ARC paper. The Committee discussed the declarations and requested that DH produce a summarised paper updated to reflect their comments and recirculate it prior to ARC (AP 1775).

The Committee discussed the Camelot audit issue, and requested that KG prepare a lessons learned report on Camelot describing what happened, how it was discovered and what the consequences are, for the next RCC meeting (AP 1776).

3.1 Top Risks and Risk Appetite

The Chair introduced the paper, explaining that the top risks had been referenced to the group risk profile reviewed by the Committee in January 2017 and reorganised into a format consistent with the risk placemat. Risks had also been linked to risk appetite statements, although key risk indicators had not yet been identified but it was expected that these would come out of the placemat work. The Committee discussed the risks and noted that not all members had yet commented on their risks. Accordingly they were requested to provide updates to RW so that the risks could be updated to reflect their comments prior to submission to ARC (AP 1777).

3.3 Risk Section of the Annual Report and Accounts

The Committee noted that this section would be reviewed to reflect the changes to the top risks.

Russell Hancock joined the meeting.

Agenda Item 4, Risk Update

4.1 Supply Chain Pilot of the Placemat

The Chair introduced the placemat pilot and explained that it would be extended to the other areas in Finance and Operations. AC noted that the pilot had been very useful but that the assessment process was still being developed, and that his leadership team were committed to running the process across Finance and Operations with a full report going to September RCC. The Committee requested an update on progress at the July meeting (AP 1778).

RH explained how the process had worked in Supply Chain, and how it had helped him identify wider risks in his area and given him a format to help monitor them. He confirmed that even though it had been a pilot, and involved an amount of pre-work, it had not been onerous. The Chair noted that a benefit of the placemat process was to enthuse members of the business unit about risk management. RH noted that the challenge going forward will be to keep the outputs up to date, and the Chair confirmed the expectation that each business unit will update their assessment once a quarter, in an activity led by the business unit Risk Champion and supported by the Central Risk Team. The Chair advised that at the July meeting the Committee would be requested to consider the roll out timetable for the placemat across the business.

RH left the meeting. Rob H and SG joined the meeting. AR left the meeting.

Agenda Item 5 Key Operational Risks

5.1 IT Controls

Rob H introduced the paper. AC asked if the work described in the paper was meant to reassure the Committee about the state of IT Controls. Rob H explained that the work had confirmed that POL is outside its risk appetite with regard to IT Controls. The Committee asked Rob H to confirm what he was most worried about. Rob H explained that it was POL SAP/HR SAP falling over and that the current control environment would still let these systems go down but that the response time would be better. He noted that focus was on improving the control environment through a combination of improving hardware and improving identification of threats. Rob H explained that SG had been preparing an operational risk 'Tube map' to enable informed decision making. The Committee requested that this be brought to the July meeting (AP 1779).

AR re-joined the meeting. Rob H and SG left the meeting.

5.2 Financial Controls

AR introduced the paper and explained that Phase 2 of the project would tackle the master data, that the team is currently making good progress and that a controls manager is being recruited.

MH and AVB joined the meeting.

5.5 Health and Safety

MH introduced the paper noting that performance was strong for all four of the key health and safety metrics, including absence accidents and lost days. The Committee discussed the presentation of metrics and noted the difficulty in benchmarking H&S metrics. MH noted that reporting and oversight were to be re-considered during Q1 and new metrics identified. The H&S subcommittee deep dive on the following day would include a review of road risk, which was a current area of concern. AC noted a recent incident in which a driver in Supply Chain had revealed his licence had been removed for alcohol dependency, and explained that they were looking at the introduction of an enhanced method of breath testing and using fingerprint testing as a permission to release keys in Supply Chain. The Network Operations Director had been asked to review safety procedures for people who drove either their own or company cars for Post Office business

MH & AR left the meeting. SS and JD joined the meeting.

5.3 Financial Crime

SS introduced the paper. The Committee discussed the disappointing completion rate for AML/CTF training for all back office employees, which was due to be completed by 21st April but only appeared to have been completed by 53% of employees. Difficulties in tracking who had completed compliance tests would be resolved once the EUM project was implemented, although there was a great deal of data cleansing to be done before implementation.

JD explained that work commenced in February on risk-assessment work on further products and services and is currently on track, although there has been a need to accelerate the risk assessment of POMS and the insurance products under its umbrella. The Drop & Go risk assessment was much improved, and Laura Plunkett, the Product Manager, had been exemplary in her approach to tackling the problems. Workshops with other product managers were being planned. The Committee discussed the role of product managers. SS explained that HMRC are to review Bill Payments later in 2017. The Committee noted that additional resource will be needed to review bill payment services and this should be viewed as a priority.

The Chair noted that the Financial Crime team had flagged that vetting procedures for corporate agents needed to be reviewed and we needed to determine what assurance was required for changes to directors and shareholders, etc.

SS and JD left the meeting.

5.6 Transformation

JE introduced the paper noting that there had been some changes to the top risks reported in March, namely that the Resourcing – Off Payroll risk had reduced but that Complex Change Portfolio Delivery and IT Vendor Renegotiation / IT Supplier Capacity remained red. The Committee noted the emerging risk posed by a Royal Mail strike.

TA joined the meeting.

5.4 FS Conduct

JH introduced the paper and explained that the conduct scorecards from Bank of Ireland and POMS had not been ready for the RCC meeting but might be ready for ARC. The Committee noted that the ARC would want to know how the business ensures that Customer Relationship Managers aren't mis-selling. JH explained that this was set out in the paper, and that the next phase of work would be focussed on counter staff and insurance products. The Committee noted that the themes of current FCA focus were culture and vulnerable customers. NK noted that there were no updates as to whether the Senior Manager Regime will apply to appointed representatives, however it will apply to POMS.

Agenda Item 4.2 Business Continuity and Crisis Management Update

TA introduced the paper, explaining that business continuity planning continues across all sites, with recent activity focussed on Swindon. Plans are underway for a full day exercise at the Chesterfield (Finance Service Centre) recovery site. A business continuity workshop with Royal Mail is planned to help assess the potential impact of a Royal Mail strike. The Committee briefly discussed the proposed workshop and requested that TA include somebody from POL who had experienced the last Royal Mail strike in the working group (AP 1780).

Agenda Item 6, Internal Audit Report

JA updated the Committee on recent audit activity, noting that two audit reports had been issued since March ARC with a further seven reports in the process of being cleared with management for reporting at the May ARC. The Committee noted the reviews planned for the first quarter of 2017/18 and KG thanked JA for bringing the review of Mails Processes forward.

JC and KT joined the meeting.

Agenda Item 7, Decision Papers

7.1 Modern Slavery

JC updated the Committee on recent activity, explaining that due diligence had been undertaken on POL business and supply chains to identify potential areas of risk for modern slavery. A revised Statement on Modern Slavery had been prepared in line with the legislation which must be published within 6 months of year end.

The Committee agreed to recommend to the ARC and Board that the 2017-2018 Modern Slavery Transparency Statement should be adopted.

POL00401625

MK, JC and KT left the meeting.

Agenda Item 8, Noting Papers

The Committee noted the following papers

8.1 Horizon Scanning

8.2 POMS RCC minutes (February and March 2017)

8.3 Whistleblowing Report

8.4 Identity Fraud Incident Report

Agenda Item 11, Any other Business

Nothing raised.

The meeting closed at 16.10

Next Meeting – 20 July 2017, Room 0.03 Moorgate 13.00 – 16.00

POL00401625

POL Risk and Compliance Committee
Action List

Status Report as at: 13/07/2017

Meeting Date	AP ref	ACTION	Action Owner	Due Date	STATUS	Open/ Closed
04/05/2017	1780	**RM IA Planning** - Include somebody with experience of the last RM IA in the planning team	Tim Armit	31/05/2017		Open
04/05/2017	1779	**IT 'Tube map'** - Bring and explain the IT Tube map of operational IT risks to the Committee	Rob Houghton	20/07/2017	See paper 3.4	Open
04/05/2017	1778	**Update on Placemat Pilot -** Update the Committee on progress of the roll out across Finance and Operations and consider the roll out plan thereafter.	Deana Herley/ Richard Williams	20/07/2017	See item 4	Open
04/05/2017	1776	**Camelot Audit Lessons Learned -** Produce a paper on the lessons learned (what happened, how we found out about it, potential consequences) for next RCC	Kevin Gilliland	13/09/2017		Open
04/05/2017	1774	**Fraud Reporting -** Hold meeting between JM, AC (& NK?) to agree accountabilities for fraud reporting and data to be reported	Jane MacLeod/Al Cameron/ Nick Kennett	20/07/2017		Open
09/03/2017	1773	**RCC Terms of Reference** - to be reviewed and updated based on changes in PO structure	Jane MacLeod	13/09/2017		Open
09/03/2017	1771	**Vulnerable customers** - policy to be reviewed and updated based on RCC feedback. Martin Kirke to review draft policy.	Jonathan Hill/ Martin Kirke	20/07/2017	See paper 6.1	Open
09/03/2017	1770	**GE accountabilities map** - to be refreshed / updated based on the new structure following discussions	Jane MacLeod	20/07/2017		Open

3.1 Financial Services Conduct Risk Update

Author: Jonathan Hill

Meeting date: 20 July 2017

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. Although the business faces some conduct risk challenges, some of which are referred to below, they are being managed within the overall risk appetite. Post Office has an averse risk appetite for not complying with law and regulations or deviation from business' conduct standards. Key assurance on this is provided through the MI dashboards and reports from BoI and POMS (attached).
4. However, there remain challenges from changes to the business model, including regulatory changes, which require on-going focus to maintain conformance and compliance. Our Principals can require us to cease activities where we cannot demonstrate adequate controls to mitigate conduct risk.

Input Sought

5. The R&CC is asked to note these developments.

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 and POMS-Post Office Joint Compliance Committee, which meet monthly.

Current risks and issues

Customer Relationship Managers (CRMs)

7. As at 2nd June there were a total of 491 active CRMs. The vast majority of these are digital tablet enabled.

8. With CRMs we have a more positive engagement with customers (on an introductory basis) on FS products and this is done within the control remit of a Training and Competence scheme that FS&T Risk oversee and monitor. Nevertheless as we seek to grow and innovate the CRM network, we need to ensure that the conduct and operational controls in place remain appropriate.

9. It was reported in June that there were a higher number of red video mystery shops (VMS) than our benchmark expectation. As required by the T&C Framework all CRMs receiving a red mystery shop are withdrawn until the Area Sales Performance Managers (ASPMs) follow this up with the individual concerned and re-trains the CRM as appropriate.

10. From the FS&T review of the videos it does appear that a key root cause of these errors are not closely following the required journey and/or not using the correct detailed product wording on the tablet.

11. The training development calls with the ASPMs given by the Post Office training team will emphasise that the compliant sales journey is 'built in' to the tablet. CRMs should not 'ad lib' and should use the tablet for the customer journey and refer to it for answers to customer questions.

12. We will monitor the next round of mystery shops and agree actions with the network teams and our principals.

Advertising breaches and Issues

13. BoI monitoring reported that some branch related campaign material was out of date. Three of the four breaches reported related to one mortgage campaign, but BoI record these as three separate breaches as there were three different items in the single campaign. Whilst the material referred to remained compliant, BoI require that the material with a 'sell by' date is re-approved. This has now been actioned.

Branch Regulatory knowledge

14. A recurrent monitoring theme from both Principals is a concern about the level of product or regulatory knowledge shown by a counter colleague when tested.

    - Whilst there may have been some gaps identified we are working with our Principals to ensure that the questions tested are appropriate. For example, we would agree that a counter colleague should know how customers can make a complaint but would not necessarily expect them to answer questions about the FOS process.

Cash Savings Remedies

15. From 1st December 2016, all savings providers have been required by the FCA to provide at the point of sale prescribed information in the form of a standardised summary box. This is to ensure customers have the appropriate information they need to be able to compare products.

16. Since Post Office Money went live with the Summary Box leaflet to circa. 4,600 branches, we have been checking levels of conformance. Mystery shopping throughout the earlier part of the year demonstrated conformance at c75%-78%, short of the 95% target.

17. The relevant savings material is being updated with a sleeve at the front for the summary box to be inserted into. This should enable high levels of compliance to be maintained. The new material was to have been distributed in June/July but this has been delayed and will now happen in August 2017. We will monitor its impact.

Future issues

Senior Managers and Certification Regime

18. The Senior Managers and Certification Regime will expand to all FSMA regulated firms by 2018; the precise timetable remains unclear but an update paper is expected from the FCA in Q1 2017/18.

19. Firms will need to put in place a 'Statement of Responsibilities' map, recording the allocation of responsibility to a senior manager for every part of its business areas and management functions. It will also need to identify any significant management/material risk takers that will be 'certified persons'. Firms must certify these as 'fit and proper' on an annual basis. There are also conduct rules for all staff undertaking regulated business under this regime.

20. It still remains unclear what the precise requirements will be for Appointed Representatives, but for POMS planning is already taking place to work through the implications. FS&T Risk is working with POMS to ensure that we are supporting the implementation of SM&CR in POMS.

21. BoI is also looking to enhance its SMCR oversight through the redeployment of the remaining CDMs. BoI and Post Office are working together to ensure that this is done without confusing existing conduct risk controls and responsibilities. We are also looking to ensure BoI meets it contractual obligations on the use of CDMs.

Insurance Distribution Directive

22. The FCA's Insurance Distribution consultation paper outlines the requirements to be in place for February 2018. These include new requirements on a customers' best interests rule, record keeping, commission disclosure and the training requirements for the new regime (15 hours CPD).

23. This will have significant impact on how insurance products are sold and intermediated. POMS is driving a project group to assess and implement the changes with FS&T Risk and the wider network.

Culture, governance and consumer vulnerability

24. These remain priority areas of focus for the regulators. We are working with Retail to ensure that we identify key FS themes and drive culture change across the network.

25. FS&T Risk has engaged with the Retail team and produced a first summary report for management action. This will be followed up jointly between Retail and FS&T Risk.

26. An updated proposed Vulnerable Customer Policy has been submitted to the Committee for approval and implementation. Both Principals have asked to have sight of this once approved. POMS will use this as the basis of its Vulnerable Customer policy and approach. In addition, Ofcom has asked to see the policy, acknowledging that it needs to encompass more than the specific requirements placed on telecoms providers (e.g., not cutting off service to vulnerable customers).

Jonathan Hill

Head of FS&T Risk & Regulation

July 2017

BOI Post Office Money branch distribution - June 2017

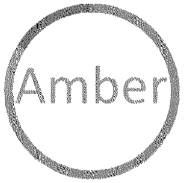
Risk ratings

May risk ratings and how they compared to April

●	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 breaches/issues	▼
●	Social media breaches/issues	◀▶
●	Savings cancellations	▼
●	Competent specialists	◀▶
●	Supervisor spans of control	◀▶
●	BOI supervisor reviews	

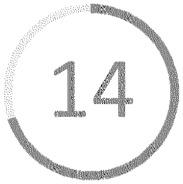
Performance measured in May

Risk ring and overall performance rating

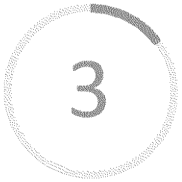


Based on the weighted cumulative outcome of the KRIs we measured in May, the overall risk rating is Amber.

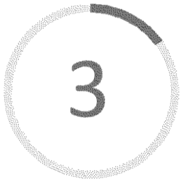
Green rated KRIs



Amber rated KRIs



Red rated KRIs



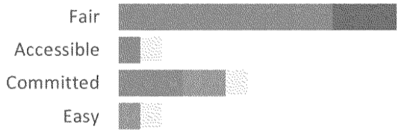
This month we were within tolerance for 17 out of the 20 KRIs we measured. 14 of our KRIs were rated green and 3 of our KRIs were rated amber. 3 of our KRIs were rated red. In comparison, in April we exceeded tolerance in 2 of our KRIs and in March we exceeded 3 of our tolerances. On average, in each month between December and May, we were within tolerance in 18 of the KRIs we measured and exceeded tolerance in 2.

May v April ratings

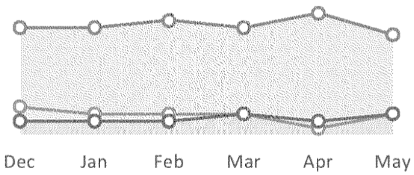
◀▶	14
◀▶	1
◀▶	2
▲	0
▲▼	2
▼	1

2 KRIs remained red and one KRI fell to red.

Performance against our FACE commitments



Distribution of KRI risk ratings between December 2016 and May 2017



Exceptions and key trends

CRM mystery shops - while the CRM credit card pilot, which resulted in a number of red-rated mystery shops, has now ceased, CRM savings shops are a cause for concern, with 12 out of 64 (18.8%) being red rated in the 3 months to the end of May. While these shops relate to lower-risk introductory activities, remedial actions are being followed up with Post Office and progress will be kept under close oversight for a period.

Counter mystery shops - the risk rating for PO counter mystery shops is currently red, although this is based on a relatively small sample size (16 shops). Once again, while these shops relate to lower-risk introductory activities, remedial actions are being followed up with Post Office and will be kept under close oversight for a period.

Advertising breaches and issues - Four material financial breaches were recorded in May and related to in-branch mortgage campaign material remaining in the public domain after its withdrawal date. POL have confirmed that the reapprovals 'were' missed' as a result of the impact of the organisational restructure on the Marketing function. All four items have since been reapproved.

Branch regulatory knowledge - 6 out of 53 branches were rated red for 'conduct and culture' during the last three months. The red ratings resulted from a range of different issues. The most prominent related to regulatory processes including the location of the branch 'operations manual' and gaps in staff knowledge of the FOS process.

Savings cancellations - Although still within tolerance, the increase in savings calculations has been followed up with the BOIUK Savings Team, who have confirmed that there are no specific concerns in relation to the increase.

◀▶ 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

POL00401625

POMS CONDUCT RISK SCORECARD

		Rating Criteria			Current						
Area	**Measure**	**Green**	**Amber**	**Red**	**May-17**	**Apr-17**	**Mar-17**	**Feb-17**	**Jan-17**	**Dec-16**	**Nov-16**
Complaints	Number of Opened complaints	0-1,000	1,000 - 1,500	1,500 - 2,000	*249	299	314	264	321	283	345
	Percentage of upheld complaints	0% - 20%	21% - 30%	31% - 100%	*25%	33.7%	36.8%	31.3%	27.5%	28.7%	28.1%
	No of FOS cases upheld	0 - 3	4 - 7	8 +	0	1	0	1	1	0	0
Mystery Shopping/VMS	Proportion of shops rated red in the month	0% - 10%	11% - 20%	20% - 100%	7%	5%	0%	13%	20%	0%	14%
	Number of shops rated black in month	0	0	1	0	0	0	0	0	0	0
Branch Monitoring	Number of red rated findings in the month	-5	5-9	10+	5	8	7	5	1		
Call Monitoring (Travel)	Percentage of red rating calls in the month	0% - 10%	11% - 14%	15% - 100%	40%	24%	19%	20%	15%	5%	4%
Call Monitoring (Life)	Percentage of red rating calls in the month	0% - 10%	11% - 14%	15% - 100%	10%	10%	6%	22%			
Cancellations (Motor, Home, Pet, Business, Motorcycle)	Percentage of products to sales, cancelled within the cooling off period (14 days)	0 % - 5%	6% - 10%	11% - 100%	3.5%	3.6%	4.1%	2.9%	2.8%	3.1%	3.1%
Cancellations (Life & Over 50s)	Percentage of products to sales, cancelled within the cooling off period (30 days)	0 % - 9%	10% - 14%	15% - 100%					9.0%	6.5%	6.7%
Cancellations (Travel)	Percentage of products to sales, cancelled within the cooling off period (30 days)	0 % - 9%	10% - 14%	15% - 100%							
Claims (Travel, Protection, Home and Pet)	Percentage of claims repudiated	0% - 5.9%	6% - 10%	11% - 100%	4.9%	5.2%	6.1%	4.6%	4.6%	7.4%	5.3%
Training & Competence	Percentage of POMS staff completed mandatory training	100% - 95%	95% - 90%	89% - 0%	96%	97%	100%	100%	87%		
	Percentage of Call Center staff completed mandatory training	100% - 95%	95% - 90%	90% - 0%	100%	100%	100%	100%	100%	100%	100%
	Percentage of Branch staff completed mandatory training (MS)	100% - 95%	95% - 90%	90% - 0%		98%	92%	88%			
	Percentage of Branch staff completed mandatory training (CRM)	100% - 80%	75% - 70%	69% - 0%	75%	72%	72%	86%			
Customer Satisfaction (CES)	Proportion of customer responses to NPS surveys that confirm adequate information was provided at the point of sale in the previous 3 months (Scores based on 3MRA)	80	79-60	>59	77%	77%	77%	82%	88%	93%	93%
Net Promoter Score (NPS)		35	34-30	>30	38	38	42	42	40	39	40
Financial Promotions	Financial Promotions right 1st Time	50%+	35-49%	-35%	75%	51%	45%	65%	52%	30%	49%
Incidents	Number of Severe Incidents (rated 1 or 2)	0	1	2	1	1	3	1	1	0	0
	Number of unresolved Incidents	0 - 15	16 - 20	20+	13	17	21	20	14	19	17

3.2 Change Risk Update

Author: Jenny Ellwood Sponsor: Angela Van Den Bogerd Meeting date: 20 July 2017 (RCC)

Executive Summary

Context

This report provides an update on the key risks being managed within the Change Portfolio. It also provides a high-level analysis of the Change risk profile, how the portfolio is performing and the key challenges being faced.

Questions addressed in this report

- What are the top risks currently being managed within the Portfolio and what is the performance of risk management based on the mitigation plans?
- What are the types of portfolio risks and how has this mix changed?
- What is the current churn rate of portfolio risks and what are future projections?
- What is the current risk weighting of the portfolio/how is this expected to change?

Conclusion

1. There have been some slight changes to the top risks reported in May 2017. Work within Success Factors and Enhanced User Management (EUM) has led to the escalation of the effectiveness of the new identity management system and a new risk 'EUM Effectiveness'. Work is underway to identify mitigation actions and a way forward to reduce this risk.
2. The two previously reported risks (Complex Change Portfolio Delivery and IT Vendor Renegotiation/IT Supplier Capacity) remain red and continue to be closely reviewed and monitored.
3. The type and mix of the portfolio remains broadly unchanged in this reporting cycle. Portfolio and key Programme risks continue to be regularly reviewed at a monthly risk workshop. The new integrated plan being developed is also driving discussions on potential risks and dependencies and progressing well. However, for this reporting period the Portfolio Risks have reduced to 26 and remain consistent with the nature and complexity of the individual projects and the timeline.
4. Monthly health checks continue and Programmes are demonstrating they understand their deliverables, risks and issues and work continues to improve dependency identification, tracking and monitoring.
5. The current residual risk exposure is tracking within appetite and threshold.

Input Sought

The RCC are asked to note the progress made since the last RCC, 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.

The Report

What are the top risks currently being managed within the Portfolio?

1. At the end of June 2017, the overall Post Office change portfolio status remained Amber, this is taking consideration of the individual status for delivery, costs and risks of each Programme.

2. In terms of the delivery status though, we are currently reporting 'red'. Key drivers include:
   - There have been a number of deployment issues in Branch Technology 'roll out' (Application packaging by our supplier Computacenter) that have impacted the deployment of branch counter and HNGA. We have deployed the new Horizon kit 'HGNA' to four branches (of planned 150) and whilst those 4 are performing well and feedback from Postmasters on performance is positive the time required to deploy during the pilot phase has not allowed deployment in branches within the agreed change window. The Programme has reached the planned deployment levels for Network Only swap (Fujitsu to Verizon) of circa 150. Issues have largely now been resolved and we will recommence roll out to schedule from 13th July. There is no requirement to change the end date of current plan as the Programme will increase installations per day following 2 weeks of successful installation.
   - Enhanced User Management (EUM): The programme continues to explore deployment options of the new identity management system and the Steering Committee has identified significant additional scope required to ensure it is effective and manageable within the network.
   - Success Factors payroll data migration: This has experienced difficulties and is delaying migration by a minimum of 3 months currently in plan for October / November 2017.
   - Ongoing testing capacity: Constraint continue to be monitored and priorities and appropriate scheduling are reviewed on a weekly basis. No immediate concerns but one we continue to monitor through the integrated plan work.

3. There are currently 26 open risks being managed at a Portfolio level, a slight reduction from the last ARC report in May 2017. The current top risks are:
   i) EUM effectiveness
   ii) IT Vendor renegotiations
   iii) Complex portfolio planning & IT Management

4. EUM will provide the necessary controls for branch colleagues on who can access and transact on the Horizon system thereby protecting the business from regulatory, financial and reputational damage. The programme are managing a number of challenges that must be overcome to ensure full and effective deployment. These include the need to obtain accurate data from agents, the willingness of agents to provide personal email addresses, to be able to access data to confirm the vetting and compliance training status of all Horizon users and to have business processes in place to manage data, password management and system access issues (in addition to providing e-mails to all employees). The additional scope will be subject to all internal governance gates.

5. The risk which has been escalated to a portfolio level is around with the existing challenges and the possibility that the process may not be able to work as anticipated. The challenges are being reviewed and alternative approaches/ workarounds being explored, including time and cost estimations. A revised business case will be produced and will need to be approved before additional programme spend is secured.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
(i) EUM effectiveness	There is a risk that EUM does not perform as expected due to 1) being unable to collate accurate data from our agents 2) POL staff/agents not having an individual email address which can be used to communicate logins and training information, and 3) agents not being able to access SuccessFactors via the internet/browser solution	**16** **I/L** **4:4**	Identify gaps within the SF/EUM design, including further due diligence Develop end to end process maps with risks and controls Revised business case and replan Model office and pilot completion	Complete July 17 31 July 17 5-26 July 17	**9** **I/L** **3:3**

6. With regard to IT vendor renegotiations, since the last ARC the contract negotiations have continued and good progress has been made to align to Fujitsu's new global operating model. A ways of working approach to redesigning the IT operating model has been agreed with Atos. Internal and external discussions are ongoing and are driving the immediate actions which have now been added to the mitigation actions.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
(ii) IT Vendor Renegotiations	There is a risk that IT Vendors engagement proves difficult and they display poor behaviours through renegotiations which could impact successful change delivery	**16** **I/L** **4:4**	• Establish Legal support to assist in vendor contract renegotiations **(Complete)** • Hire negotiation and procurement expertise **(Complete)** • Contract Managers are in place to manage transition and ensure Vendor SLAs and commitment is maintained **(Ongoing)** • Leverage GE/Board and other connections **(Ongoing)**	Ongoing	**9** **I/L** **3:3**

7. Work continues to maintain, and in time, reduce the impact and probability of the Complex Change Portfolio Delivery risk. The integrated plan is developing well and the monthly planning sessions are taking shape with detailed discussions on potential congestion, risks, issues and dependencies. Those sessions will continue to improve the knowledge management within programmes and help identify areas which require further deep dive reviews and analysis.

8. The current watch item on the plan relates to the Horizon Data Centre refresh activity which requires 24 weeks of testing, currently due to complete Q3 2017. Given competing pressures such testing is intermittent to allow other changes to be tested in Model Office i.e. Transaction Simplification/Drop and Go enhancements. Ideally we would have a change freeze in place whilst

undergoing such a major transformation but given wider business pressures this is simply not viable.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
(iii) Complex change portfolio delivery	The next phase of Transformation will have increased dependencies and interconnectivities leading to more complexity to manage, which if not managed well could significantly impact our execution plans.	**16** **I/L** **4:4**	• Develop single Business/IT Master Plan to schedule/smooth Change Delivery • Create a single view of all change • Ensure clear lines and demarcation of accountability between Change Programmes and Enterprise Portfolio Management activities • Prioritisation exercise to be completed to identify they key activities to be progressed • Produce new integrated plan and identify scheduling and hotspot constraints in line with prioritisation exercise above • Implement central dependency tracking to allow increased visibility, management and control • Analyse high-level dependencies to ensure robustness and integrity of high level plan	Ongoing Ongoing Ongoing Complete June 2017 June 2017 June 2017 (ECG)	**8** **I/L** **4:2**

9. A full list of the 26 portfolio risks is shown as an Appendix.

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

10. At the last ARC meeting there were 27 portfolio level risks. The current total is 26 which, however, has been subject to churn in the intervening period in that 4 risks were closed namely:

- IT Network Branch and Admin Delivery Risk: There was a risk that the IT Networks Branch & Admin project would not deliver its objectives in line with the current approved business case/budget. This was agreed that this risk should be closed at Portfolio level as its impact/likelihood had reached target.
- IT Strategy Development – Alignment with Transformation: There was a risk that the IT Strategy currently under development could cause a cost risk to Transformation activity. This risk was closed on the basis that the socialisation of the IT Strategy has taken place and meetings were in place to provide updates on the strategy as part of a regular GE member engagement process.
- Portfolio Plan: There was a risk that we would be unable to recruit technical planning resource and unable to plan sufficiently within Transformation. This risk has now been closed. This was on the basis that, following an initial review of the current level of planning resource across the programmes, the view is that capacity is not the issue. The issue is with adherence to planning standards which the Central team are tackling.
- Chameleon: There was a risk that Network Simplification may fail to deliver technical capability solution due to an IT partner's lack of capability and experience in this area. This was closed on the basis that Fujitsu were on board and had supplied required resources.

The 3 new risks opened are:

- EUM Effectiveness: As reported on page 3.
- Adverse Impact of Change/Organisational Change on Agents: There is a risk that the extent and timing of remuneration changes on Agents (including multiples) could result in increasing adverse reaction/hostility from Branches to wider change activity.
- Operational Impact of Generic Training Expiry Dates: There is a risk that a significant number of network individuals who have not completed their compliance training by the required date will cease to have Horizon access for certain products on the same date.

11. The table below, illustrates how the mix of risks at portfolio level continues to flex and shows the open portfolio risks by severity.

RAG Impact/Likelihood	**Minor (1)**	**Moderate (2-4)**	**Major (5-11)**	**Significant (12-19)**	**Critical (20-25)**	**Total**
Jun-17	0	2	15	9	0	26
May-17	0	2	13	9	1	25
Apr-17 (last ARC data)	0	2	14	11	0	27
% of total (current period)	0%	8%	58%	35%	0%	100%
Number of New Risks						3
Number of Emerging Risks						2
Number of Closed Risks						4

Figure 1: Please note the minor/moderate risks are managed at a local level and not escalated to the Portfolio view. The risk reported as critical in May was around EUM effectiveness and as work is underway on mitigations this has reduced slightly,

What is the current churn rate of portfolio risks and what are future projections?

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

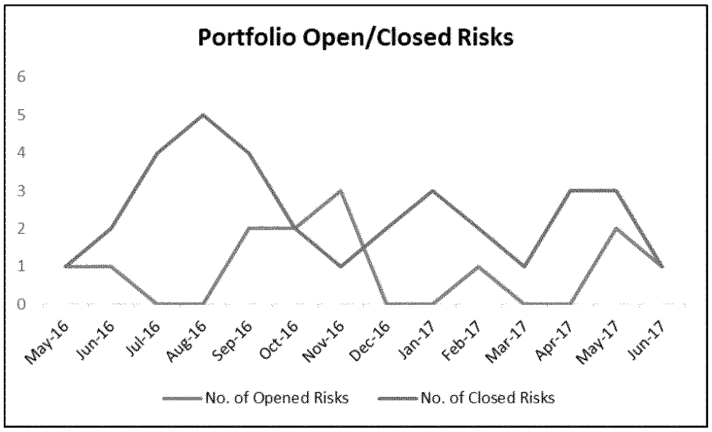


Figure 2: A comparison of open/closed risks (by month)

13. As we have seen within this report we have had a reasonable churn of risks being closed and new risks being raised during this reporting period.

What is the current risk weighting of the portfolio and how is this expected to change?

14. 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 257.

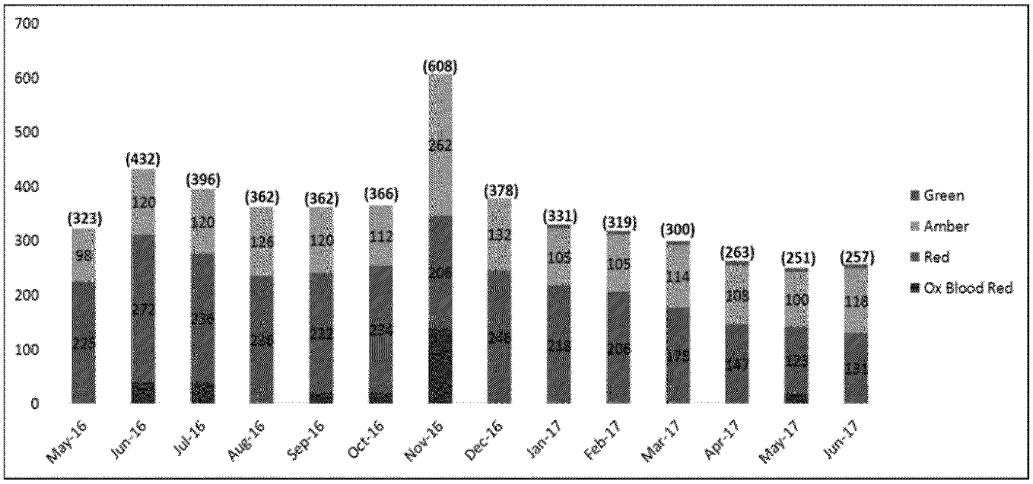
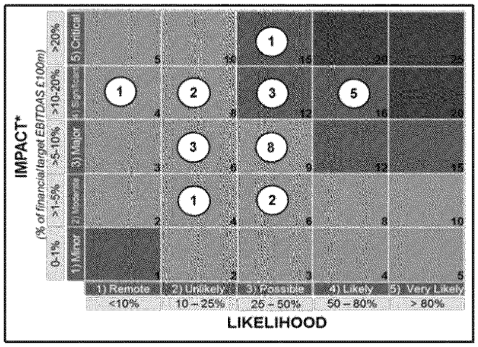


Figure 3: Current cumulative portfolio risk weighting score by month

15. The overall risk severity score has reduced by around 3% since April 2017. This has been the result of risk closures. The risks continue to be monitored in line with the change portfolio risk review process.

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



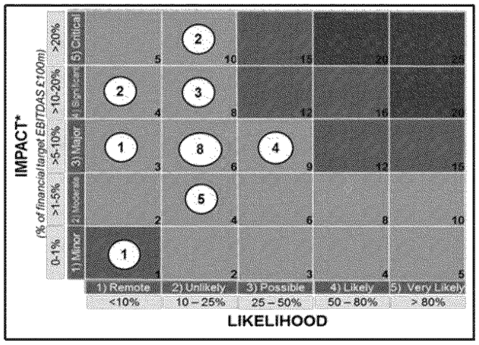


Figure 4: Current portfolio risk weighting (June 2017) Figure 5: Projected portfolio risk weighting (Dec 2017)

Appendix: Change Portfolio risks

	Risk Title	Mar ARC	May ARC	July ARC	Grid Ranking CURRENT	Grids Ranking TARGET
1	EUM Effectiveness			✓	16	9
2	IT Vendor Renegotiations	✓	✓	✓	16	9
3	Complex Portfolio Planning & IT Management	✓	✓	✓	16	8
4	IT Delivery Capability	✓	✓		16	6
5	Operational Impact of Generic Training Expiry Dates			✓	15	6
6	IT Networks Branch Incumbent Supplier Proactive Engagement - BT				12	10
7	IT Change Operating Model (previously known as IT Supply Chain)				12	8
8	Capacity of IT Key Suppliers	✓	✓		12	6
9	Data Risk				12	8
10	Delivery - Integrated Plan Delivery Performance				12	8
11	Financial Risk – Insufficient Funds to Deliver Transformation				9	6
12	Resourcing Risk – Payroll Legislation	✓	✓		9	9
13	Transformation Delivery Oversubscribed				9	4
14	Unintended consequences on Operational Performance – Process				9	9
15	Availability of Key Skills and Knowledge				9	6
16	Unintended consequences on Operational Performance – People				9	6
17	Adverse Impact of Change / Organisational Change on Agents				9	6
18	Financial risk - Benefits/Revenue Realisation				8	6
19	Deployment of Non-Compliant Solutions/Systems				8	4

	Risk Title	Mar ARC	May ARC	July ARC	Grid Ranking CURRENT	Grids Ranking TARGET
20	Responsible use of public funds				9	1
21	Strategy & Design: current BaU and Transformation conflict				6	3
22	Accounting & Reconciliation				6	4
23	Reputational Damage - Media risk				6	4
24	Reputational Damage - Political stakeholder risk (local government)				6	4
25	Reputational Damage - Political stakeholder risk (national government)				4	4
26	Poor coordination of communications about change activity with stakeholders and employees				4	4

3.3 Financial Crime Risk Update

Author: Sally Smith Sponsor: Jane MacLeod Meeting Date: 20th July 2017

Executive Summary

Context

This paper updates the Risk and Compliance Committee on progress with the HMRC Regulatory Activity project which has been established to manage both the HMRC's Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) audit and the risk assessment work being undertaken to address Financial Crime Risks.

Questions this paper addresses

- What is the current position with the HMRC Audit and potential penalties?
- What is the current position on progress with the Financial Crime risk assessment work and next steps?
- What are the impacts for Post Office of regulatory changes

Conclusion

1. HMRC met with us on 29th June to review the action plans for Bureau de Change and the wider Financial Crime activities to support regulatory requirements. They are broadly satisfied with the progress made to date and the proposals in relation to improving controls for Bureau de Change, however they have asked for more granularity on the timescales of the product proposals at the next meeting which is scheduled for the 26th July 2017.
2. HMRC have now issued the pre-penalty notice for historic branch premises registration errors - £796,500. We are reviewing the notice to determine whether there are grounds for challenge. Sanctions in respect of issues identified in the current audit relating to Bureau de Change are still under consideration.
3. Risk assessment work is broadly on plan, with the six high risk products nearing completion, and work has now commenced on Bill Payments. Risk Assessment work for POMS and their insurance products was completed in May.
4. The UK legislation for the 4th Money Laundering Directive came into effect on the 26th June 2017 and, whilst in line with expectations previously reported, does include requirements that could have significant impacts for Post Office. The extension of the Fit and Proper regime requirements are unclear and difficult to assess until clarification is received from HMRC. The HMRC Money Service Business (MSB) Guidelines requirement to retain physical or electronic copies of customer due diligence documentation for 5 years appears to be inconsistent with other industry guidance. Post Office is currently formulating a response to HMRC on both these issues.

Input Sought

The R&CC is asked to review this report, endorse the recommendations, and consider whether further actions should be considered.

The Report

HMRC Audit status

5. A meeting was held with HMRC on the 29th June 2017 at which the Bureau de Change product risk assessment and action plan was presented by Nick Kennett. Key points included the following proposals:
   - An overview of customer type, normal/expected transaction activity and market information to demonstrate that the Post Office service is aimed at lower value travel/holiday money business;
   - Lowering the overall customer due diligence from £5k to £2k and introducing PEPs and Sanctions checks and eKYC at this level;
   - Implementing a lower data capture and one form of primary ID for transactions between £1k and £1,999 – this is in line with current data and ID capture for card transactions (which protects Post Office from chargeback rights associated with breaches of Card Scheme rules);
   - Building a daily feed of all Bureau de Change activity (regardless of amount) into a central Post Office data depository, with appropriate tools that provide rules based transactional pattern activity exception reports together with the ability to undertake ad-hoc and holistic transaction monitoring;
   - The resulting enhanced data monitoring would enable Post Office to be confident that it can identify non-conformance and breaches, and assure both Post Office and HMRC that customer data capture and due diligence thresholds have been set at an appropriate level to manage the risk exposure;
   - Timeframes for delivering the system enhancements and requirements.
6. HMRC advised that the proposals were broadly in line with their expectations but more information is needed on implementation timescales – they expressed concern as to the length of time that some of the changes identified in the plan would take (many of which were targeted for January - June 2018); the view from HMRC was that they would normally expect action plan activities to be implemented within 6 months. Whilst understanding the implications of OJEU for any system procurement that may be required, they have asked for more granular detail about the delivery and how this will be achieved at the next meeting.
7. At the meeting, HMRC advised that the penalty notice in relation to the historic premises registration issues would be issued shortly. This has now been received and covers two periods:
   - 1 May 2007 – 26 April 2016 - £784,500
   - 23 May 2016 – 5 September 2016 - £12,000

   We are reviewing the notice to determine whether there are grounds to challenge.
8. HMRC are still considering penalties in relation to potential breaches in regulations in relation to Bureau de Change and have asked for further detail in relation to the

profitability of the product. Forensic accountants within HMRC have raised some queries and since the meeting they have provided the detail of their queries in writing and the product team are now reviewing these.

9. Depending on the outcome of the profitability queries, our supervisor believes that a fine in the order of c£300k would be appropriate based on their 'normal' methodology (the period under review is January 2015 – August 2016), however there is a view within HMRC that it should be as much as c£1 million. Finance are looking at raising a provision to cover any potential penalty.

10. HMRC were briefed on the progress of mandatory AML/CTF training completion (see update below) and whilst happy with the progress made, have asked for a further update by 20th July. HMRC stated that they are not considering sanctions in relation to the historic training, due to the improvements that had been made prior to the commencement of the audit. A further meeting is scheduled for 26th July 2017.

Financial Crime Risk Assessment Update

11. The action plan in Appendix A gives full updates, but in summary:
    - Drop and Go –completed and logged for next annual review March 2018.
    - MoneyGram, Gift Cards, Travel Money Card, International Payments and Postal Orders – re-assessment has been completed and draft report, risk assessment and product information pack are with the product managers for review and sign-off. These will then be presented to the next available AML Steering Group for completion and approval of closure.
    - Bill Payments – work has commenced on the re-assessment. Legal have provided a draft view that Post Office is not directly regulated for these services, however, a number of contracts are incomplete or missing and this will hinder work to understand any contractual obligations that Post Office may have in relation to financial crime. HMRC will be advised of the legal view so that the current premises registration requirements can be amended.
    - POMS – Risk Assessment and ABC Risk Assessment were completed and provided to POMS in May

12. Non-conformance issues in the Network in Q1 2017/18 include 54 incidents identified at 48 branches (see Appendix B for details):
    - 17 branches are on the non-conformance watch list and manually monitored monthly
    - 2 branches have been added this quarter
    - 1 branch has been removed this quarter
    - 2 branches with reduced ID threshold had their limit reduced lower following further breaches

Anti-Bribery and Corruption (ABC) Risk Assessment update

13. The action plan in Appendix B gives full updates, but in summary:
    - ABC policy – R&CC paper submitted for review and sign-off at July 2017 meeting.
    - Gifts and Hospitality reporting tool has been designed and built, and should be ready to implement on 1st August 2017. It will be accessed via the Intranet, together with documented procedures.

- Gifts and Hospitality Register Report for 2016/17 submitted to July 2017 R&CC for noting.
- ABC training content has been prepared and is due to launch in September 2017.

AML/CTF training update

14. Back Office training completion is 97.5% with 44 individuals still to complete as at 11th July 2017. Prior to the latest figures received on the 11th July 2017 the HR Director had written to the GE members asking for any non-conformance to be managed through the disciplinary process.

15. Network training is currently at 95.8%. A final MBS has been targeted to the branches that have not completed and this will be followed up by a letter warning of a chargeable visit if non-conformance continues. This is being proactively managed by the Branch Standards Team.

Regulatory updates

16. The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 came into force on Monday 26th June 2017. HMRC have published some interim guidance for Money Service Businesses in relation to the new legislation and the new Fit & Proper test requirements, but further clarity is required:

    - eKYC - HMRC Money Service Business Guidelines suggest that copies of paper primary and secondary ID documentation for customer due diligence need to be retained during the relationship (i.e. where customer due diligence has been performed) and for 5 years after a relationship has terminated. This is contrary to the guidance from the JMLSG[1] which specifically states that "Firms may choose to use electronic/digital identity checks where this is possible, either on their own or in conjunction with documentary evidence". We attended an HMRC MSB forum on the regulations on Wednesday 28th June at which their Policy Team talked through their interpretation of the new regulations, and confirmed that copies of paper documentation must be retained. Further clarification was requested from our HMRC supervisor at the meeting on Thursday 29th June, and the HMRC Policy advice was again confirmed.

      We are currently obtaining an external legal review of the regulations and the guidance, and will look to use this to challenge the view of the HMRC Policy Team. The requirement to retain either physical or electronic copies of customer ID&V has severe implications for Post Office (we would not want to retain physical paper copies in branch for 5 years for data protection reasons, and branches do not currently have the capability to scan and submit electronic copies).

    - Fit & Proper test - The new regulations impose an obligation on firms to ensure that those providing MSB services are 'fit & Proper'. However it is clear from both the HMRC MSB forum and the meeting with our supervisor, that HMRC

[1] The Joint Money Laundering Steering Group (JMLSG) is made up of the leading UK Trade Associations in the Financial Services Industry. Its aim is to promote good practice in countering money laundering and to give practical assistance in interpreting the UK Money Laundering Regulations. This is primarily achieved by the publication of industry guidance.

do not yet have an agreed approach to the requirements of the Fit & Proper regime, and whilst they have now published some interim guidelines, they will hold a consultation in the autumn relating to the re-testing requirements of Fit & Proper (currently there are none) and the amount of the fee. The impact for Post Office could be material depending on the outcome of the consultation and the interpretation of the requirements. For example, whether the regulations would apply to all existing agents or just new agents; what tests will need to be done; what the fees will be; and how the term 'agent' will be interpreted for Post Office and its agents (e.g. the extent to which we would need to verify the 'Fit & Proper' status of the staff, directors, beneficial owners, shareholders of multiples as well as individual agents, etc.).

We are collating details of the 'Fit & Proper' tests that are currently conducted by Post Office in relation to its own staff and across the different types of agents with a view to being able to demonstrate the level of regulatory compliance that is currently in place under the AR arrangements for each of BOI and POMS, and the potential gap between those existing requirements and those contemplated by HMRC. The output from this exercise will be discussed with relevant stakeholders and will help to inform the response that goes to the HMRC Policy Team. We have been advised that a formal response from the HMRC Policy Team would normally take about 30 days.

Post Office have until the date of our next annual registration (1st June 2018) to comply with these new requirements.

17. Any penalty levied in relation to the new regulations will be published without delay and remain on the HMRC website for 5 years. Penalties in relation to breaches arising under the previous regulations would be captured by the prior regulations and therefore not made public.

18. Post Office will need to ensure that all relevant risk assessments, polices and processes are fully documented and kept up to date. These policies, controls and procedures must include risk management practices, internal controls, customer due diligence and the monitoring and management of compliance with these.

19. The full JMLSG and HMRC MSB guidance on the new regulations are currently under review by the Financial Crime Team to ensure there are no other immediate impacts.

20. There has been no further guidance or update relating to the Fifth Money Laundering Directive announced on 30 November 2016 and the updates given in March remain current.

21. A working group has been set up by Legal with support from Financial Crime to review The Criminal Finances Act 2017 (new corporate strict liability offence) which comes into force in September, and ensure that a documented risk assessment is produced and measures put in place to establish a defence for Post Office. The primary risk relates to the criminal facilitation of criminal tax evasion by a Post Office 'associated person', although this is currently deemed to be low risk.

External threats

22. The four recent terrorist attacks in the UK (Westminster Bridge, Manchester, London Bridge and Finsbury Park Mosque) saw financial investigations being co-ordinated via the Joint Money Laundering Intelligence Taskforce members.

23. In all, 13 requests for information were responded to by members (including Post Office) in the hours after each event, which collectively resulted in c.70 positive responses. These have assisted law enforcement to piece together the events that led up to these attacks.

24. Prior to these attacks, the main terrorist finance red flags were to help identify funding activity for overseas terror groups, funding the outward or inward journeys of terrorist fighters, and the funding and activities of groups that preach or incite racial hatred. C. 40% of this terrorist financing is financed by low level criminality, basic fraud and robbery. Overseas terror group funding is frequently linked to charities, whose donors believe that the funds are being used for humanitarian purposes.

25. From the four recent UK attacks and others in mainland Europe, it is likely that security services will require the financial services industry to be able to do more to review 'pattern of life' activity, and focus more on domestic activity. This is because in these incidents the transactions were small, money was obtained and used quickly, often in cash or through other instruments like prepaid cards and gift cards. The transactions are also consistent with normal activity – hiring vehicles, booking hotel rooms, buying kitchen equipment (knives) from supermarkets. The NCA have also advised that monitoring activity will be more about named individuals, and there is an expectation that there will need to be some regulatory or legislative changes to facilitate this.

26. From a Post Office perspective, risk assessment and financial crime work continues to focus activity on the products and services deemed to be high risk or anonymous. Following a recent incident where a branch Officer in Charge appears to have absconded to the Yemen via Oman with c.£400k from the Post Office, the Financial Crime Team are supporting work being undertaken by the Network Operations Director to review agent on-boarding screening and ensure that the terrorist finance threat is understood.

POL00401625

Appendix A – Action Plan

PROJECT / SPECIFIC TASK	STATUS	COMPLETION DATE	WEEKLY UPDATE
ABC Training - All Staff	In Progress	31/10/2017	07/07/2017 Training content is currently being drafted.
Gifts & Hospitality Procedures and Comms Review	In Progress	31/08/2017	04/07/2017 Procedures have been drafted and are under review.
AML/CTF Policy Review (for Sept RCC/ARC)	In Progress	31/07/2017	05/07/2017 4MLD has now been published. Guidance is being reviewed and the policy update and analysis is underway.
Whistleblowing Process overview	In Progress	31/07/2017	03/07/17 Currently reviewing case examples from Executive Correspondence Team and Grapevine, in order to draft a process and appropriate Comms for the teams.
RAT Ref 2016/4 - Digital Wallet	In Progress	30/08/2017	07/07/17 Product Manager (Martin Thackray) is reviewing the product proposition to ensure compliance with regulations (including 4thMLR). Follow up meeting scheduled for July.
RAT Ref 2015/7 - Digital Passport/ Digital Check & Send	In Progress	31/07/2017	08/06/17 The project is now named Digital Check & Send. It is approaching the final stages of its Assess phase. The high level document has just been completed and requests for supplier proposal design are being sought.
RAT Ref 2016/10 - Network Development Hot House 5	In Progress	31/07/2017	07/07/17 Financial Crime have no concerns with proposed service. Project is part of the Transaction Simplification project.

POL00401625

PROJECT / SPECIFIC TASK	STATUS	COMPLETION DATE	WEEKLY UPDATE
RAT Ref 2017/4 - Smart Metering	In Progress	30/09/2017	07/07/17 Smart Metering project go live has been delayed. It is expected the generic Smart Meter Hub and SSE (energy company) Hub will go live in August 17. Npower is expected to go live in September and other energy providers to follow after this.
RAT Ref 2017/6 Change Giving Lite	In Progress	30/09/2017	07/07/17 Risk assessment has been completed and reviewed. Only concern raised is regarding remuneration of the service - this is still yet to be decided.
Review of POMS Compliance Meetings	In Progress	30/09/2017	03/07/17 First call completed on 30.06.17 with POMS Compliance, Financial Crime and Chris Russell (DPA). Terms of reference discussed and agreed. POMS Compliance advised that they have suspended branch monitoring pending a full process review.
Non-Conformance Process Review	In Progress	31/07/2017	07/07/17 Contracts Team have agreed the new non-conformance process and SLA's. This will be reviewed after 3 months. The new process has been presented to the South Team with the North Team is scheduled for July. Expected go live date 01/08/17.
Cash Centre Referral Process Review	In Progress	31/07/2017	07/07/17 A proposed process has been shared and active discussions held with the Cash Centre teams. Looking to agree new process in July.
Branch Premises Registration Policy & Procedures Review	In Progress	30/07/2017	06/07/207 Most recent fortnightly premises registration updates received from Network Design Team on 01/07. There are a few minor keying errors that need to be addressed before forwarding to HMRC.

Santander Business Deposits	In Progress	14/07/2017	04/07/2017 Report detailing concerns is currently with Sally Smith for review.
PROJECT / SPECIFIC TASK	**STATUS**	**COMPLETION DATE**	**WEEKLY UPDATE**
Deferred Checking	In Progress	TBC	07/07/17 Some concerns have been raised regarding this proposed service. Ongoing discussions are occurring with the Product and Project Managers to address.

Appendix B – Branch Non-Conformance P1-3 2017/18

Month Identified	Branch	Issue	Action
April	Wyton RAF Station	- A customer breached the £10k limit and purchased $36,090 split into three transactions on the same day. - Funds were to pay for a group Ministry of Defence Skydiving trip. - Branch claimed the Cash Centre had given approval to go ahead with the transactions.	- Investigation and telephone interview completed by the Financial Crime team. - Remedy Letter sent to PM by the Contracts Manager. - A referral process is under review between the Cash Centre and the Financial Crime Team.
April	Multiple Branches (London Area)	- Fraud Analysis Team identified a group of customers committing high volume of Bureau de Change card fraud. - They targeted various branches in the London area. - 4 out 14 customers had breached the £10,000 limit across multiple branches.	– Investigation and telephone interview completed by the Financial Crime team. – Referral to card issuers. – Information passed onto police for a criminal investigation to be undertaken. – Grapevine contacted branches to request CCTV footage. – Manual monthly monitoring is being completed.
April	Middlesbrough	- A customer purchased £60,000 worth of Sterling Travellers Cheques (£10,000 x6) on one visit. - Branch breached £10,000 limit.	- Product Manager contacted American Express regarding breach. - Financial Crime Team investigation and branch telephone interview completed. - Area Sales Manager notified and non-conformance addressed with the branch.
May	Marsh	- Branch sold £15,000 to a customer for business use - For all 3 transactions, the clerk inputted his own information and ID details as the customer did not have his. - Historic data showed that the clerk had previously done this in 2014 and 2015.	– Investigation and telephone interview completed by the Financial Crime Team. – Reduced ID threshold of £1,500 imposed – Manual monthly monitoring is being completed. – Remedy Letter sent to PM by the Contracts Manager.

Month Identified	Branch	Issue	Action
May	Nyetimber	- FRES reported concerns that a customer had breached card limit by purchasing 4 Multi Currency Cards (maximum 3 per customer) - Each card had reached the following limits; Load limit of £5,000, Balance held of £10,000, and Annual balance of £30,000.	- Investigation and telephone interview completed by the Financial Crime Team. - Information shared with FRES to support their investigation. - Remedy Letter sent to PM by the Contracts Manager.
May	London Road	- Executive customer complaint that this branch was unable to provide a Bureau de Change refund. - Branch failed to follow correct process and were issuing quote receipts rather than sale receipts to customers.	- Investigation and telephone interview completed by the Financial Crime Team. - Information shared with FRES to support their investigation. - Remedy Letter sent to PM by the Contracts Manager. - Concerns raised with the Product Manager and complaint resolved
May	St Stephens Parade	- FRES shared concerns that the branch had a high average Bureau de Change transaction sales value but low sales volume - High value card transactions confirmed as fraudulent	- Ongoing investigation with the following planned actions: ▪ Reduced ID threshold of £2,000 imposed manual monthly monitoring ▪ Remedy Letter to be sent to PM by the Contracts Manager.
June	Stowmarket	- FRES shared concerns that the branch had sold more than £10,000 worth of US Dollars to an individual customer.	- Investigation and telephone interview completed by the Financial Crime Team. - Information shared with FRES to support their investigation. - Remedy Letter sent to PM by the Contracts Manager. - PEPs and Sanction check completed by the Fraud Analysis Team. - Branch Standards Team confirmed branch AML training completion.
June	Keswick	- FRES raised concerns that a Postmaster was processing Bureau de Change sales for customers but recording his own ID details - Postmaster paid using his own card and accepted cash from the customers for each order - Postmaster has processed transactions in excess of £10,000.	- Ongoing investigation with the following planned actions: ▪ Reduced ID threshold of £2,000 imposed ▪ Manual monthly monitoring ▪ Remedy Letter to be sent to PM by the Contracts Manager.

Month Identified	**Branch**	**Issue**	**Action**
June	Kentish Town	- Branch on Non-Conformance Watchlist with a reduced ID threshold. - Branch still continued to non-conform to Bureau de Change requirements.	- Investigation and telephone interview completed by the Financial Crime Team. - ID threshold has been further reduced to £2,000. - Manual monthly monitoring is being completed. - Remedy Letter sent to PM by the Contracts Manager.
June	Rugby	- Branch on Non-Conformance Watchlist with a reduced ID threshold. - Branch still continued to non-conform to Bureau de Change requirements.	- Investigation and telephone interview completed by the Financial Crime Team. - ID threshold has been further reduced £1,500. - Manual monthly monitoring is being completed. - Remedy Letter sent to PM by the Contracts Manager.
June	Dewsbury	- Branch on Non-Conformance Watchlist with a reduced ID threshold. - Branch still continued to non-conform to Bureau de Change requirements.	- Investigation and telephone interview completed by the Financial Crime team. - ID threshold has been further reduced to £1,500 - Manual monthly monitoring is being completed. - Remedy Letter sent to PM by the Contracts Manager.

3.4 Gifts & Hospitality 2016-17 Review

Author: Paul Blackmore and Thomas Richmond Sponsor: Jane MacLeod Meeting Date: 20th July 2017

Executive Summary

Context

As part of our annual Anti-Bribery and Anti-Corruption (ABC) obligations, this paper provides an overview of the Gifts & Hospitality reporting for the period 2016-17.

Questions addressed in this paper

- What issues have been highlighted based upon the review?
- What actions need to be undertaken to cover any issues?

Conclusion

1. Whilst there have been breaches relating to the adherence to the policy, we have not identified any instances indicative of Bribery or Corruption.

2. As part of an external Risk Assessment completed by Thistle Initiatives a number of recommendations to improve our controls have been made.

3. The majority of Gifts & Hospitality has been reported by senior managers or above, however in most instances the agreed policy threshold has been breached or an amount has not been reported. This highlights that the present Gifts & Hospitality thresholds are either too low or that senior staff are not querying and clarifying the amount prior to accepting an offer.

Input Sought

This report provides an overview of Gifts & Hospitality for the period 2016-17 and to propose amendments to the existing reporting limits.

The Report

Summary of ABC activities relating to Gifts & Hospitality reporting 2016-17

1. During 2016-17 Thistle Initiatives conducted a full risk assessment and gap analysis of Post Office Limited and Post Office Management Services Limited's risk exposure and existing control strength.
2. At the end of 2016 Anti-Bribery and Anti-Corruption training was delivered to directly employed staff via SuccessFactors Learning and Orbit.
3. Financial Crime Team has reviewed Gifts & Hospitality across the group and has identified a number of policy breaches. These breaches have led to the design and development of a simple reporting tool.

Summary of Gifts & Hospitality received and offered 2016-17

4. Analysis of the 2016-17 Gifts & Hospitality Register (please see Appendix A) has highlighted that the quality of the submissions made during this period has been very poor. For example there were a number of inconsistent reporting standards:
   - Value not recorded in all instances.
   - Full details of the offering/receiving company not recorded.
   - Unclear business rationale for acceptance of hospitality.
   - Lack of Line Manager/GE approval.
   - Unable to identify employees' business areas.
5. Within the register a number of breaches were identified; for example a member of staff appears to have accepted a cash gift of £100. Whilst the member of staff reported the gift, cash gifts should never be accepted in any circumstances and as such should have been returned to the customer. This should also have been reiterated to the member of staff after the report was submitted.
6. A large number of hospitality is recorded at above the agreed thresholds without corresponding Line Manager/GE approval.
7. Due to the inconsistencies in recording we have been unable to provide an accurate reflection of the volume and value of Gifts & Hospitality offered and received (please see Appendix B).

Actions to address:

8. The following activity is planned, to address the issues identified:
   - The Gift & Hospitality reporting limits are to be amended as follows:

	Existing Reporting Limit	New Reporting Limit
Gifts	£200	£100
Hospitality	£100	£200

   - The Anti-Bribery & Anti-Corruption Policy has been updated to include reporting guidance, clarity of amounts and line manager or GE approval limits.
   - An online reporting tool, associated documented guidance and procedures have been created and will be published on the intranet with links to the applicable policies and processes.
   - Enhanced Anti-Bribery and Anti-Corruption training will be delivered to all employees in September 2017.
   - A compliance monitoring programme has been established.
   - Anti-Bribery and Anti-Corruption has been added to the half yearly GE declaration.
   - Each GE member will receive a quarterly report showing the Gifts & Hospitality in their business area.

Appendix A

The below tables sets out by Business Team the Volume and aggregated total Value of Gifts & Hospitality received in 2016-17 business year. The value field is blank where we are aware that an offer of hospitality or a gift has been accepted however the figure has not been provided.

Business Team	Volume	Aggregated Value
Chief Financial Officer	1	£ -
Business Transformation	4	£ 2,120.00
Commercial Director	2	£ -
Financial Services Director	22	£ 175.00
Personal Assistant to Nick Kennett	2	£ -
Group People Director	1	£ -
Network & Sales Director	1	£ -
Corporate Services	1	£ -
Finance Director	16	£ -
Legal	10	£ 264.00
Mediation	1	£ -
Group	2	£ -
ISAG	2	£ 50.00
Network	13	£ 150.00
IT	4	£ 82.00
Financial Specialist	1	£ 20.00
Commercial	2	£ 50.00
Security	9	£ 220.00
Post Office Money	14	£ 994.00
Risk	2	£ 100.00
Internal Audit	1	£ 100.00
Fleet Contracts	1	£ -
Cosec	3	£ -
Studio & Social Media	2	£ -
Property	1	£ -
Branch Support Services Team	1	£ -
Supply Chain	2	£ -
Procurement	2	£ 200.00
Finance	1	£ -
Operations	7	£ 20.00
Vendor Management	1	£ -
Marketing	5	£ -
Sales	2	£ -
Branch Standards team	1	£ -
Financial Services	4	£ 100.00

Appendix B

Gifts		**Hospitality**	
Total volume	17	*Total volume*	128
Total value	£230.00	*Total value*	£5,475.55
Amount without value recorded	7	*Amount without value recorded*	100
Amount with value recorded	10	*Amount with value recorded*	28
Declined	1	*Declined*	14
Value within policy amount (<£200)	10	*Value within policy amount (<£100)*	23
Value above policy amount (>£200)	0	*Value above policy amount (>£100)*	5
Policy Breaches	1 – acceptance of £100 cash	*Policy breaches*	0

Comments

Due to the inconsistencies in the information captured we have not been able to properly analyse the data and also owing to the business wide restructure it is also difficult to establish the separate business areas. The focus now therefore is to put this right culturally.

POST OFFICE
Risk & Compliance Committee

PAGE 1 OF 9

CONSIDERATION PAPER

3.5 IT Controls Update

Author: Sharon Gilkes Sponsor: Rob Houghton Meeting date: 20th July 2017

Executive Summary

Context

PO IT have embarked on the development of the IT Control Framework (ITCF), the programme commenced in January 2017 supported and advised by KPMG. The objective of the ITCF is to improve IT controls for managing IT operational services.

Since the commencement of this programme, the focus has been on implementing a sustainable ITCF that maps end to end IT processes and risks, identifies remediating controls, and introduces evidenced self-assessment and monitoring. The purpose of this paper is to update the RCC on the progress made in implementing the ITCF, and the priorities for the next quarter.

Questions addressed in this paper

- What progress has been made in implementing the IT Control Framework?
- Will the ITCF improve our ability to manage IT operational risks?
- What are the next steps, and when do we expect to complete the work?

Conclusion

The development of the ITCF, based on COBIT5, is on track. Working with our core suppliers (Accenture, Fujitsu, Atos, Verizon and Computacenter), all 11 priority Cobit 5 processes (Tranche 1) have been reviewed with core suppliers controls identified, and gap assessments completed. Some 123 control gaps are open, of which 61 are considered risk. Self-assessment technology is in place, and a number of process owners have been identified.

By the end of March 2018, we expect all gaps for Tranche 1 to have been identified and remediated, or at least have work-around controls. In addition, every control will have been through at least one round of self-assessment, and every process will have had a sample of controls independently assessed either by external auditors, EY annual audit, or by PO Internal Audit.

Input Sought

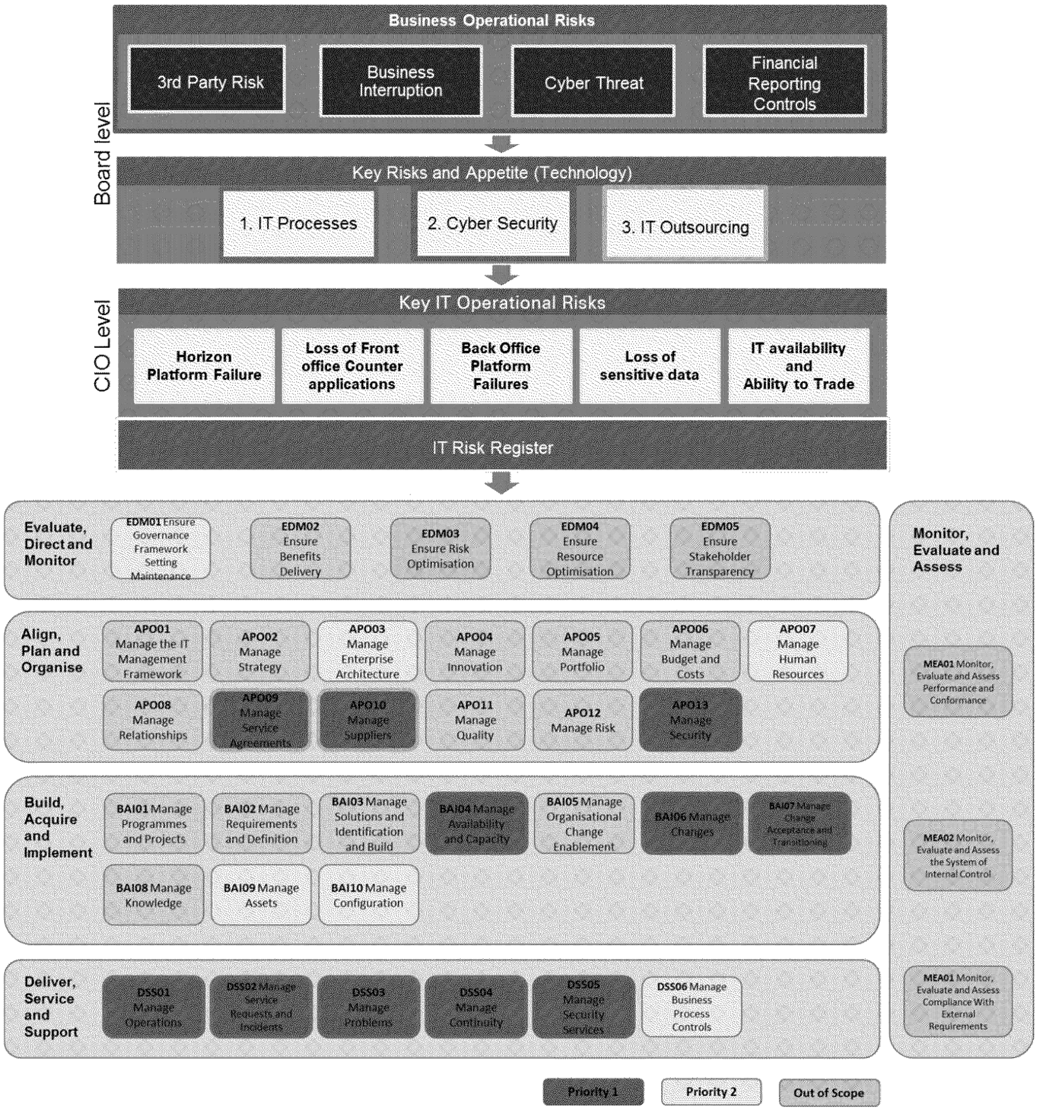
The RCC is asked to note the progress made and comment on the priorities and approach.

Strictly Confidential

The Report

What progress has been made in implementing the IT Control Framework?

1. The creation of the ITCF followed a standard methodology (Appendix 1). The scope of the ITCF, with line of sight from individual controls to board level risks, can be summarised as set out in the diagram below. The priority focus for Tranche 1 highlighted in green.


Board level
Business Operational Risks
3rd Party Risk
Business Interruption
Cyber Threat
Financial Reporting Controls
Key Risks and Appetite (Technology)
1. IT Processes
2. Cyber Security
3. IT Outsourcing
CIO Level
Key IT Operational Risks
Horizon Platform Failure
Loss of Front office Counter applications
Back Office Platform Failures
Loss of sensitive data
IT availability and Ability to Trade
IT Risk Register
Evaluate, Direct and Monitor
EDM01 Ensure Governance Framework Setting Maintenance
EDM02 Ensure Benefits Delivery
EDM03 Ensure Risk Optimisation
EDM04 Ensure Resource Optimisation
EDM05 Ensure Stakeholder Transparency
Align, Plan and Organise
APO01 Manage the IT Management Framework
APO02 Manage Strategy
APO03 Manage Enterprise Architecture
APO04 Manage Innovation
APO05 Manage Portfolio
APO06 Manage Budget and Costs
APO07 Manage Human Resources
APO08 Manage Relationships
APO09 Manage Service Agreements
APO10 Manage Suppliers
APO11 Manage Quality
APO12 Manage Risk
APO13 Manage Security
Build, Acquire and Implement
BAI01 Manage Programmes and Projects
BAI02 Manage Requirements and Definition
BAI03 Manage Solutions and Identification and Build
BAI04 Manage Availability and Capacity
BAI05 Manage Organisational Change Enablement
BAI06 Manage Changes
BAI07 Manage Change Acceptance and Transitioning
BAI08 Manage Knowledge
BAI09 Manage Assets
BAI10 Manage Configuration
Deliver, Service and Support
DSS01 Manage Operations
DSS02 Manage Service Requests and Incidents
DSS03 Manage Problems
DSS04 Manage Continuity
DSS05 Manage Security Services
DSS06 Manage Business Process Controls
Monitor, Evaluate and Assess
MEA01 Monitor, Evaluate and Assess Performance and Conformance
MEA02 Monitor, Evaluate and Assess the System of Internal Control
MEA01 Monitor, Evaluate and Assess Compliance With External Requirements
Priority 1
Priority 2
Out of Scope

2. In summary, for the areas marked green, with the support of KPMG, the following steps have been undertaken:

    a. Gap Analysis has been formally documented

    b. Risk and Control Matrices (RACMs) have been created

    c. Controls have been assessed and gaps identified

    d. Process and control owners have been identified

3. Overall, 225 controls and 123 control gaps have been identified. The gaps were graded by impact, with 61 having high impact, 46 medium, and 16 low – low risk gaps are typical where we believe that an effective control is in operation but the evidence is not routinely collected. We are currently reviewing the priority of these gaps and expect a significant decrease in the number of high-rated gaps as we work through the remediation plans with the process owners:

RACM	**No. Cntrls (of which key)**	**No. Gaps (of which in key controls)**	**H**	**M**	**L**
1. Manage Changes	19 (10)	16 (6)	5	7	4
2. Manage Service Requests and Incidents	21 (12)	23 (14)	11	8	4
3. Manage Problems	25 (17)	17 (10)	3	12	2
4. Manage Security	9 (5)	3 (3)	3	0	0
5. Manage Security Services	33 (27)	27 (24)	16	10	1
6. Manage Change and Acceptance Testing	21 (11)	12 (9)	9	1	2
7. Manage Service Agreements	12 (5)	6 (3)	1	2	3
8. Manage Suppliers	13 (8)	4 (4)	3	1	0
9. Manage Availability and Capacity	14 (7)	5 (5)	3	2	0
10. Manage Continuity	20 (13)	6 (6)	5	1	0
11. Manage Operations	28 (12)	4 (2)	2	2	0
Total Gaps		123 (86)	61	46	16

4. A number of controls have remediation plans underway, at the moment we are in Phase 3 of the project and are currently reviewing the remediation plans to ensure we can determine the Who, What, and how against each control/remediation. We have provided a list of activities below that will support the full control when complete in the Phase 4 of the project

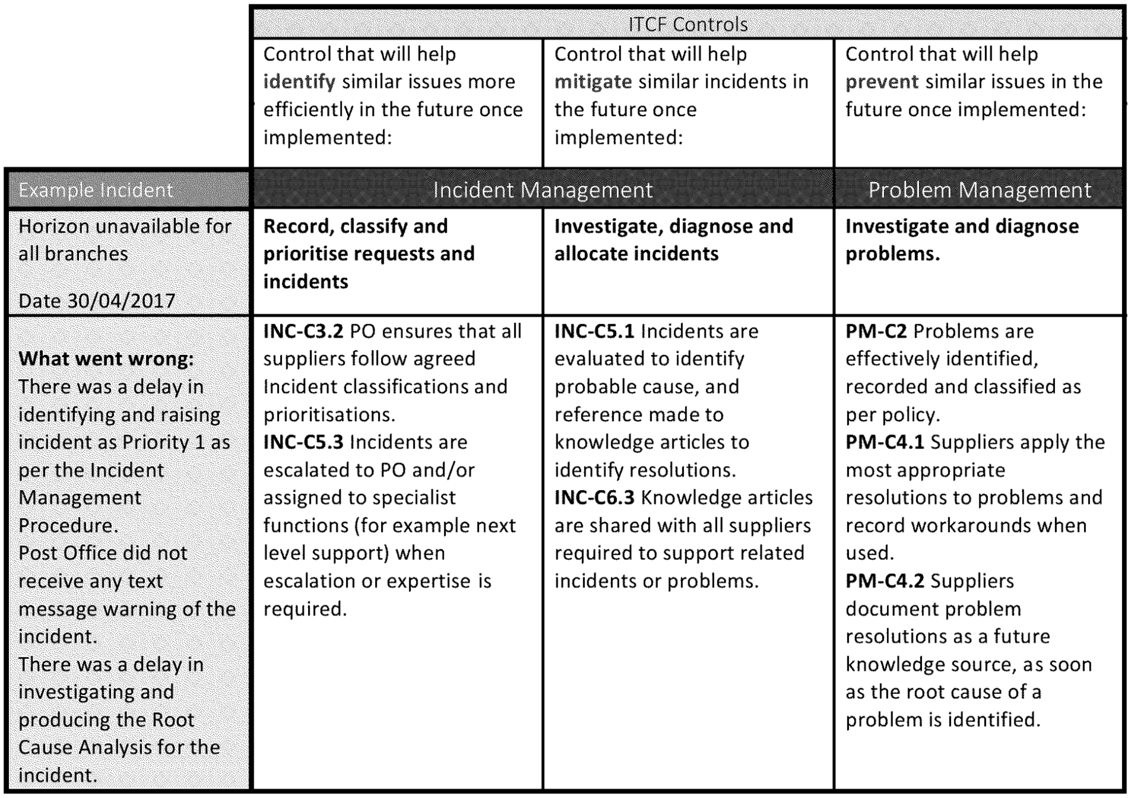
Key Control Dependencies	Action
There isn't a catalogue of services in place with details of accountable owners and support teams	A library of service maps is currently being developed. This will provide an accurate understanding of the service topology empowering employees to determine which business services are affected by component-specific changes, failures of performance issues.

Demand management information is not being provided to supply chain members, which inhibits forecasting and trend analysis, as acknowledged by Accenture and ComputaCenter	Recruitment of a Portfolio Manager to address the gaps highlighted in the Available and Capacity Process. The Portfolio manager will; -improve resource Allocation -improve alignment of work -increased collaboration
Several gaps were highlighted around the Service Management tool which is used by Atos (SDM12).	Several Gaps were highlighted from core suppliers and internal Post Office colleagues around the lack of a service management tool which gives visibility management information throughout the lifecycle. Activity is currently underway to introduce a new service management tool, timelines are yet to be determined. The tool will provide: - modernisation of IT Service Management using a cloud base tool - provide visibility of the status of service to the business at a glance - assign incidents to the correct resolver groups and hand over of incidents to be slicker
There is lack of knowledge available for the levels of Disaster Recovery against our core suppliers.	Work is underway to implement a Disaster Recovery Framework. The purpose of this is to ensure the business understands the recovery time objectives and DR test frequency, which will reduce the risk of key tests being delayed. Any postponement of a test will now require business sign off.

Will the ITCF improve our ability to manage risks?

5. To be able to assess if IT Controls would have been successful in managing risk to the business, we have inspected a number of historical incidents; what went wrong, and what approach was taken to resolve and address these incidents. We can confirm that, had the ITCF controls been in place at the time of the incident, the overall business risk would have been lower.

6. The examples below illustrates two aspects of what went wrong during a recent incident with Horizon downtime. We have summarised ITCF controls that will help identify, mitigate and prevent similar incidents in the future. If the controls were in place at the point of the incident, the impact would have been reduced if not totally eradicated. The incidents, if not prevented in the first place, would have been identified more quickly and the severity would have been smaller.



	ITCF Controls		
	Control that will help **identify** similar issues more efficiently in the future once implemented:	Control that will help **mitigate** similar incidents in the future once implemented:	Control that will help **prevent** similar issues in the future once implemented:
Example Incident	Incident Management		Problem Management
Horizon unavailable for all branches Date 30/04/2017	**Record, classify and prioritise requests and incidents**	**Investigate, diagnose and allocate incidents**	**Investigate and diagnose problems.**
What went wrong: There was a delay in identifying and raising incident as Priority 1 as per the Incident Management Procedure. Post Office did not receive any text message warning of the incident. There was a delay in investigating and producing the Root Cause Analysis for the incident.	**INC-C3.2** PO ensures that all suppliers follow agreed Incident classifications and prioritisations. **INC-C5.3** Incidents are escalated to PO and/or assigned to specialist functions (for example next level support) when escalation or expertise is required.	**INC-C5.1** Incidents are evaluated to identify probable cause, and reference made to knowledge articles to identify resolutions. **INC-C6.3** Knowledge articles are shared with all suppliers required to support related incidents or problems.	**PM-C2** Problems are effectively identified, recorded and classified as per policy. **PM-C4.1** Suppliers apply the most appropriate resolutions to problems and record workarounds when used. **PM-C4.2** Suppliers document problem resolutions as a future knowledge source, as soon as the root cause of a problem is identified.

POL00401625

	ITCF Controls		
	Control that will help **identify** similar issues more efficiently in the future once implemented:	Control that will help **mitigate** similar incidents in the future once implemented:	Control that will help **prevent** similar issues in the future once implemented:
Example Incident	Change Management		
Horizon unavailable for all branches Date 30/04/2017	**Solution and user documentation is reviewed and updated.**	**Plan, evaluate, assess and approve change requests**	**Schedule and test changes before implementation**
What went wrong: WEB GUI process enhancements that were running in the background at the time the Fujitsu employee logged onto the system have not been properly assessed and tested for impact as part of a change management procedure.	**CHM-C3.3** PO Change Advisory Board (CAB) is responsible for ensuring changes are evaluated and assessed reviewed by affected parties/stakeholders and either approved or rejected. Risk and Impact assessment completed and rationale documented as a part of the RFC process.	**CHM-C7.2** Where change testing results in a failure, a post-implementation report is prepared and submitted to the PO service manager for review and record. The change should be closed and not implemented.	**CHM-C4.1** All changes are tested in a test environment against documented acceptance criteria. **CHM-C4.2** Business-sign off for acceptance of test results must be recorded in the change management tool before implementation of the change, for audit trail purposes.

Next Steps

7. Train all control owners on their new accountabilities by end October 2017

8. Rectify the Tranche 1 identified high-gaps with remediation plans. This is scheduled to be completed in most cases during Q2 and entirely by end of Q3.

9. Validate control designs and gaps with control owners and expand control design to include defined control operators and audit trail.

10. Test scripts for Tranche 1 controls will be documented to test operating effectiveness of controls and support ongoing self-assessment by end September 2017.

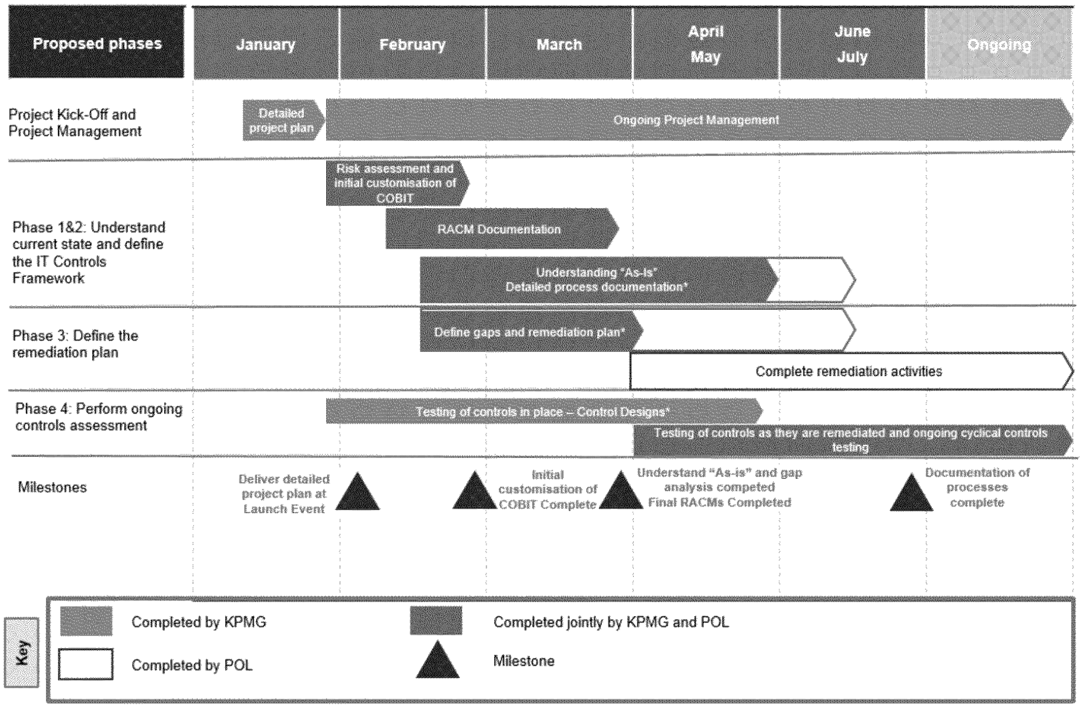
11. The RACMS have been formatted to align with the existing financial controls already in use in the self-assessment tool, (TrAction). Discussions will take place over the next month obtain user access for control owners within IT.

12. Agree an approach to operationalising the process of self-assessment and testing for the ITCF. Based on experience, this may require off-shoring the capability to a 3rd party partner.

13. Tranche 2 process controls have not yet been started, and represent the priorities for the remainder of the fiscal year, in the following order: manage assets; manage business process controls; governance framework; enterprise architecture; manage configuration; human resources. Gap analysis and remediation is expected to be complete by end December 2017

14. All processes will have had some sample checking of self-assessment through external auditors' annual audit by end February 2018.

15. In summary, we expect to have controls operating against all identified key risks by fiscal year end, with every control having been through at least one round of self-assessment and sample audit checks undertaken on each process.


Proposed phases
January
February
March
April
May
June
July
Ongoing
Project Kick-Off and Project Management
Detailed project plan
Ongoing Project Management
Phase 1&2: Understand current state and define the IT Controls Framework
Risk assessment and initial customisation of COBIT
RACM Documentation
Understanding "As-is"
Detailed process documentation*
Phase 3: Define the remediation plan
Define gaps and remediation plan*
Complete remediation activities
Phase 4: Perform ongoing controls assessment
Testing of controls in place – Control Designs*
Testing of controls as they are remediated and ongoing cyclical controls testing
Milestones
Deliver detailed project plan at Launch Event
Initial customisation of COBIT Complete
Understand "As-is" and gap analysis competed
Final RACMs Completed
Documentation of processes complete
Key
Completed by KPMG
Completed jointly by KPMG and POL
Completed by POL
Milestone

* Includes walkthroughs with relevant suppliers

Appendix 1: ITCF Methodology and Progress

Phase	Description	Status
Phase 0 Detailed Planning	- Defined a detail plan and scope of the project. - Roles and responsibilities and governance framework defined	Complete
Phase 1 Understand Current State	- Refinement of COBIT5 to more appropriately align to POL's needs. - 60 walk through sessions have taken place, all core suppliers walkthroughs are now complete. - Perform gap analysis, consolidating gaps identified across suppliers	Complete
Phase 2 Define the IT Controls Framework	- Documentation of control design for all 11 RACM's has been completed for each process. - The RACMs have been designed to mirror the Financial Controls format, to ensure consistency when the information is uploaded into the self-assessment tool (TrAction). - We are working through comments from Internal Audit and control owners in their review of the RACMs	Largely complete
Phase 3 Define remediation plan	- Work in progress with process owners, control owners and third parties to agree remediation activities for identified gaps. - Remediation activities will be prioritised and timelines assigned to support the completion of the activity.	Ongoing
Phase 4 Ongoing controls self-assessment	- Testing of controls found to be already in place. - Testing of controls as they are remediated - Development of test scripts and training of POL Staff to enable ongoing control testing. - Dashboard-based monitoring will provide clear status updates to management.	start date mid July

Appendix 2: Terminology

Term	Description
Process	COBIT defines 37 ‘processes’ which include ‘management practises’ over different areas of IT Service Delivery, including both control and process steps.
Control	Set of activities which mitigate risk.
Gap	Reflects weakness, issue or deficiency in a control, where the identified risk is only partially covered or not addressed at all.

3.5 IT Risk Management

Authors: Rebecca Barker   Sponsor: Rob Houghton   Meeting date: 20th July 2017

Executive Summary

Context

This briefing paper forms an update on our management of IT operational service risk, which was highlighted as an area of concern in the Technology Strategy paper to the PO Board in January 2017. At that time, we outlined that we remained outside of our risk appetite zone in key operational areas. After gaining a better understanding of our operational risk, and more detailed planning on infrastructure related change programmes, this paper is an update on how we are focused on reducing these risks over time.

Question addressed in this report.

1. What is the scope of our operational risks?
2. How will we reduce our risks and when will we be within our risk appetite?
3. What are the key activities required to mitigate our risks?
4. What are the next steps for IT Risk Management?

Conclusion

- We remain outside of our risk appetite in key operational areas
- Infrastructure related change programmes are focused on reducing these risks over time.
- Security Transformation programmes are reducing the risk of cyber-attacks and security breaches, whilst the introduction of an Operational Command Centre will enable real-time monitoring of critical applications
- Mitigation actions have been identified and are being addressed to minimise risks
- In addition, a process for creating risk awareness (including risk evaluation and risk management) will be established

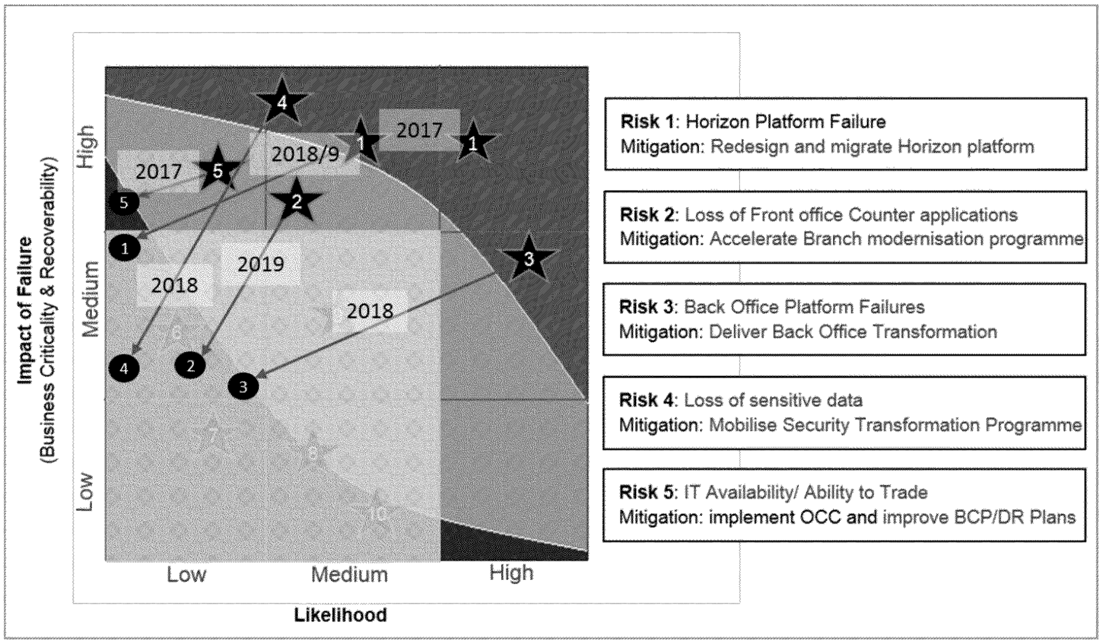
Input Sought

The RCC is asked to note the progress made, and comment on observations and approach.

The Report

What is the scope of our operational risk?

1. The Technology Strategy outlined a view that we remain outside of our risk appetite zone in key operational areas. Five key IT operational risks were called out, which required closer monitoring and management of mitigation controls, with a timeline for bringing those risks into our risk appetite zone:



Risk 1: Horizon Platform Failure
Mitigation: Redesign and migrate Horizon platform

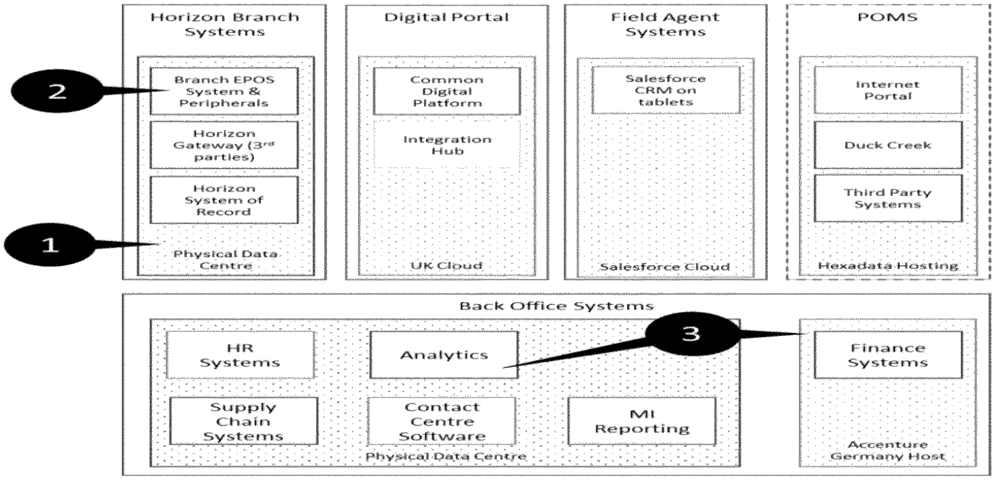
Risk 2: Loss of Front office Counter applications
Mitigation: Accelerate Branch modernisation programme

Risk 3: Back Office Platform Failures
Mitigation: Deliver Back Office Transformation

Risk 4: Loss of sensitive data
Mitigation: Mobilise Security Transformation Programme

Risk 5: IT Availability/ Ability to Trade
Mitigation: implement OCC and improve BCP/DR Plans

2. By mapping the 5 key risks onto our systems architecture, we were able to identify where the risks are from an architecture perspective (key risks 4 and 5 are more process driven):



How will we reduce our risks and when will we be within our risk appetite?

3. The identification of the operational risks confirmed that the delivery of the infrastructure change programme is essential to move us within our risk appetite. Specifically, we are:

   a. Moving applications to modern and supplier supported operating infrastructure that will facilitate the move of the business systems to Cloud

   b. Rolling out an integrated central and secure IT network core

   c. Deploying to branch a modern counter/desktop asset that is replacing HNGX, and will support operational continuity of service whilst enabling the counter for a new Thin Client Electronic Point of Sale (EPOS)

   d. Transitioning our reporting systems (Credence) to cloud, transforming supply chain, finance, and reporting systems as part of Back Office Transformation

4. To gain more understanding of our risk profile and appetite, we created an IT Risks Tube Map in the format of a timeline, which highlights the key activities/events required to mitigate to within our risk appetite over time (see Appendix 1). In addition, the IT Risks Tube Map also enables us to clarify our thinking on the nature and impact of risks, and to improve our risk assessment capability.

What the key activities required to mitigate our risks?

5. Whilst we remain outside of our risk appetite, we have several key mitigation activities in progress that will help reduce our exposure to risk:

Where we are now	Mitigation	Where we will be
• POLSAP Infrastructure is over 15 years old with many components currently out of or due to be out of support. • POLSAP operating systems (SAP) is out of support • Increase in failure rates/Incidents for aged Infrastructure • There are several Security vulnerabilities due to software age.	A review of failure rates and number of spares has been conducted. This is being re-visited regularly. Several minor fixes have been proposed by Fujitsu/Accenture/Post Office and are currently being priced in CRs. SAP has indicated that they will provide extended support, on the condition that PO share detailed plans showing our plans to exit.	POLSAP Services will be migrated by February 2018. Back Office Transformation intends to design POLSAP out – removing it entirely by June 2018 Enablement of appropriate MI/data and controls, providing stability and a robust Financial system.

Where we are now	Mitigation	Where we will be
Several systems across the estate have not had full testing of DR – particularly Fujitsu	Improve DR Plans. PO IT is carrying out a thorough review of DR across core suppliers. This will enable IT to be confident that we can recover service according to Recovery Time Objectives (RTO) We will perform an assessment of the DR status for "gold/Silver services (gold being the critical services). "bronze" services will be out of scope in the first part of the exercise We will enforce the exception process on any proposed deferments of testing, which will ensure there is full business sign off and visibility. The Operations Command Centre is in planning stage which will further support DR, along with improved event management, and reduction in lost trading hours.	In the next 6 months, we will have full visibility of planned tests, RTO, failed tests, and the actions to remediate. We will understand the potential level of investment required to increase Recovery Times, aligned to our business needs.

Where we are now	Mitigation	Where we will be
Several risks in IT Security: • vulnerability testing and the high number of tests that require urgent remediation. • a lack of preventative controls for data access from BYOD. • no centralised tracking of firewall incidents, resulting in an increased risk that potential incidents may not be reported on a timely basis leading to business disruptions and/ or data loss	Mobilise Security Transformation Programme. Work is underway to implement a Security Operations Centre (SOC) Focus is on improving the control of remote access into the O365 solution. The approach for adequate controls relates to BYOD, the controls will be in place by Sept 2017. The current solution for DLP controls are; encryption of data, size limits on email traffic, controls at zscaler (which need further enhancement once the service transitions to Verizon – September 2017).	In Q4, the first phase of the SOC will be live, providing efficiency, visibility, and control to facilitate continuous monitoring for detecting, preventing, and analysing security incidents. The SOC will enable the management of firewalls to be centralised, including tracking, resolving and reporting the incidents on a real-time basis.
Horizon data centre is running on legacy infrastructure and would not be able to support the move to Cloud	Redesign and migrate the horizon platform. The preparation of migrating the 39 business systems onto a new platform that will support a move to Cloud commenced in April 17. The live Application Migration will run between 23.07.17 - 31.10.17 Due to change freeze, the pivot to Cloud is expected to commence in January 2018,	In Q3 the Horizon Data centre 39 business system groups (applications) will have transitioned to a modern and supplier supported Operating infrastructure that will facilitate the move of the business systems to Cloud.

Where we are now	Mitigation	Where we will be
There is increased risk in our Branch technology environment: • The Horizon (HNGX) platform is end of life and is running on unsupported Windows software, therefore needs replacing • Branch counter technology is aged and unreliable, with frequent hardware failures, resulting in branch disruptions. • The branch IT network service (ISDN) provided by Vodafone will be switched off on 30th September 2017, and therefore needs transitioning	Accelerated plans to transition from HNGX to updated HNGA – provides an updated Windows version, but same architecture. Rollout underway. Upgrading the technology for 8,500 branch counters In parallel, developing "Thin Client" architecture which will be rolled out to the remaining branch counter estate. Replacement of 9000 receipt printers is being planned, with potential to co-deploy alongside branch counter refresh. Deploying a virtualized secure IT network for Branches which will be complete by end August 2017	Modernising and stabilising the Branch counter technology and associated operating system, deploying a new version of Horizon (HNGA), and simultaneous migration to the new secure Branch IT network.
HRSAP is running on legacy unstable infrastructure, the environment is managed by DXC on a contract that is due to be exited in March 2018	Services are being from HRSAP to Successfactors. The transition will begin 10th October 2017- Core HR, Payroll, Recruitment & On-boarding Employee & Manager self-service, followed by Agents pay February 2018	In the next 7 months the legacy service and suppliers will be decommissioned, and a more stable and secure environment will be stood up, enabling improved HR system functionality

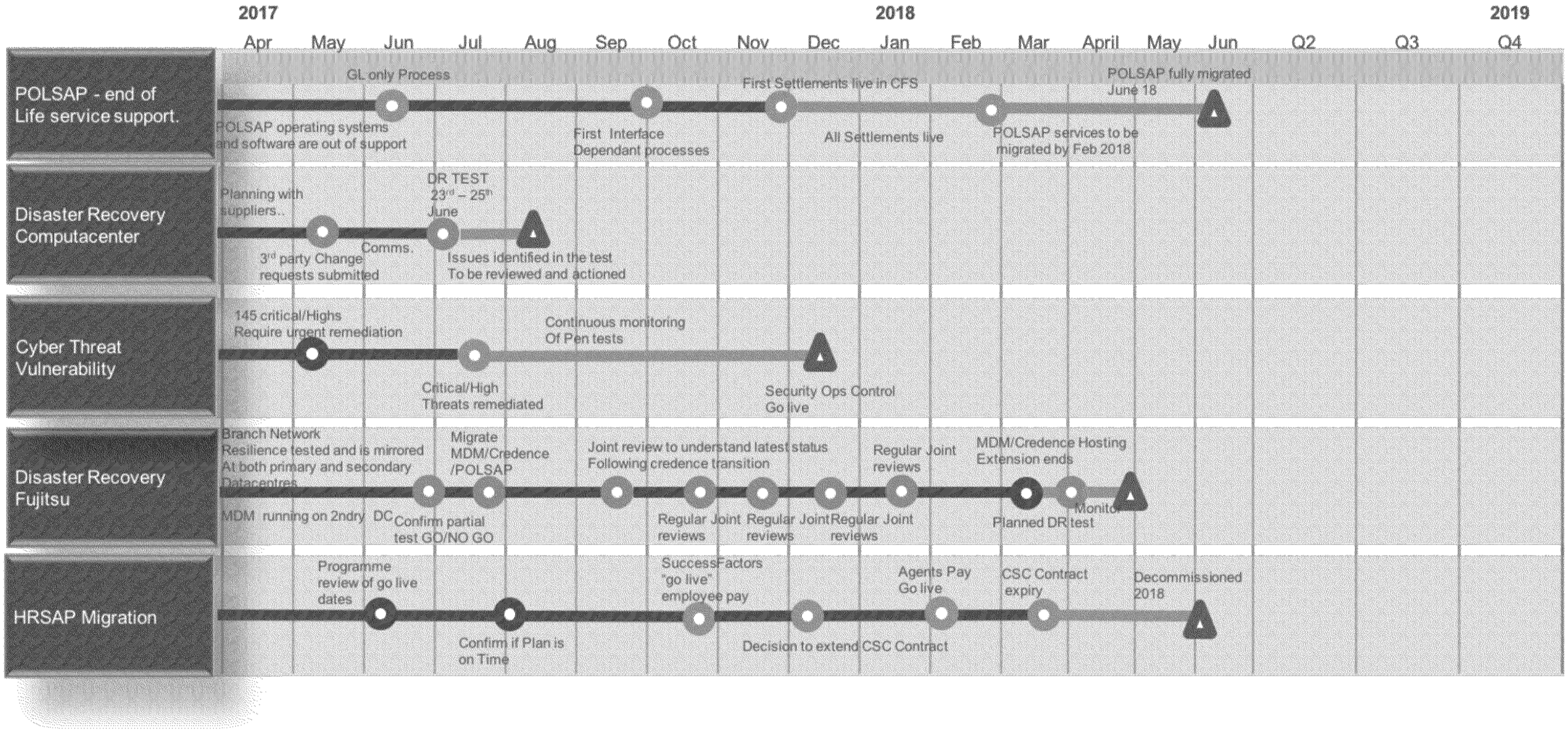
Where we are now	Mitigation	Where we will be
Historic high cost, fixed-service contracts, and a complex operating model, has prevented us from accelerating the changes required for improved security, agile delivery, and fit for purpose test environments. The effort required to improve our operating environment, and to have more control, involves renegotiations with key suppliers (Computacenter, Fujitsu, and Atos), which exposes us to the greatest operational risk (increased incident volumes, lost trading hours, poor service responses, negative behaviours, increased cost).	Computacenter renegotiations concluded in March 2017, changes in account team, closely monitoring performance, behaviours, and cost reduction targets. The Fujitsu renegotiation (project Everest) has commenced, with a Letter of Intent being drafted to enable migration to Cloud. This will also help accelerate movement to within risk appetite. The Atos renegotiation (project Amada) is nearing final stage with agreement reached on service migrations and cost, expected to conclude by end July 2017	In Q3 PO takes back control of business-critical services, with new accountabilities for IT security operations and real-time monitoring of critical applications through an Operational Command Centre (OCC) (reducing incident volumes and lost trading hours) Creating the ability to re-architect and accelerate the Horizon DC move to the Cloud

Next Steps

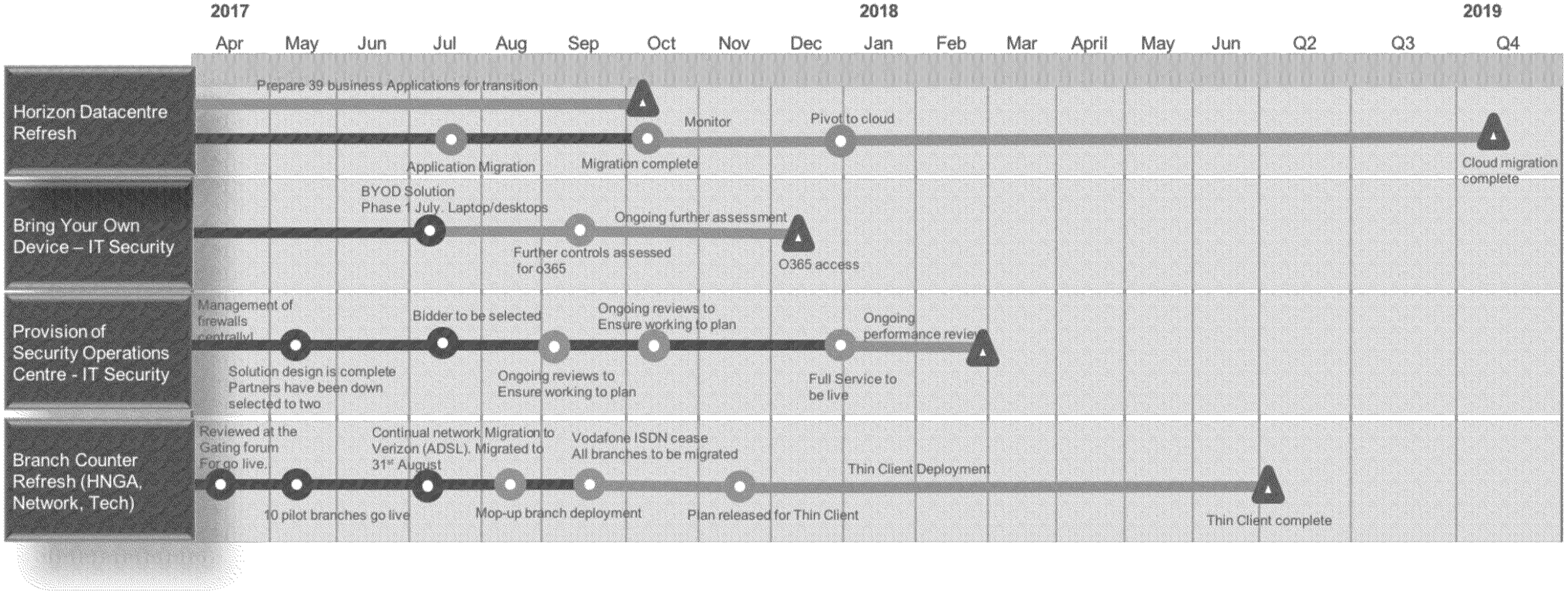
6. The DR framework will be developed, providing a current view of Recovery Time Objectives, agreed test plans and alignment to the critical services this will be provided at the next RCC in September.
7. By the end August, a risk awareness process and governance framework will be established to ensure system and process owners actively take responsibility for risk management and risk minimisation.
8. By end October, a risk evaluation model and risk repository in Sharepoint will be created to give better visibility of risk status.

Appendix 1 – IT Risk Tube Map

Red = High Risk / Amber = within appetite but attention required / Green = OK


2017
2018
2019
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
April
May
Jun
Q2
Q3
Q4
POLSAP - end of Life service support.
GL only Process
POLSAP operating systems and software are out of support
First Interface Dependant processes
First Settlements live in CFS
All Settlements live
POLSAP services to be migrated by Feb 2018
POLSAP fully migrated June 18
Disaster Recovery Computacenter
Planning with suppliers..
3rd party Change requests submitted
Comms.
DR TEST 23rd – 25th June
Issues identified in the test To be reviewed and actioned
Cyber Threat Vulnerability
145 critical/Highs Require urgent remediation
Critical/High Threats remediated
Continuous monitoring Of Pen tests
Security Ops Control Go live
Disaster Recovery Fujitsu
Branch Network Resilience tested and is mirrored At both primary and secondary Datacentres
MDM running on 2ndry DC
Confirm partial test GO/NO GO
Migrate MDM/Credence /POLSAP
Joint review to understand latest status Following credence transition
Regular Joint reviews
Regular Joint reviews
Regular Joint reviews
Regular Joint reviews
MDM/Credence Hosting Extension ends
Planned DR test
Monitor
HRSAP Migration
Programme review of go live dates
Confirm if Plan is on Time
SuccessFactors "go live" employee pay
Decision to extend CSC Contract
Agents Pay Go live
CSC Contract expiry
Decommissioned 2018

POL00401625


2017
2018
2019
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
April
May
Jun
Q2
Q3
Q4
Horizon Datacentre Refresh
Prepare 39 business Applications for transition
Monitor
Pivot to cloud
Application Migration
Migration complete
Cloud migration complete
Bring Your Own Device – IT Security
BYOD Solution
Phase 1 July. Laptop/desktops
Ongoing further assessment
Further controls assessed for o365
O365 access
Provision of Security Operations Centre - IT Security
Management of firewalls centrally!
Bidder to be selected
Ongoing reviews to Ensure working to plan
Ongoing performance review
Solution design is complete Partners have been down selected to two
Ongoing reviews to Ensure working to plan
Full Service to be live
Branch Counter Refresh (HNGA, Network, Tech)
Reviewed at the Gating forum For go live.
Continual network Migration to Verizon (ADSL). Migrated to 31st August
Vodafone ISDN cease All branches to be migrated
Thin Client Deployment
10 pilot branches go live
Mop-up branch deployment
Plan released for Thin Client
Thin Client complete

POST OFFICE
RISK AND COMPLIANCE COMMITTEE

ADVISORY PAPER

Financial Reporting Controls

Author: Danielle Goddard Sponsor: Amanda Radford, Al Cameron Date: 20 July 2017

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, any emerging issues or developments, and the next steps into the second phase of the project.

Questions addressed in this report

1. What is the current status of the FRC?
2. What are the latest self-assessment results?
3. What further control gaps have been identified and how are these being addressed?
4. What progress has been made on the next phase, and what are the next steps?

Conclusions

The existing framework has continued to expand (262 controls at end May 2017 from 241 at year end) as we have introduced new Masterdata and other controls. Monthly self-assessment is continuing in the TrAction online self-assessment tool and results are being monitored.

Of the 262 controls at end May 2017, 173 (66%) were issued for self-assessment. 161 (93% of those issued for self-assessment) were operating effectively. Of the remaining controls, 8 were not operating effectively and 4 were not self-assessed. 3 of the 8 controls marked as not operating effectively have since been confirmed as effective; the remainder relate to the change in the Fixed Assets control environment which is under review, and staff absence.

Of the 89 controls not issued for self-assessment at the end of May, 67 were not due to be operated in the period. 12 controls were still in remediation, and 10 were still being set to live. For the 12 controls in remediation, workaround controls are in place or remediation is in progress. The 10 controls being made live for self-assessment relate to the overall control environment and have been reviewed to ensure there were no unaddressed risks which could affect the financial statements.

PwC testing is now complete with the exception of Spreadsheet controls which are due to be tested this month. PwC's draft results show that of 80 controls tested, there were 12 amber exceptions and no red exceptions. The amber exceptions have now been addressed.

An incident was raised in May 2017 regarding a £0.5m unsupported debit balance in relation to the closed Merlin House cash centre. This was undetected due to insufficient POLSAP user access controls and manual journal controls allowing a user to manipulate the location and ageing of the balance, as well as a lack of rigour in certain areas of the Balance Sheet probity sign off.

We have identified gaps in training on Balance Sheet probity, and a medium risk control gap currently exists within the framework in relation to this. A new high risk gap will be raised in relation to POLSAP user access and manual journals.

The FRC team are working with the Back Office Transformation team to ensure that user access and manual journal risk is addressed through automated controls after BOT implementation. However a manual control has been implemented in the intervening period, where POLSAP journals over a defined materiality threshold are now subject to independent authorisation.

Further work is also being performed over the year-end Balance Sheet in response to this, with results to be concluded by end July 2017.

Further work has been performed on Masterdata, however progress has been delayed after the departure of our Masterdata specialist. Recruitment is underway to fill this gap and also for controls specialists who will manage the further areas which we have brought into scope.

Input Sought

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

The Report

1. What is the current status of the FRC?

1.1 The controls within the 12 processes included in the original scope of the FRC are being self-assessed by control owners on a monthly basis. Results are monitored by the FRC Manager on a monthly basis. The results of the most recent control self-assessment (May 2017) are summarised in section 2 below.

1.1. The number of controls is expanding, with controls increasing from 241 at end March 2017 to 262 at end May 2017. 10 new controls relate to new Masterdata controls embedded within the original 12 processes. The remaining 11 new controls relate to splitting out existing controls, where we believe it is relevant to recognise sub-controls or individual reconciliations as separate controls. The number of controls will continue to grow as we introduce new processes to the framework; these are discussed further within section 4.

1.2. PwC have completed their independent testing of controls, with the exception of Spreadsheet controls which will be tested in July 2017. PwC have provided a

POL00401625

draft consolidated report, showing that of the 80 controls tested there were 12 amber exceptions identified and no red exceptions identified. The amber exceptions mainly related to ownership issues and wording changes. These have since been resolved. An extract from the PwC draft results report is shown in Appendix 2. A full time FRC Manager is now in place and a permanent Controls Analyst is currently being recruited, who will perform monthly cycle testing over controls.

1.3. There were 12 open control gaps remaining at end of May 2017 (down from 18 at end March 2017) for which workaround controls are in place or remediation is being completed. None are considered high risk; 8 are considered medium risk and 4 low risk.

1.4. There were still 10 controls to be set to live at end of May 2017, all had owners but were awaiting final confirmation to go live. These all related to controls which sit under the overall control environment. None of these are expected to have a direct impact on the financial statements but work is being done to bring these live and into self-assessment.

1.5. This paper reports the FRC status at end May 2017. Since this date we have added an additional control gap in relation to POLSAP manual journals, which we consider to be high risk. Remediation has commenced in respect of this. Further detail is given in section 3 below.

2. What are the latest self-assessment results?

2.1. The results of the May 2017 self-assessment are summarised in the table below. See appendix 1 for further detail of the May self-assessment results by process.

May 2017 - Total controls	**262**	
Less: Controls in remediation	-12	
Controls to be set to live	-10	
Controls not due to be operated due to frequency	-67	
Total population for self-assessment	**173**	**66%**
Self-assessed and operated effectively	161	93%
Self-assessed but not operated effectively	8	5%
No self-assessment submitted	4	2%

2.2. 67 controls were not due to be self-assessed for May 2017, this is because the controls are annual, bi-annual or quarterly controls and did not fall due in the month.

2.3. 93% (161 controls) of the controls due for self-assessment operated effectively in the month.

2.4. 5% (8 controls) had not operated effectively; 3 of these related to Fixed Asset controls which are being transformed as a result of the recent Fixed Assets review. 2 relate to controls over GRIR and open WBS codes, these were not performed due to staff absence; however they were confirmed as performed effectively for year end, and for May a central review was performed of the GRIR balance. The remaining 3 controls have since been confirmed as operating effectively.

2.5. 2% (4 controls) had no self-assessment submitted. We have followed this up with line managers and repeat non-compliance will result in disciplinary action.

2.6. The June self-assessment is currently being performed and results will be assessed mid-July.

3. What further control gaps have been identified and how are these being addressed?

3.1. We had 10 high risk gaps in the initial assessment. At end May 2017, 7 of these were closed and 3 were reduced to medium risk. The remaining medium risk gaps were subject to additional procedures at year end, and currently have workaround controls in place or remediation work is being completed.

3.2. An incident was raised in May 2017 regarding a £0.5m unsupported debit balance in relation to the closed Merlin House cash centre. This was undetected due to insufficient user access controls and manual journal controls allowing a POLSAP user to manipulate the location and ageing of the balance, as well as a lack of rigour in certain areas of the Balance Sheet probity sign off. How the balance arose is currently unconfirmed, however further analysis is being performed over the relevant POLSAP transactions and further interviews will be held with the POLSAP user.

3.3. Under the original scope of the FRC, we identified a control gap in relation to lack of authorisation in respect of manual journals. An authorisation process was implemented covering our main Finance system CFS; this has now been effective for approximately 9 months. We are now extending the authorisation process to cover POLSAP, and also performing a review over HRSAP.

3.4. As part of the review performed over the Merlin incident, we have assessed access controls in POLSAP. It has been identified that various users require access to post manually into POLSAP in order to carry out transactions such as manual file uploads, transaction corrections, cash receipts and cash dispatches, treasury clearing account transactions, and client settlements. There are various controls in place to detect any errors or issues as a result of these postings, for example; probity returns over POLSAP balance sheet GL accounts > £5k, independent authorisation of high value transaction corrections, vendor reconciliations on client settlement vendors, and bank reconciliations.

3.5. The Merlin incident highlighted the need for remediation to be performed in the following areas; independent authorisation of manual journals in POLSAP, high risk user access in POLSAP, improvement in quality and rigour of balance sheet probity. The following remedial action has been taken to address each of these:

3.5.1. Independent authorisation of manual journals in POLSAP; an authorisation process has been developed, trialled, and rolled out effective from 5 July 2017. Individual teams have been engaged with and an official communication has been issued from the Financial Controller to POLSAP users. The authorisation process covers manual POLSAP entries which are > £250k in value, or > £30k for Transaction Corrections and Supply Chain / Cash Centre postings which we expect to be smaller. A review will be performed at the end of the month; this will include monitoring of the manual postings in the month (scanning for unusual items), checking a sample of manual entries back to evidence of approval to ensure compliance, and ensuring that there are no obvious instances of splitting journal values to circumvent the authorisation process.

3.5.2. High risk user access in POLSAP; options are being explored around the possibility of centralising processing of manual journals without affecting operations, or assigning automated posting restrictions by value and by GL specific to user profiles.

3.5.3. There is a focus on immediate control improvement to reduce risk, however the FRC team are working with the Back Office Transformation team to ensure that strong controls are in place going forwards after the migration of POLSAP processes into CFS.

3.5.4. Improvement in quality and rigour of balance sheet probity; a medium risk control gap remains open in respect of this. Completed remediation includes the introduction of independent authorisation of all probity returns, however further remediation is still required to drive quality and consistency of reconciliations and review. Training will be performed over the next quarter to address this.

3.6. In addition to the remedial actions listed above, a Balance Sheet review over Debtors and Creditors is currently underway. Deloitte have been engaged to assist with this. Work has been focused on testing the existence and accuracy of debtors and creditors at the year end by tracing through to post-year end cash receipt or payment. Where balances have not cleared after year-end we are focusing on reviewing the ageing, and reviewing the individual transactions to assess whether there is any risk of manual transactions masking the true ageing. We expect the results of this review to be concluded by end July 2017.

4. What progress has been made on the next phase, and what are the next steps?

4.1. We are currently re-assessing controls across Fixed Assets. The financial reporting risk has changed within fixed assets due to the potential change from full impairment to capitalise and depreciate and for this reason we are re-assessing risks and controls in this area.

4.2. We have reviewed ownership of controls as part of the new roles and responsibilities in the finance restructure; the changes as a result of the restructure have not had an impact on the performance of controls.

4.3. We have added Masterdata to the scope of the FCR; so far 3 processes have been covered and RACMs are under review and being finalised with control owners. 10 Masterdata controls were added into the framework and included in the May 2017 self-assessment. Within the 3 processes covered, 30 controls have been identified and 8 control gaps (excluding duplicate controls across the 2 processes). Most of the gaps are due to reliance on manual processes with a lack of monitoring controls. None of the gaps indicate a risk of material misstatement however are currently in the process of being prioritised as high, medium or low risk. We are currently recruiting a replacement Masterdata specialist; progress has been delayed until this is complete.

4.4. A site visit was performed at Atos in order to assess the control environment and identify any control gaps which require remediation. The results are being finalised and actions are being agreed with Atos. Some gaps have been identified regarding changes being made by Atos without prior approval from Post Office, we will implement workaround controls until these gaps are remediated.

4.5. As noted previously, in reviewing the programme we have identified a further four areas that we want to add to the FRC which were not considered high risk for the original scope: agents' debt; the branch correction process; agent remuneration; and POMs. A business case has been approved to cover this, as well as; the remaining Masterdata work to be performed, Finance Service Centre controls, and Cash Management and Forecasting controls. Recruitment is underway.

Appendix 1 – May CSA results by process

Controls	**Control Gaps**					**Control Owners**		**May CSA Results**				
Process	Total Controls	Control Gaps	H/M/L risk			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	29	0	2	0	0
Bill To Cash	18	2	0	1	1	18	0	11	0	5	0	0
Control Environment	21	1	0	1	0	21	0	1	0	9	0	10
Fixed Assets	19	3	0	0	3	19	0	10	0	3	3	0
Payroll	46	1	0	1	0	46	0	42	0	3	0	0
Procure To Pay	27	0	0	0	0	27	0	16	0	10	1	0
Project Accounting	11	0	0	0	0	11	0	3	2	4	2	0
Record To Report	40	3	0	3	0	40	0	25	0	10	2	0
Settlement Process	14	0	0	0	0	14	0	9	2	3	0	0
Stock	7	2	0	2	0	7	0	3	0	2	0	0
Tax	18	0	0	0	0	18	0	4	0	14	0	0
Treasury	10	0	0	0	0	10	0	8	0	2	0	0
	262	**12**	**0**	**8**	**4**	**262**	**0**	**161**	**4**	**67**	**8**	**10**

Appendix 2 – PwC independent assurance results (draft)

Figure 1 - Internal Audit's assessment of performance against management's own self-assessment.

We have sample tested 43% of the total manual controls in the risk and control matrices (RACM) of in-scope processes. The table shows Internal Audit's assessment of the sample of controls compared to management's CSA for the same sample.

Finding rating	Assessment rationale
Red	Control is not operating effectively.
Amber	Control is not designed effectively, but remediation plan is in place or the control operated partially.
Green	Control is designed and operating effectively

In scope processes	Internal Audit Testing Results					POL Management CSA results					Total Manual Controls in RACM	% tested
	In Remediation	Red	Amber	Green	Total	In Remediation	Red	Amber	Green	Total		
No issues noted	-	-	-	56	**56**	-	-	-	59	**59**		
Design effectiveness	12	-	12	-	**24**	21	-	-	-	**21**		
Operating effectiveness	-	-	-	-	-	-	-	-	-	-		
Total	**12**	-	**12**	**56**	**80**	**21**	-	-	**59**	**80**	**187**	**43%**

At the time of our testing we found that nine controls (5.4.a.1-fixed asset, C9.2.j-payroll, C9.2.g-payroll, C9.2.r.2-payroll, C9.4.c-payroll, D1.9.b.1–record to report, D1.10.b.1–record to report, D1.11.e.1–record to report, D1.12.d.1–record to report) "in remediation" had been implemented without an exception. From the walkthrough performed of controls in remediation, we believed the risks are appropriately addressed by the remediation plan in place.

We did identify controls which required updating or further clarity. These have been listed in the Appendix.

Health and Safety

Authors: Martin Hopcroft Sponsor: Al Cameron Meeting date: 20th July 2017

Executive Summary

Context

1.1 The Risk & Compliance Committee requested a regular update on our management of risks around the health and safety of our people and customers.

1.2 Health and Safety performance is reported monthly to the Group executive and at each Board meeting, together with information on health and wellbeing.

1.3 Accountability for safety is with Operations, recognising that the greatest risks are to our people in the field.

1.4 Our Health & Safety performance has improved significantly in the past 6 years and we have a rolling 3-year plan to drive health and safety compliance and year on year risk reduction, targeting a reduction in four key safety metrics: accidents; lost time accidents; days lost; and personal injury claims.

Questions this paper addresses:

2.1 What is going well across health and safety and what is not going so well?

2.2 What are we doing to mitigate the key risks, including driving and robberies?

2.3 Are there any significant emerging risks?

Conclusion:

1. Accident Performance, including absence accidents and lost days, increased over Q1, however, volumes returned to normal in June (see Report-H&S Metrics). A recent increase in the number of accidents reported in May has been investigated and remedial action taken with ongoing monitoring and support provided. **Benchmark data** has been requested from suppliers for ARC in September.
2. Mitigating action has reduced **road risk** which remains at a low level. The Road Risk Policy is being reviewed and an overarching policy will be developed for all business drivers (including those using personal cars)
3. There was one CViT attack in May, and Post Office robberies remain higher with a review being undertaken by the Security team.
4. Property H&S **training workshops** have been delivered to Persons in Control of Directly Managed branches and coaching provided to Supply Chain Managers.
5. We have undertaken an annual deep dive review of safety and agreed a number of areas for focus in 2017/18 including a review of road policy, guidance for lone workers, safety of vacated buildings, competency and statutory compliance.
6. A number of initiatives have been implemented to raise awareness of mental health resources. From August we aim to train and introduce up to 60 Mental Health First Aiders to provide proactive support to colleagues across the business.

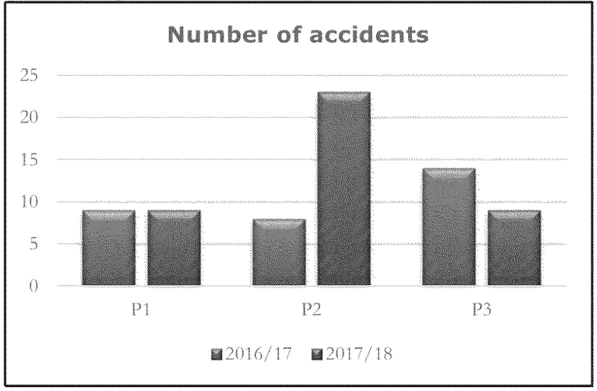
Input Sought

The Risk & Compliance Committee are requested to **note** the update on safety.

The Report – H&S Metrics

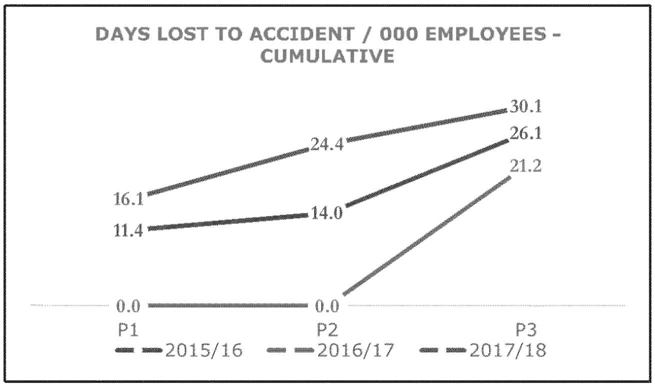
Summary of Safety Performance - YTD Period 3 (June 2017)

All Accidents – Monthly - Period 3
(Target to achieve a 5% year on year reduction)



Accidents have increased by 32% YTD P3 (June) when compared to previous year. There have been 41 accidents compared to 31 in 2016/17.
Lifting and handling related accidents remain at a low level. However stepping and striking accidents have increased in the Supply Chain, esp. the Stock Centre, with colleagues bumping into inanimate objects due to a lack of attention. Investigations and follow up briefings have been provided to raise awareness at the Stock Centre. There were also a few vehicle door related injuries, due to faults or a lack of awareness.

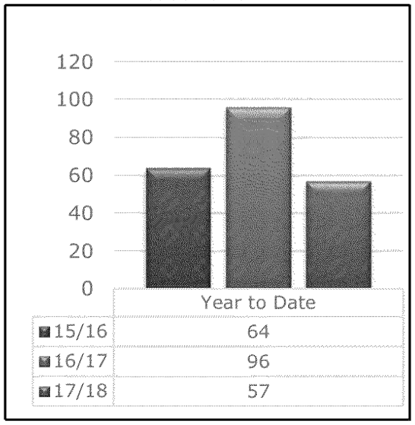
There have been **7 lost time accidents** in 2017/18 and 152 total lost days which is an increase of 9% compared to 2016/17. **Trauma** related lost days, following an attack, are down 50% on 2016/17.



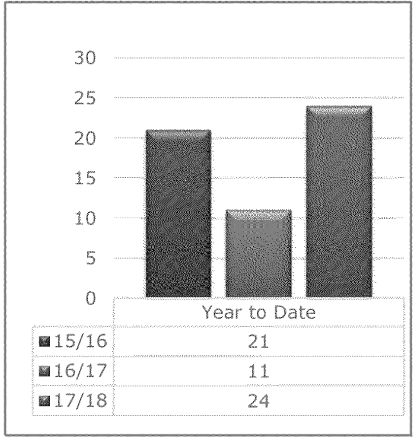
Post Office lost days: 28 in Period 3
DMB lost days P3 YTD : 57 (96 in 16/17) – 1 slip/trip & 1 lifting injury
Supply Chain lost days P3 YTD: 89 (43 in 16/17) 1 RTA, 2 slips & trips
Support lost days P3 YTD : 6 (6 in 16/17)
Trauma days lost: Supply Chain P3 YTD: 11 (21 in 16/17)

Post Office CViT Robberies – P2 (May 17)
Following a low volume of incidents reported in Q4 of 2016/17, there were 5 incidents reported in P1 and 1 incident in P2, which was violent and led to injury. Trend is being monitored closely, esp. the Birmingham area.

Directly Managed Branch
Accidents P3 YTD



Supply Chain Accidents P3 YTD

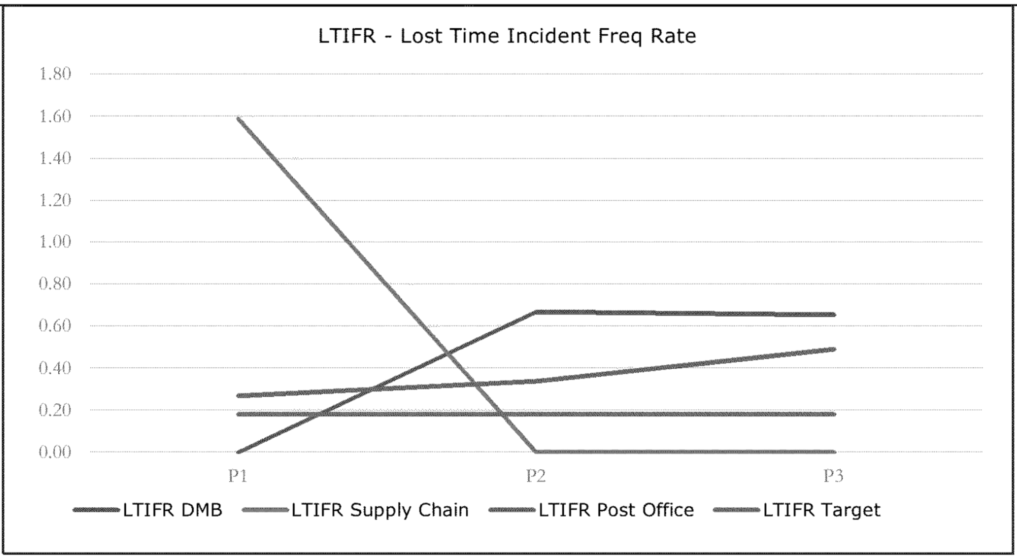


Post Office (All branch types) Robberies – P2 (May 17)
There were:

14 incidents in March v 9 (15/16)
(152 incidents in 2016/17 v 104 in 2015/16)
13 incidents in April v 3 (16/17)
15 incidents in May v 7 (16/17)

A review of causation and mitigating activity is being undertaken by the Security Team and a paper being prepared for GE.

2017/18
Violence – 2 vs 1 last year
Injuries – 1 vs 0 last year
Weapons - 13 (3 firearm) vs 5 last year (2 firearms)



Lost Time Injury Frequency Rate (LTIFR) – Period 3 YTD

Supply Chain

YTD P3 – 0.592
2016/17 out turn – 0.586
2017/18 target – 0.500

All Post Office – Employee

YTD P3 – 0.357
2016/17 out turn – 0.168
2017/18 target – 0.180

Road Risk

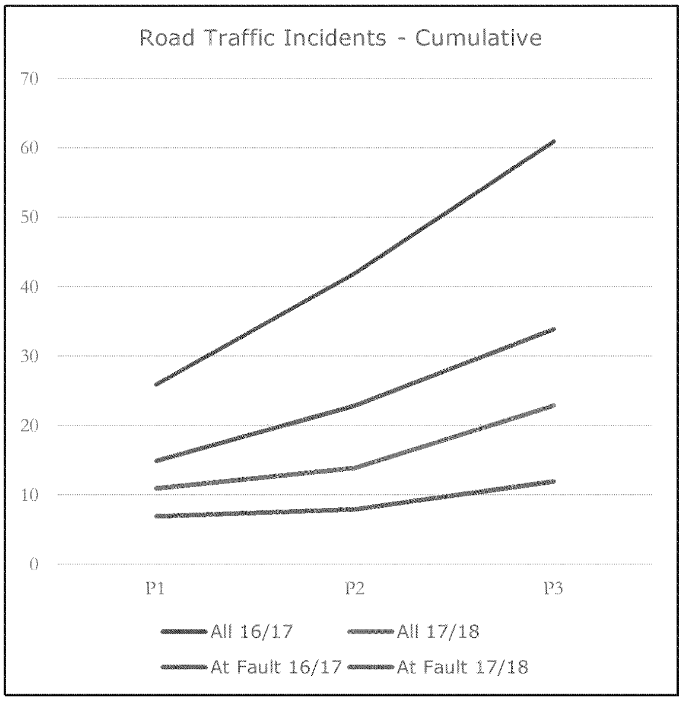
YTD RTC's

- 23 RTC's – YTD.
- 7 at fault, 6 not at fault
- 11 minor RTC's, 2 major.
- Some additional analysis is being done regarding fleet size, staff hours and headcount for future reporting.

Comparing 2016 v 2017

- There were 61 RTCs YTD in 2016/17 v 23 this year (17/18), a 62% reduction YTD.
- At fault RTC's were 34 in 2016/17 and have reduced to 12 in 2017/18, a 64% YTD improvement

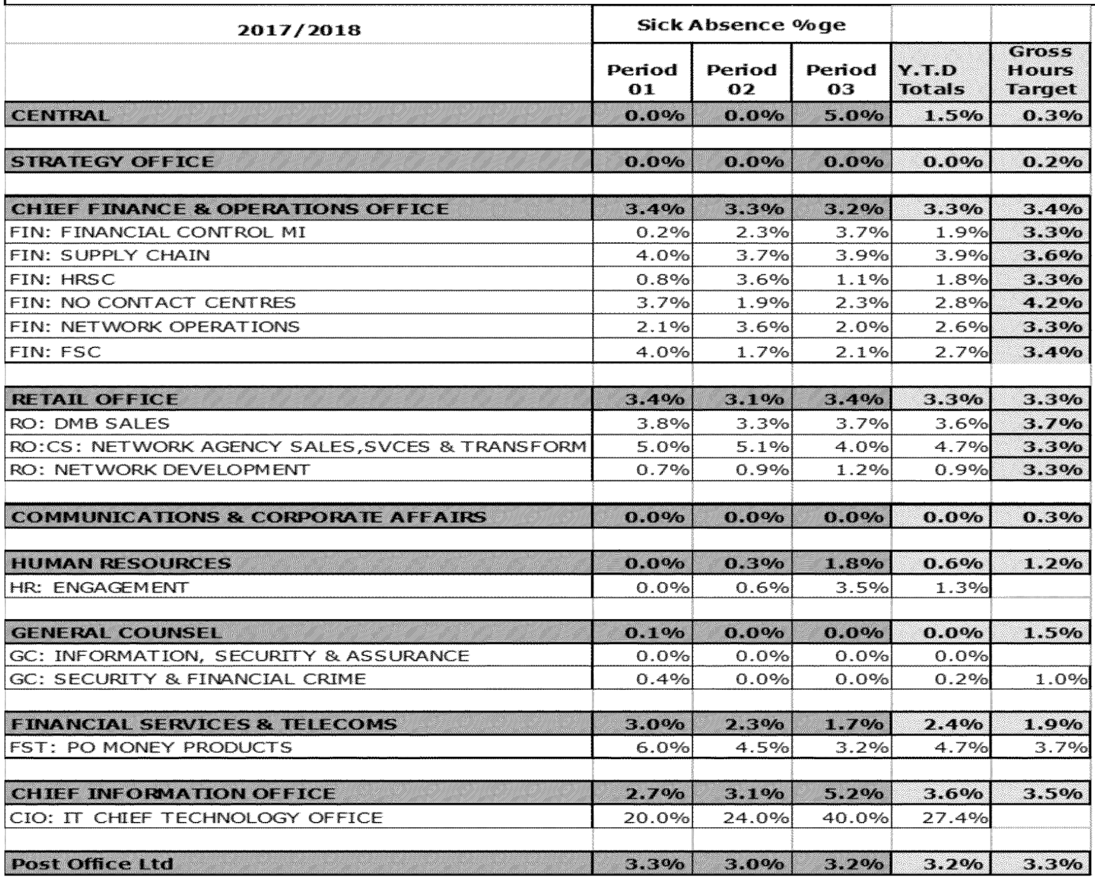
New providers have been confirmed for maintenance and accident management for Commercial fleet and for provision, maintenance and accident management of Business Car fleet. Enhanced MI and accident analysis can be expected later in 2017/18.
An overarching Road Risk Policy, with improved training and compliance checks is being developed by the Fleet Management team to cover Commercial, Business Cars and Personal Car use.



Summary of Wellbeing Performance - YTD Period 3 (June 2017/18)

- The overall attendance level remains stable at 96.8% YTD P3 (June 2017/18). Short Term absence is 0.9% YTD and long term absence is 2.2% YTD. Supply Chain LTS is reducing to 2.3% and DMB LTS increasing to 2.7%
- Mental health related absence remains the most common cause of long term absence and there is an increase in lost days in Directly Managed Branches. Some additional analysis is being undertaken by our Occupational Health and HR Service Providers to understand trends and areas of concern to target intervention.
- Proactive activity across the business, includes 'positive mental health awareness' sessions for colleagues, additional awareness training being piloted for line managers and the introduction of Mental Health First Aid initiatives. The recruitment approach for MHFA is being developed with the HR Business Partners and OH Assist ™ and training courses planned for August and September.

Business Area Absence Performance v Target – P3 YTD 2017/18



2017/2018	Sick Absence %ge				
	Period 01	Period 02	Period 03	Y.T.D Totals	Gross Hours Target
CENTRAL	**0.0%**	**0.0%**	**5.0%**	**1.5%**	**0.3%**
STRATEGY OFFICE	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.2%**
CHIEF FINANCE & OPERATIONS OFFICE	**3.4%**	**3.3%**	**3.2%**	**3.3%**	**3.4%**
FIN: FINANCIAL CONTROL MI	0.2%	2.3%	3.7%	1.9%	**3.3%**
FIN: SUPPLY CHAIN	4.0%	3.7%	3.9%	3.9%	**3.6%**
FIN: HRSC	0.8%	3.6%	1.1%	1.8%	**3.3%**
FIN: NO CONTACT CENTRES	3.7%	1.9%	2.3%	2.8%	**4.2%**
FIN: NETWORK OPERATIONS	2.1%	3.6%	2.0%	2.6%	**3.3%**
FIN: FSC	4.0%	1.7%	2.1%	2.7%	**3.4%**
RETAIL OFFICE	**3.4%**	**3.1%**	**3.4%**	**3.3%**	**3.3%**
RO: DMB SALES	3.8%	3.3%	3.7%	3.6%	**3.7%**
RO:CS: NETWORK AGENCY SALES,SVCES & TRANSFORM	5.0%	5.1%	4.0%	4.7%	**3.3%**
RO: NETWORK DEVELOPMENT	0.7%	0.9%	1.2%	0.9%	**3.3%**
COMMUNICATIONS & CORPORATE AFFAIRS	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.3%**
HUMAN RESOURCES	**0.0%**	**0.3%**	**1.8%**	**0.6%**	**1.2%**
HR: ENGAGEMENT	0.0%	0.6%	3.5%	1.3%	
GENERAL COUNSEL	**0.1%**	**0.0%**	**0.0%**	**0.0%**	**1.5%**
GC: INFORMATION, SECURITY & ASSURANCE	0.0%	0.0%	0.0%	0.0%	
GC: SECURITY & FINANCIAL CRIME	0.4%	0.0%	0.0%	0.2%	1.0%
FINANCIAL SERVICES & TELECOMS	**3.0%**	**2.3%**	**1.7%**	**2.4%**	**1.9%**
FST: PO MONEY PRODUCTS	6.0%	4.5%	3.2%	4.7%	3.7%
CHIEF INFORMATION OFFICE	**2.7%**	**3.1%**	**5.2%**	**3.6%**	**3.5%**
CIO: IT CHIEF TECHNOLOGY OFFICE	20.0%	24.0%	40.0%	27.4%	
Post Office Ltd	**3.3%**	**3.0%**	**3.2%**	**3.2%**	**3.3%**

The Report

2.1 What is going well across health and safety and what are the current activities?
2.2 What are we doing to mitigate the key risks, including driving and robberies?

SAFETY

Performance remains strong across many key health & safety metrics, including road risk and CiT related robberies (see Report–H&S Metrics). The number of accidents reduced in June following the spike in May. Current activities include:

1. **Person in Control (PiC) Training -** Refresher PiC training and Property H&S workshops have been delivered to all Supply Chain and DMB Managers. This is being extended to all Support Centres and satellite offices. A Team Talk session is also being developed for all colleagues in DMBs to ensure minimum awareness and support for H&S and will be issued in July.
2. **Property related risk (As reported in the Property Compliance Report)**
   - The overall level of risk remains low with property compliance 95.5%.
   - Current activities include 'Fabric inspections', shipment of the site log books and the re commencing of site audits. Vacant property inspections are currently being reviewed on a monthly basis.
3. **Health & Safety Activity Calendars -** To ensure Health & Safety activities are undertaken, H&S calendars have been updated and launched for 2017/18. H&S BPs are attending Lead Team meetings to help raise awareness and compliance and this is being extended across all areas of the business during July - September.
4. **Road Risk -** The volume of road traffic incidents continues to reduce. The Fleet Management Team and H&S Team are creating an overall driver policy to provide additional guidance and training to all commercial and business drivers including those using own vehicles.
5. **Security / Robbery Risk -** A report is being developed by Security Manager to support a GE discussion, due to the recent increase in Post Office robberies. CViT related incidents have remained relatively low.
6. **Hosted Directly Managed branches -** Post Office and WHSmith H&S Managers and Property Compliance Managers are working closely to share processes and documentation. Guidance for Post Office Managers has been issued by H&S BPs.
7. **Environment -** The Environmental Tactical Group is currently reviewing policy and plans and checking energy, recycling and carbon data for year-end reporting with the Facilities Management suppliers, CBRE and Servest.
   Guidance has been provided to 'Persons in Control' for the management of waste and to raise awareness of the risk of receiving fixed penalties/enforcement notices.

WELLBEING

1. The Health & Safety team are raising awareness of resources that are available to colleagues at Support Centre, Supply Chain & Directly Managed team meetings.
2. Mental Health awareness 'Time to Talk' sessions are being rolled out to all areas of the business, including use of the Team Talk session to encourage the conversation at Directly Managed Branches and Supply Chain sites.

3. The Occupational Health provider has provided guidance for 'Mental Health First Aid' training for volunteers across the business (approx 60) and selection criteria which has been considered by the HR Directors and BPs in June. The preferred approach has been agreed to invite applications, endorsed by line managers and HR BPs to undertake short video interviews. Training is being scheduled for Aug / Sept.
4. A new MH Awareness training product is being piloted for line managers in July.
5. Health Checks will continue to be offered to all employees (either Kiosk or Mobile)
6. The range of available OH services has been extended and current activity includes:
    - Launch of the Post Office Wellbeing Portal in July, enabling access (externally and internally) to all services and resources through one landing page.
    - Extension of the absence 'case management' pilot, OH Assist™ Advice Plus.
    - Training provided to Support Centre call advisers and team leaders for 'difficult' and traumatic calls to be extended to Contract & Security Managers.

What additional activity has been undertaken to address specific risks?

1. **Compliance to Driving and Mobile Phone Policy**
   A policy check has been incorporated into the local risk assessment undertaken by all line managers who have staff who drive for work. This will be incorporated into a new online training module that has been developed and will be issued in August via Success Factors.
2. **Environmental Policy**
   The Property Compliance and H&S teams are working closely with Legal, Servest and IT to minimise risk associated with waste, especially hazardous. Guidance has been issued to Persons in Control to minimise the risk of waste reaching landfill sites.
3. **Security and lone working in Support Centres**
   H&S, Property and Security Managers are reviewing personal security arrangements in place at all Support Centres and satellite offices. A report will be discussed at the GE Safety Board in July, following the current review of Security at Finsbury Dials.
4. **Hosted DMBs**
   The CND, H&S, Legal and Property teams are working closely with WHSmith's lead team to address recent concerns raised regarding ineffective air conditioning in stores during the hot weather. A temporary process has been agreed.
5. **Trauma Support and Self Harm / Suicide Policy**
   Additional training has been provided to call handlers in Chesterfield and the HR Service Centre to help them manage 'difficult calls', including threats of suicide. Similar appropriate training will be extended to their team leaders, contract advisers and field advisers who may also benefit. This is being planned for July – September.
6. **Fire Training and Evacuation Plans – Finsbury Dials**
   Additional Fire Wardens and First Aiders have been identified for Finsbury Dials and are receiving training as a priority. Additional Persons in Control are also being trained. Communications have been issued to remind all staff of the evacuation plan. Online Fire Training is being issued July via Success Factors to all employees.

2.3 Are there any significant emerging risks for 2017?

1. **Change Programmes**
   - H&S BPs are monitoring absence, accident trends and causation and working closely with lead teams, providing training and improving the focus on safety, attendance management and wellbeing, prioritising across the business.
   - Induction programme including H&S content has been reviewed and updated to ensure line managers of new employees complete the checklist.
   - Support and training has been provided to upskill Supply Chain Shift Managers, ensuring records brought up to date to meet OHSAS 18001 audit requirements.

   Property / IT – Disposal of hazardous waste - Previous concerns on how we dispose of IT hazardous waste, in particular Horizon printer cartridges are being addressed by IT. **Property –** General poor condition of the fabric around the estate continues to be a concern and is being addressed via site surveys. **Current Objectives** include: Closure of outstanding remedial actions from previous '5 Year Electrical Inspections', further fabric inspections and site audits to review risk of vacant buildings. Our CRC submission will be completed for 16/17 by CBRE in July.

2. **An annual Health & Safety 'deep dive review'** has been undertaken by the GE H&S Sub Committee (Safety Board).

   Areas carrying a higher risk of fatality or serious injury were reviewed including:

   a. Property (Fire, Electrical, Fabric and Asbestos, Legionella, behaviour)
   b. Security (ATMs, Agents robberies, Supply Chain attacks)
   c. Road Risk for Commercial and Business Drivers (maintenance, fatigue and distraction, alcohol and drugs, mobile phone use, working hours and travel policy, lone working).

   A review of H&S in Supply Chain, Directly Managed branches and Support teams also took place. GE Committee members and senior leaders for each function discussed and reviewed the risks and considered the current controls, agreeing areas for prioritisation and attention during 2017/18. These include:

   a) Implementation of a single road risk policy for all business drivers and to monitor its application, including document checks and risk assessments
   b) Identifying and then providing guidance and training to all lone workers
   c) Improving safety of our vacated buildings, to include surveys of external fabric
   d) Review and reissue personal security guidance for agents and consider best ways to share guidance for H&S and Business Continuity related matters.
   e) Improve H&S competency of new line managers and PiCs across the business
   f) Monitor compliance to H&S Activity Calendars and procedures and provide reports to GE, Safety Board and Senior Leaders to enable them to support and satisfy their business areas are compliant.
   g) Consider an external audit of H&S governance, procedures and compliance during the second half of the year.
   h) Urgently increase the number of Fire Wardens and First Aiders at Finsbury Dials and review provision at all largely populated sites.
   i) Summarise and review the business crisis plan updates and evacuation plans.
   j) Review Stay Calm manuals, update contents, simplify instruction and guidance and develop a consistent process that is fit for purpose.

An action plan has been developed and an update will be provided to GE in August

3.8) Business Continuity & Crisis Management update

Author: Tim Armit Sponsor: Jane MacLeod Meeting date: 20th July 2017

Executive Summary

Context

Post Office continues to develop its Business Continuity Plans and framework for Incident Management in order to appropriately protect the business and its reputation, and give confidence to stakeholders. Since the last report in May, there have been number of significant external national incidents - a number of which have touched our business in differing ways, and which are being reviewed to ensure that Post Office benefits from the learnings.

Questions this paper addresses

- How effective was Post Offices response to significant external incidents?
- What are the next steps to improve levels of continuity and resilience nationally?

Input Sought

The Committee is requested to note the report.

Conclusion

How effective was Post Office's response to significant external incidents?

Manchester bomb, London stabbing, London fire, NHS cyber attack, and BA IT systems failutre

1. Each incident touched Post Office in different ways (operational impacts from branches and supply chain depots being within security cordons, requirement to support cash distribution for those affected by Grenfell Tower fire etc). Overall Post Office responded well to each incident. Nevertheless, there are a number of learnings from these incidents which are now being assessed. These include ways of responding to different forms of crisis, content and timing for staff and wider branch and operational communications, engagement with other stakeholders and players (security services, COBRA etc), and protocols to provide reassurance and support to staff and customers.
2. Existing processes including the Stay Calm manual and the use of the Business Protection Team are all being revisited and will be simplified, re-issued and training provided.
3. A review of the security levels in key Post Office sites has commenced.
4. Our approach to communications to branches and all operational areas is under review.
5. To enhance resilience nationally other key programmes are being implemented:
    a. A recovery solution for Bolton is being reviewed to bring it to the level of Chesterfield.
    b. Supply Chain offices across the UK are undergoing facilitated training sessions.
    c. An online Business Continuity training and questionnaire session for all staff has been constructed and will be made available to every employee in July.

Chesterfield Relocation Exercise

6. 'Proof of concept' testing of the viability of the Sungard Work Area Recovery site for Chesterfield has now been undertaken. Two teams from Chesterfield representing Financial Operations and the Call Centre were both relocated to the Sungard Work Area Recovery site. The teams established a working environment and worked on business as usual functions for the period of the exercise. The exercise was a success but had been pre-planned, so further testing will be required to ensure it operates effectively in a live 'stress' event. The lessons learnt in the preparation and the weaknesses seen during the test will now be worked through with IT to ensure an improved capability is put in place which can be re-tested. Confidence can be taken that this proposed solution does work if required.

Royal Mail Industrial Action planning

7. A workshop of all areas touched by Royal Mail has been completed and a report published detailing potential areas of risk. These will now be worked through with the relevant teams to develop contingency strategies for these risks.

Current areas of concern and next quarter activities

8. Set out in the Appendix is the most recent assessment of Post Office's BCP framework. Key activities through to September 2017 are:
   - Further training and education for the Business Protection Team including improvement of the procedure to invoke the Business Protection Team
   - The IT DR capabilities and subsequent impact on the business need defining and plans considered
   - The Industrial Action plans needs to be reviewed in light of current risks
   - Development and implementation of a recovery strategy for Bolton
   - Home working as a mitigator for a potential failure of Finsbury Dials needs to be tested and proved
   - Stay Calm manual needs to be simplified and training provided as to its use
   - Resilience levels across all key locations and facilities needs to be tested, improvements identified and implemented.

Appendix

Business Continuity

Current status and the roadmap to "good"

July 2017

Overview

This document describes what is seen as best practice within business continuity by the Business Continuity Institute and ISO standards. It then considers how the Post Office currently measures up to this level, how we will move any areas which might be red or amber towards green, which would be "good". Finally it shows how the Post Office will demonstrate in an ongoing manner that "good" is in place and being maintained.

From this document many work packages will be developed across the company.

Summary

As a current holistic overview, with the exceptions listed below, should a major incident befall Post Office operations we will be able to continue to open branches and serve customers in a timely manner.

Exceptions to this where further investigation is required to improve resilience or determine the capability are:

- Key IT systems
- Suppliers
- Bolton

The summary table over leaf presents where Post Office currently stands with regards to its implementation and testing of its recovery capability. The tables after this show the detail to support this table. Going forward this table will be updated to demonstrate progress.

SUMMARY TABLE OF - What does "good" business continuity management look like?	
A management system in place aligned to ISO22301	■
Management system operational and signed off	■
Impacts of the loss of buildings, systems, suppliers and people are understood	▒
Risks in which the operations work are understood, mitigated or planned for	▒
Recovery strategies for locations and business processes are in place	
• Finsbury Dials	■
• Chesterfield	■
• Bolton	■
• Supply Chain – Cash Centres and Swindon.	▒
• Branches	▒
Plans to respond to crisis are in place	▒
Plans to recover business operations are in place	▒
Plans to mitigate the loss of key suppliers are in place	▒
Tests of plans have been undertaken	
• Some IT DR testing has been undertaken where possible.	▒ ■
• Initial high level crisis exercises have been run.	■
• Initial Chesterfield to Sungard exercise has been run.	■
• Communication test to GE crisis team and the BPT completed.	■
• Annual Test Programme to be in place	▒
• BPT team is in place but not trained or exercised in their roles	▒
Training of personnel involved has been completed	▒

Detailed breakdown of business continuity progress

What does "good" business continuity management look like?	RAG	Where are we	What do we have to do to get to green	How do we demonstrate "good"
A management system in place aligned to ISO22301	■			Full system in place and used in tenders to prove our capability
Management system operational and signed off	■			Signed off and used in our approach to BCM and tenders
Impacts of the loss of buildings, systems, suppliers and people are understood	▒	Work has started on this and there is varying levels of information across locations, business areas and IT.	Formally document impacts across agreed variables (cash flow, income, reputation etc) for each business area, location and system. Agree impacts with the owners and use this as a base for all recovery strategies.	Strategies in place ensure impact tolerance thresholds are not breached.

POL00401625

What does "good" business continuity management look like?	RAG	Where are we	What do we have to do to get to green	How do we demonstrate "good"
Risks in which the operations work are understood, mitigated or planned for	▨	Work has been completed by CBRE on facilities risks across all offices. Further operational and continuity risks are being captured in ongoing work. Risks to systems are being captured by IT.	Formally document the risks to each location in which we operate. Identify all key risks to the resilience levels of our systems. Document all outcomes and agree with business and location owners what the risks are and discuss if increased resilience is required or if better recovery planning is needed.	Risks are known and signed off. There are "no surprises" to senior management should a risk be realised, that risk will be in line with our plans and has been considered. Levels of resilience are increased where the risk and cost of solution mitigate it.
Recovery strategies for locations and business processes are in place				

What does "good" business continuity management look like?	RAG	Where are we	What do we have to do to get to green	How do we demonstrate "good"
	▨	Finsbury Dials is a low criticality building and all staff have the capability to work at home.	Test this by having everyone work at home for a day across the summer.	Everyone can work at home on their own devices.
	▨	Chesterfield is a key building and a tested recovery solution with Sungard is in place.	Test this in late June by working from Sungard for a full operational day. Agree recovery strategy and implement the solution by September.	A call centre and finance function can operate to acceptable business levels at the remote site. The Chesterfield solution has been tested and proven to work. Methods to make this easier and better were identified and are being reviewed.
	▨	Bolton is a secondary level critical building and whilst there is a home working capability there is no proven alternate work solution in place.	Work with the Bolton team to agree a strategy to recover operations	A Bolton HR operation can be operational to meet business requirements in an alternate manner. Costs to implement this have been sourced and a meeting on July 20th will agree if the proposed solution is to be implemented.

What does "good" business continuity management look like?	RAG	Where are we	What do we have to do to get to green	How do we demonstrate "good"
	▨	Cash Centres at London, Hemel and Birmingham can mutually support each other. Supply Chain depots can mutually support each other. Swindon is a single point of failure but strategies to restore key operational areas have been considered.	Test the capability to stand up alternative Bureau machines. Review with the Supply Chain locations at a workshop in May how this would operate. Continue to work with Swindon team on options at other depots and to agree what is critical and how to liaise with RM	London and Birmingham are proven to work in a stand alone manner for a day. Hemel services are proven to be recovered at another site. Methods to switch routes, agreement to move drivers and evidence that sites can support each other is proven through testing. An alternate capability is recovered at a depot to demonstrate systems can pick items, secure items can be managed and service can be restored.
	▨	Branches are mitigated by the proximity of other branches. Key operations in branches are also covered in others Stay Calm manuals are within DMB's.	Ensure every branch has a simple set of procedures to consider in planning for their own response to a large scale incident.	During any incident a branch knows how to respond. Key DMB's will be assessed by Business Continuity audit annually on their awareness in conjunction with Health and Safety.

What does "good" business continuity management look like?	RAG	Where are we	What do we have to do to get to green	How do we demonstrate "good"
Plans to respond to crisis are in place	▨	Stay Calm manuals are in place for all locations. These are very large and hard to use documents but they are well known and used by many areas. Finsbury Dials has a high level crisis team in place. There is a Business Protection team in place to respond to all major incidents.	Review and simplify these documents to ensure they are user friendly and known by all that need them. Document the crisis plan for Finsbury Dials and how this would support a crisis anywhere in the Post Office Enhance the BPT membership, its empowerment, ensure all members understand this role, test this and link it to all forms of crisis.	Exercises run in all locations to prove the team understand their roles and the documents work for them. Exercise run to prove the team understand the plan and their roles. Exercises to be run to prove the membership can work together on a crisis response. There are many live invocations of this team which we learn from each time.

What does "good" business continuity management look like?	RAG	Where are we	What do we have to do to get to green	How do we demonstrate "good"
Plans to recover business operations are in place	▨	There are some specific service to customer plans in place. There are a few strategies to allow operations to continue should IT systems fail (Polsap, Credence). There are very few specific business continuity plans in place for business areas.	Ensure these plans are still valid and upto date and simplify the approach (currently many are over 40 pages long). Group the strategies in place into plans for specific business areas and share what is known to work with other areas with similar challenges. Document a simple plan for every business unit.	Annual review and annual challenge by customers pass each year. Reaction and response to IT system failure is known and works efficiently each time they are needed within minimal impact on business. All areas work through table top tests and all staff are aware of a plan in place and how it affects them. As a standard KPI a questionnaire can be sent to all staff to confirm awareness.

What does "good" business continuity management look like?	**RAG**	**Where are we**	**What do we have to do to get to green**	**How do we demonstrate "good"**
Plans to mitigate the loss of key suppliers are in place	▨	There is a list of key suppliers and their services. In current contracts the continuity capability of suppliers is required.	Every supplier is documented and the service they supply is shown with the impact of a failure to supply this service documented. The recovery time and capability of this supplier is then proven and the Post Office plan to cover the failure is documented.	Suppliers work with the Post Office to demonstrate their recovery capability. In Post Office tests the capability to continue operations without key suppliers is challenged.
Tests of plans have been undertaken				

What does "good" business continuity management look like?	RAG	Where are we	What do we have to do to get to green	How do we demonstrate "good"
	▨ ▨	Some IT DR testing has been undertaken where possible.	Continue to work with the IT DR team on the capability to test systems and to ensure where tests are undertaken results and capability are passed to the business.	Annual full switch over DR of all key systems is undertaken.
	▨	Initial high level crisis exercises have been run.	Complete further crisis exercises in all key areas and continue to enhance the central crisis team through exercise	Annual crisis exercises for all areas are completed and more complex challenges are used each year.
	▨	An initial Chesterfield to Sungard exercise has been run.	Run a full day exercise in June 2017 of the capability to operate Chesterfield at Sungard	Chesterfield can relocate to Sungard at anytime to operate in a normal manner.
	▨	A communication test to the GE crisis team and to the BPT team has been completed.	Run out of hours communication tests of the capability to contact all key areas.	Every member of these teams can be contacted by SMS, email at any time of night or day.

What does "good" business continuity management look like?	**RAG**	**Where are we**	**What do we have to do to get to green**	**How do we demonstrate "good"**
	▨		Create a test programme for all offices and business areas across the Post Office and work through the entire estate to ensure all areas are aware of their plans and their strategies are proven.	Every function and key office across the estate has an annual exercise. Each Supply Chain depot is being visited in the next quarter to complete and exercise.
	▨	BPT team is in place but not trained or exercised in their roles	Facilitate a workshop of scenarios and confirm the roles and responsibilities and scope of the BPT.	BPT exercised annually and all members have clear plans and roles.
Training of personnel involved has been completed	▨	Other than through initial workshops and exercises no structured training has been completed.	Identify business continuity champions in each location and business area. Run training workshops to introduce them to business continuity and their responsibilities within their own area.	Champions are in place across all key areas with a good knowledge of the subject, proven through review that they can take responsibility to drive BC in their own areas.

All areas are subject to customer challenge and to internal audit review.

3.9 POL Disaster Recovery Position Paper

Authors: Mick Mitchell/Rebecca Barker Sponsor: Rob Houghton Meeting date: 20th July 2017

Executive Summary

Context

The recent BA Data Centre systems failure has shown again the criticality of having a strong Disaster Recovery (DR) framework, which is regularly tested and improved.

POL have contracted for regular Disaster Recovery exercises to be carried out by each IT supplier, with the results of their tests documented and refined to provide assurance that we can invoke Disaster Recovery in times of crisis.

POL IT have also recommended that there is a further postponement to carrying out a DR exercise on the IT services provided by Fujitsu until the Spring of 2018, noting that there has been no DR exercise on the Fujitsu estate since 2013 due, in part, to the fragility of the existing legacy estate.

The IT strategy further outlined the need to get the current DR position within POL, under control and ensure the appropriateness of recovery currently evidenced and assurance against the business needs of the organisation. This paper provides an update on the current position of DR within POL and the steps required to quantify and mitigate the current risks of this position.

Questions addressed in this report

1. What is the current state of our IT DR plans?
2. What actions do we need to take to mitigate our current risk exposure regarding Disaster Recovery?

Conclusion

- We have carried out a review of the current state of IT DR plans and find that, although we are performing IT DR testing, there are significant gaps
- We will implement a number of improvement actions to improve the definition of what we need, align this with business needs, and improve the governance and reporting against these plans.
- We propose a further review of progress at the next RCC in September.

Input Sought

The RCC is asked to support the proposed next steps outlined within this report and further review status in September 2017.

The Report

What is the current state of our IT DR Plans?

1. Although there are many examples of IT DR testing being progressed across our supplier base (see Appendix), POL IT do not have sufficient evidence that the level of Disaster Recovery across our IT estate is suitable for our business needs. This results in POL running with a higher risk position than our desired risk appetite around the recovery of core IT services.
2. The above position is somewhat difficult to specify as there is a lack of definition of requirement from POL on their specific DR needs for each key IT service – there is limited definition on the Disaster Recovery of each IT Service and these definitions are not periodically reviewed with changing business needs.
3. The governance around DR testing has been too weak and is being strengthened moving forwards. Atos, our SIAM partner, provide a service where they review IT Service Recovery plans but there have been historic examples of DR periodic exercises being postponed/cancelled due to business pressures without too much challenge. This has now changed and our IT Service Recovery reporting will give more visibility across IT and our business areas.

What actions do we need to take to mitigate our current risk exposure regarding Disaster Recovery?

1. We will carry out a full review of the current state of all services to understand what has been tested and summarise if there are any specific business risks exposed (e.g. we have a risk exception in place for Fujitsu IT Services until Spring 2018) and any risk mitigation action plans or business continuity actions required.

2. We will define a robust DR Framework for all our IT services to be used going forwards. This will address the current issue around the lack of definition of testing and recovery required.

3. We will carry out a review with business owners to ensure our IT DR plans align to the business continuity planning needs of POL.

4. We will implement improved governance around the process of periodic IT DR testing from our supplier base (e.g. only allow IT DR postponement after active challenge and sign off by IT and business owners).

5. We will improve the visibility of IT Service Recovery reporting within POL.

6. Where we believe we are carrying too much operational risk as a result of an outstanding DR we will build recommendations to “bring forward” DR for that

component and if that's not possible, run business continuity tests (as we are doing for FJ)

What do we need to do next to progress?

1. Get feedback from RCC on the action plan we are executing.
2. Represent the status of progress at the September 2017 RCC.

POL00401625

Appendix

Supplier	Gold Service	Silver Service	Bronze Service	Service Description	DR Availability target from official notification	last tested	successful	Managed By Atos	Service Owner	Process Owner	comm
Fujitsu	✓			Network Banking Service (POCA/Vocalink/Santander)	Within 2 hours	May-16	✓	✓	Martin Godbold		FJ rout
Fujitsu	✓			Network	Within 2 hours	May-16	✓	✓	Martin Godbold		Catalys
Fujitsu	✓			Debit Card System	Within 2 hours	May-13	TBC	✓	Martin Godbold		
Fujitsu	✓			On-line Transaction processing Service	Within 2 hours	May-13	TBC	✓	Martin Godbold		
Fujitsu		✓		Automated Payments Outpay (APOP)	Within 2-5 hours	May-13	TBC	✓	Martin Godbold		
Fujitsu			✓	Bureau Service	Within 2-5 hours	May-13	TBC	✓	Martin Godbold		
Fujitsu		✓		Web Services Including Moneygram	Within 2-5 hours	May-13	TBC	✓	Martin Godbold		
Fujitsu			✓	Logistic Feeder Service (LFS)	Within 2-5 hours	May-13	TBC	✓	Martin Godbold		
Fujitsu		✓		Automated Payments Service (APS)	Within 2-5 hours	May-13	TBC	✓	Martin Godbold		
Fujitsu			✓	Department of Vehicle Licensing Authority - Post Office MOT Enquiry	Within 2-5 hours	May-16	✓	✓	Martin Godbold		Faliure router,
Fujitsu			✓	Electronic Top-ups Service	Within 2-5 hours	May-13	TBC	✓	Martin Godbold		
Fujitsu			✓	Postal Address File (PAF) service	Within 2-5 hours	May-13	TBC	✓	Martin Godbold		
Fujitsu			✓	Transaction Enquiry Service (TES)	Within 2-5 hours	May-13	TBC	✓	Martin Godbold		
Fujitsu			✓	Track and Trace	Within 2-5 hours	May-13	TBC	✓	Martin Godbold		
Fujitsu	✓			PODG	Within 2-5 hours	May-13	TBC	✓	Martin Godbold		
Fujitsu		✓		Collect & Return Web Service	Within 2-5 hours	May-13	TBC	✓	Martin Godbold		
Fujitsu	✓			MDM (production environment)	Within 2-5 hours	May-13	TBC	✓	Martin Godbold		
Fujitsu	✓			Credence (production environment)	Within 2-5 hours	May-13	TBC	✓	Martin Godbold		
Fujitsu	✓			POLSAP (production environment)	Within 2-5 hours	May-13	TBC	✓	Martin Godbold		
Gemalto	✓			Biometric Application, Enrolment and Identification	within 4 hours	Mar-17	partial	✓	Martin Godbold	Charles Brown	further workal Katrina
FRES		✓		Travel Money Card	tbc	tbc	tbc	N/A	Jeff Smyth	Chris Dewe	
FRES			✓	Bureau Service	tbc	tbc	tbc	N/A	Jeff Smyth	Chris Dewe	
Computacenter	✓			DHCP	no RTO specified	Jun-17	✓	✓	Mick Mitchell		
Computacenter	✓			Active Directory	no RTO specified	Jun-17	✓	✓	Mick Mitchell		
Computacenter	✓			Email	no RTO specified	Jun-17	✓	✓	Mick Mitchell		
Computacenter	✓			OneDrive	no RTO specified	Jun-17	✓	✓	Mick Mitchell		
Computacenter	✓			Sharepoint	no RTO specified	Jun-17	✓	✓	Mick Mitchell		
Computacenter	✓			Skype	no RTO specified	Jun-17	☒	✓	Mick Mitchell		Furthe
Computacenter	✓			Ricoh Printer Server	no RTO specified	Jun-17	☒	✓	Mick Mitchell		Furthe
Computacenter	✓			Admin LAN	no RTO specified	Jun-17	✓	✓	Mick Mitchell		
Computacenter	✓			Firewall and DDoS	no RTO specified	Jun-17	✓	✓	Mick Mitchell		
Computacenter	✓			Core network	no RTO specified	Jun-17	✓	✓	Mick Mitchell		
Computacenter	✓			Wifi	no RTO specified	Jun-17	✓	✓	Mick Mitchell		
Computacenter	✓			VPN	no RTO specified	Jun-17	✓	✓	Mick Mitchell		
Accenture	✓			Credence (software)	tbc	not known	not known	N/A	Ben cooke		
Accenture	✓			POLSAP (Software)	tbc	not known	not known	N/A	Ben cooke		
Accenture	✓			CDP Web platform	21.4 hours	May-17	☒	✓	Jeff Smyth		IPSEC t fault re
Atos	✓			Service Desk	tbc	not known	not known	✓	Mick Mitchell		
Atos		✓		SDM12 (management tool)	tbc	not known	not known	✓	Mick Mitchell		
NCR		✓		Self Service Kiosk	tbc	not known	not known	tbc	Martin Godbold		ITSCM contra
BT / Verizon	✓			Branch Network	tbc	Feb-17	not known	N/A	Martin Godbold		BT no Verizo
BT / Verizon			✓	voice services	tbc	Feb-17	not known	tbc	Jeff Smyth		BT no Verizo
BT / Verizon			✓	Mobile Phones	tbc	not known	not known	tbc	Jeff Smyth		BT no
Ingenico			✓	Paystation	tbc	May-17	✓	✓	Martin Godbold		27th M
Moneygram		✓		Moneygram service	tbc	not known	not known	N/A	Jeff Smyth	Rob Scott	
Qmatic			✓	branch queue system	tbc	Aug-16	not known	✓	Martin Godbold		Should
Vocalink	✓			The Link network acts as a switching system	tbc	Jul-16	✓	✓	Martin Godbold		
HP		✓		Post Office Card Account services Contact centre	50% within 4 hours	not known	not known	N/A	Caroline Hilton	Caroline Hilton	David other
HP	✓			Post Office Card Account services Cheque Printing	Within 2 hours	not known	not known	N/A	Caroline Hilton	Caroline Hilton	David other
HP	✓			Post Office Card Account services Banking Engine	within 3 hours	not known	not known	N/A	Caroline Hilton	Caroline Hilton	David other
HP			✓	Post Office Card Account services Document Processing	within 24 hours	not known	not known	N/A	Caroline Hilton	Caroline Hilton	David other

4.1 LRG - Risk and Controls

Author: Richard Williams/Deana Herley Sponsor: Jane MacLeod Meeting date: 20 July 2017

Executive Summary

Context

The central risk team has used the underlying Placemat methodology with management to assess the risks relevant to Legal, Risk and Governance (LRG). This paper gives a summary of the results for the LRG Placemat.

Questions this paper addresses

1. What process did we go through?
2. What are the outputs by Team?
3. How has the Placemat been populated?
4. Where do we continue to learn and improve?
5. Where next?

Conclusion

1. As an initial step, LRG's capabilities within the Target Operating Model (TOM) were re-assessed with management. A "bottom up" approach was then taken to identify key enabling processes, risks (including the mapping to Placemat principle risks) and controls.
2. A Risk and Control Matrix (RACM) document as an output has been developed for each team. The outputs will be used as Risk Registers going forward.
3. Whilst recognising the presentation of the Placemat remains conceptual, as per the format used by Barclays, it has been populated as an aggregation of the detailed information contained within the RACMs. Appendix 1 shows the Placemat through two lenses, firstly by team and secondly by stakeholder impact.
4. We have learnt that the way in which the Placemat is currently populated as an aggregation of team risks "bottom up", would now benefit from a "top down" functional view, consolidating risks across teams where relevant. We believe this approach will identify a more integrated / strategic view of LRGs top risks to drive the most effective remediation response. A remediation plan will be developed to align with this approach and will be presented to RCC members in September. The way in which the Placemat is presented will also be reviewed in light of this work and informed by working in unity with Finance and Operations on the current roll out. In addition, further roll outs may also identify other dependencies on LRG, which may in turn challenge its own internal assessment of capabilities, principle risk ratings and stakeholder impacts.

5. A pilot with the Payments team is planned for late July, after which it is proposed that the approach is rolled out to the wider Retail business.

Input Sought

6. The Committee is asked to review this report and confirm its support for the direction of the roll out.

The Report

What process did we go through?

7. The capabilities for LRG within the Target Operating Model (TOM) were firstly re-assessed with management from which key enabling processes, risks and controls were identified. This has given greater clarity over LRG's operating model, ensuring it is aligned to objectives, processes and outputs as well as, identifying what potentially prevents the function from delivering.

LRG Teams	Capability Description
BCP	The ability to determine impacts of incidents and improve response.
	The ability to develop and embed BCP governance framework.
	The ability to support external bids.
	The ability to train staff on their responsibilities.
CoSec	The ability to design, implement and maintain the governance framework by which the organisation is directed and controlled; and ensure accountability, fairness, and transparency in its relationship with stakeholders.
Financial Crime	The ability to manage identify and monitor compliance with applicable law and regulation relating to Financial Crime.
	The ability to detect and investigate fraudulent activity within the organisation and use / ownership of products and services supplied by the organisation.
	The ability to lobby for changes in legislation/regulation affecting Financial Crime.
IPA	The ability to (a) provide advice regarding compliance with Data Protection and Information Security laws; (b) the design of policies, and setting of standards to ensure our ability to use Personal Data; and (c) the assurance of the effectiveness of the control frameworks to protect Personal Data, other valuable information and information systems from unauthorised access and use in order to ensure the confidentiality, integrity and availability of valuable data (including Personal Data).
Internal Audit	The ability to systematically and independently examine data, records, operations and performances of the organisation's activities to ensure compliance with standards, policy, regulation and legislation. Working knowledge of professional internal auditing standards and of risk management frameworks.
Legal	The ability to provide legal advice and guidance regarding legal and regulatory issues relevant to the organisations business and operations. The ability to provide advice on and assess the effectiveness of controls and processes to mitigate legal risk.
Portfolio	The ability to identify, monitor and manage compliance with law, regulation, standards and guidelines, in respect of the FOIA, Section 7 of the DPA.
	The ability to ensure all security, training, awareness and campaigns are delivered to minimise crime and business loss through ensuring Post Office personnel and the general public are risk aware, cognisant of impacts and able to minimise the effects.
Risk	The ability to provide second line oversight by establishing a risk management framework and supporting policies, the provision of risk guidance across the business and embedding, monitoring and reporting on the level of risk relative to set appetite.

8. The assessment of risks and controls has been undertaken through a series of workshops and follow up meetings with relevant colleagues. This has enabled management to identify risks affecting their particular areas of responsibilities, assess the effectiveness of the various controls, and ensure a greater awareness of areas where risks could be outside appetite.
9. As part of the process, Team Leads in conjunction with their teams were requested to assess the risks before and after the application of their mitigating controls taking into consideration assurance results, historical incidents and audit findings. This

exercise has informed which principal risk categories of the placemat were applicable, or where reliance is placed on controls operated by other business areas.

10. As a final step the Placemat (by Team and Stakeholder) has been populated by assessing and rating each principle risk. This process demonstrated the dependencies, and helped to assess the adequacy of existing controls and the need for any remediation or additional controls. The risk rating process takes into account:

Likelihood and impact of risks Effectiveness of design and operation of controls (self-assessment) Minimum standards by principle risk Reported risk incidents and exception requests Internal and external assurance, including audit findings and follow up

What does the LRG risk and control portfolio look like?

11. A total of 79 risks have been identified, from which,
    - 25 risks are scored as low risk (green) and considered out of scope.
    - 54 risks are scored as amber (39) and red (15) and considered in scope.

12. The risks in scope have an average of score of 9, with an overall amber control rating. 53% of the risks sit within the Legal and Regulatory category of the Placemat followed by People (19%), Operational Financial and Technology (28%). By team, Financial Crime is currently carrying the largest proportion of risks (31%).

13. The initial self-assessment of LRG's top risks suggested that 7 have significant control exposures (red rating) set out below. Further work will be done to ensure that risks have been properly described, the controls are appropriate and ratings are proportionate. Further a "top down" view of risks and controls across LRG will be undertaken with particular consideration of the impact of on stakeholders.

Risks	Risk / Control	Current controls	Owner
Errors when managing disputes and a failure to prosecute. **(Legal / Legal and Litigation)**	■ ■	A dispute management process/protocol is being developed including specifically Agent Debt / Losses in the Network.	Ben Foat
Non-conformance in Bureau de Change. **(Financial Crime / Governance and Compliance)**	■ ■	Manual monthly monitoring by FAT. Bureau ID file – transactions market suspicious and / or of £5K and over is captured.	Sally Smith
Ineffective systems and insufficient staff may result in failure to effectively prevent and detect Financial Crime. **(Financial Crime / Staff Resourcing)**	■ ■	Resource requirements paper draft highlighting associated risks.	Sally Smith
Bureau de Change relationships for business purposes. **(Financial Crime / AML)**	■ ■	Coordinated reporting through Grapevine and SAR.	Sally Smith

Failure to accurately capture accurate ID details for mandatory and suspicious activity , as currently incorrectly captured on Horizon. **(Financial Crime / IT Controls)**	■ ■	As no automated controls to enforce this Fraud Analysis team are required to identify anomalies manually.	Sally Smith
Insufficient transaction monitoring driven by lack of centralised data, system / tools and therefore a reliance placed on third parties to provide this information. **(Financial Crime / Dependence on 3rd party IT)**	■ ▒	A risk based approach is being taken on a product basis to assess the exposure.	Sally Smith
Limited knowledge of and assurance over, compliance with regulatory requirements. **(Legal /Legal and Litigation)**	■ ▒	Current processes provide some measure of control based on people based controls. Legal has developed a regulatory matrix register, which defines the breath of regulatory requirements on Post Office and identifies the relevant regulator. Various policies have been established to manage these risks (AML, ABC) etc. The Legal team also uses a regulatory development tracker to update the business on changes to the legislative and regulatory landscape which are reported to the RCC and ARC through the Horizon Scanning report.	Ben Foat
Lack of understanding of how to manage contracts, including contractual obligations, contractual law and Public Contract Rules. **(Legal / Legal and Litigation)**	■ ▒	A Contract Obligations database has been developed, which currently applied to the 'Top 25' contracts. Legal news and updates bulletin (LAW NOW) has started for business users-also various training programmes have been and are being rolled out (for e.g. contract, judicial reviews, procurement). A legal instructions template will be created to ensure early and developed instructions.	Ben Foat
Insufficient budget and or resourcing may result in an inability to provide effective legal advice and management of legal risks. **(Legal / Wellbeing)**	▒ ■		Ben Foat
Inadequate adherence to PEPs and sanctions. **(Financial Crime / Governance and Compliance)**	▒ ■	Currently applying manual processes and screening with the use of Worldcheck.	Sally Smith

POL00401625

LRG - Management Self Assessment of Control Environment (red and amber risks only)

As at 14072017

Risk Alignment				By Team								By Stakeholder					
	Principal Risks	GE Owner	Overall	Legal	IPA	Financial Crime	CoSec	Portfolio	BCP	Risk	Internal Audit	Board & ARC	Regulator	Customer	Agent	Client	Partners
OPERATIONAL	Process Mgt	TBC	3						3			▨		▨	▨		
	Outsourcing Governance	Alisdair Cameron	1			1										▨	▨
	Health & Safety		1				1					▨					
	BCP	Jane MacLeod	1				1					▨					
	11%		6	0	0	1	2	0	3	0	0						
TECH	IT Controls	Rob Houghton	1			1						■	■				
	Cyber Threat	Jane MacLeod / Rob Houghton	1		1							▨	▨	▨	▨	▨	▨
	Dependence on IT 3rd Parties	Rob Houghton	1			1						▨	▨				
	6%		3	0	1	2	0	0	0	0	0						
LEGAL & REGULATORY	AML	Jane MacLeod	1			1						■	■	■	■	■	■
	Financial Crime & Fraud		5			2		3				▨	▨	▨	▨	▨	▨
	Information Protection & Assurance		6		4	2						■	■	■	■	■	■
	Legal & Litigation		8	5	3							▨	▨	▨	▨	▨	▨
	Governance & Compliance (inc Policy)		9			7		1	1			▨	▨	▨	▨	▨	▨
	53%		29	5	7	12	0	4	1	0	0						
FINANCIAL	EBITDAS Growth, inc Scorecard	Alisdair Cameron	2	2								▨					
	MI & Data		1			1						▨					
	Financial Controls & Reporting		3							3		▨	▨				▨
	11%		6	2	0	1	0	0	0	3	0						
PEOPLE	Staff Resourcing	Martin Kirke	7	2	1	1	1	2				▨					
	Staff Engagement		1	1								▨					
	Staff Wellbeing		2	2								▨					
	19%		10	5	1	1	1	2	0	0	0						

(Principal Risk Coverage 18/34 = 53%)

	Overall	Legal	IPA	Financial Crime	CoSec	Portfolio	BCP	Risk	Internal Audit
NUMBER OF RISKS (count)	54	12	9	17	3	6	4	3	0
VALUE of RISKS (accumulative score)	480	113	100	156	18	45	26	22	0
RISK AVERAGE SCORE (= score / count)	9	9	11	9	6	8	7	7	0
CAPABILITIES	14	1	1	3	1	2	4	1	1

	Risk RAG	Control RAG	No of Risks	Placemat
Metrics used in Placemat				
	▨	■	11	✓
		▨	26	✓
		■	2	✓
	■	■	3	✓
		▨	7	✓
		■	5	✓
			54	✓

Key		
	■	Significant control weaknesses and gaps
	▨	Control deficiencies exist where mitigating controls may be in place, but where improvements are required to reduce exposure, which contain risks with red rated control effectiveness
	▨	Control deficiencies exist where mitigating controls may be in place, but where improvements are required to reduce exposure
	■	Controls within minimum standards
	P	Reliance on controls in other areas (Work in Progress)

Risk & Compliance Committee meeting-20/07/17

POST OFFICE
RISK AND COMPLIANCE COMMITTEE

4.2 Incident & Exception Reporting

Author: Adnan Killedar Sponsor: Richard Williams Meeting date: 20 July 2017

Executive Summary

Context

The purpose of this paper is to provide a summary of *material* risk incidents and exceptions, and an analysis of how these can provide useful information about the assessment and management of the Top Risks.

Questions this paper addresses

- What do the incidents we have experienced tell us about our risk assessment?
- What do the exceptions being raised tell us about the effectiveness of our policy and control environment?

Conclusion

1. The number of material **incidents** reported has increased to fifty five since the last RCC (May 2017). This is against twenty nine between the March and May RCC meeting and thirty one between January and March RCC meeting.
2. The Central Risk team continues to highlight the importance of the Incident Reporting process to the Risk Champions and business teams to ensure that this process is known to all key staff members in the new organisation structure of the Post Office. The Central Risk team used the opportunity provided by the Placemat workshops to renew this message.
3. The **Exceptions** process was implemented from December 2016. A review of the process is underway with Risk Champions been asked to provide their feedback. By the nature of each exception case, we seek an understanding of which aspect of the risk framework is being breached. This picture will develop as the process matures and we expect to start to get insight over the next six months to inform on the effectiveness of our policy and control environment.

Input Sought

4. The Committee is asked to note the incidents and exceptions and consider whether these are consistent with the assessment of how well risks are being assessed and managed.

The Report

What do the incidents we have experienced tell us about our risk assessment?

5. All reported incidents align to our principal risks and have not highlighted the need for any new risks. A mapping of incidents to principal risks is provided in Appendix A. Of the eighty four incidents since the March RCC, the following incidents would appear to be the most material based on number of impact and frequency.

- Network Fraud
  There have been fifteen cases of fraud in our network in the last eleven weeks. The total amount of the fraud is circa £3.18 million.
- Customer Complaints
  There have been eight incidents where we were not able to meet customer expectations. Range of incidents ranged from not handling their personal information appropriately, delay in lodging request for blocking of account and not treating customers in an appropriate manner.
- Safety
  There were four cases of robbery at branches which was higher than the previous period in which there were three reported cases of robbery. Two of these resulted in a combined loss of £36k and there was no financial loss in the other two cases as the alarm and smoke cloak were activated. There were no injuries in any of these cases.
- IT and Information Security
  There have been three incidents, namely inappropriate access of one staff member to confidential information, HR help desk holding user's passwords in clear text and vulnerability on Post Office website due to errors in coding.

What do the exceptions being raised tell us about the effectiveness of our policy and control environment?

6. No new exceptions have been approved and none have been closed since the last RCC. There are two approved exceptions relating to Robotics software in the service centre and Project Finch (now renamed as Project Phoenix) which are past due. Actions to close the Robotics exception have not been completed by 1 May 2017, and by the revised date of 30 June 2017 was provided. The delay is due to lack of funding for hosting the required infrastructure. Project Finch closure deadline has been moved to end of August 2017. Nine draft exceptions are at various stages of the process.

- Approved Exceptions

Name / Area	Exception Category	Accountable owner	Close date
Robotics / Finance Service Centre	Policy	Angela Van-Den-Bogerd	1 May 2017, revised to-30-06-17. New closure date unknown as funding currently not available.

Project Finch / Financial Services	Regulatory	Owen Woodley/ Nick Kennett	30 May 2017, revised closure date August 2017.
SalesForce – Procurement	Regulatory	Barbara Brannon	29 April 2018

- Exceptions In-progress

Name / Area	**Category**	**Accountable owner**
AEI Cameras	Appetite	Rob Houghton
Back Office Transformation Tower Pen Test / IT	Policy	Rob Houghton
First Contact Resolution	Policy	Rob Houghton
Interchange	Regulatory	Rob Houghton
Kalido licensing	Appetite	Rob Houghton
Paystation / IT - Procurement	Regulatory	Rob Houghton
Qmatic / IT – Procurement	Regulatory	Rob Houghton
TDC	Appetite	Rob Houghton
Toto Smart metre	Policy	Kevin Gilliland

Appendix – A

Risk Management Information - as at 30 June 2017

No	Principal Risk	Incidents by RCC			
		Jan-17	Mar-17	May-17	Jul-17
OPERATIONAL	Process Mgt	4		2	9
	Product Development				
	Payments Process				
	Records Management	3			
	Suppliers, inc Procurement & Contracts		5	1	1
	Outsourcing Governance				
	Change		2	2	3
	Health & Safety	5	7	4	3
	BCP	1		2	3
	Operational	**13**	**14**	**11**	**19**
TECH	IT Controls	3	2	3	4
	Business Interruption	16	6	1	
	Cyber Threat			2	1
	Dependence on IT 3rd Parties				1
	Technology	**19**	**8**	**6**	**6**
LEGAL & REGULATORY	AML				1
	Financial Crime & Fraud	6	1	2	15
	Conduct, inc TCF, Product, Vulnerability				
	Information Protection & Assurance			5	8
	Reputational inc Customer Brand, Stakeholder		1	1	2
	Taxation				
	Legal & Litigation		1		
	Governance & Compliance (in Policy)	5	3	1	
	Legal & Regulatory	**11**	**6**	**9**	**26**
FINANCIAL	EBITDAS Growth, inc Scorecard				
	MI & Data			1	
	Financial Resources / Cash			1	2
	Subsidy Dependence				
	Pension Cost				
	Financial Controls & Reporting	4	1		
	Financial	**4**	**1**	**2**	**2**
STRATEGY	Competitiveness				
	Market		2		
	Customer Relevance	1			
	Strategic Risk	**1**	**2**	**0**	**0**
PEOPLE	Staff Resourcing			1	
	Staff Engagement				
	Staff Wellbeing	2			2
	Staff Integrity				
	People	**2**	**0**	**1**	**2**
	Totals	**50**	**31**	**29**	**55**

POST OFFICE

RISK AND COMPLIANCE COMMITTEE

5. Internal Audit Report

Author: Johann Appel   Sponsor: Jane MacLeod   Meeting date: 20 July 2017

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 Audit, Risk and Compliance Committee (ARC) in May 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 March RCC and ARC meetings?
- What progress is being made with completion of audit actions?
- Have any significant issues arisen that the committee should be aware of?
- What are the terms of the agreed timetable for internal audit reports, which is aimed at improving the audit reporting process?

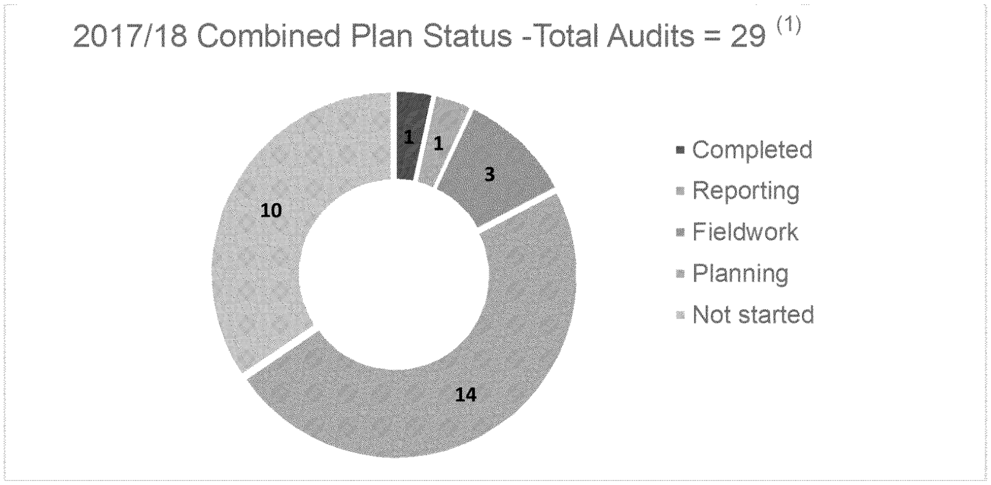
Conclusion

1. Progress against plan (2016/17):

At the time of the May ARC meeting, five reports from 2016/17 were still being finalised and cleared with management. These reports have since all been issued and circulated.

2. Progress against plan (2017/18):

Having finalised the 2016/17 audit programme, work on the 2017/18 plan has started and is progressing well. Current status is as follows:



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

3. Open and Overdue Audit Actions (as at 30 June 2017):

Audit Action Status:	
Open (not yet due)	56
Overdue (<30 days)	6
Overdue (>30 days)	2
Total	64

For details please see par. 10.

4. Significant Issues:

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

5. Internal Audit Service Level Agreement (SLA):

The introduction of an internal SLA between Internal Audit and the business was supported by the ARC. In terms of this SLA, Internal Audit will issue a draft report within 10 days from the close of audit fieldwork, thereafter management will have 10 working days to review and comment. The SLA is explained in more detail in par. 11.

Input Sought

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

The Report

6. Changes to Plan since May RCC and ARC meetings

Following a request from management, a review of the Lottery Pay-out Verification Process was added to the plan. This will be a low effort review limited to assessing the design effectiveness of new controls that are currently being implemented.

7. Internal Audit Reviews Completed

Since the May RCC and ARC meetings, we have finalised and issued the following five review from 2016/17. These have been separately circulated and will not be discussed in further detail in this paper:

	Audit	**Rating**
1.	FS - Branch Network Sales Quality Assurance Process	Average
2.	Network Branch Service Centre - Handling of Agents Queries and Complaints	Needs Improvement (Average)
3.	Project Expenditure Approval Process (Change Assurance)	Lessons Learned
4.	3rd Party Vendor Management (Change Assurance)	Average
5.	Financial Controls Framework (Independent Testing)	Satisfactory

We have also finalised one review from the 2017/18 year plan. Following is a summary of the key findings from this review:

Audit	Key Messages
VAT Process & Controls (Ref. 2017/18-02) Needs Improvement Audit actions: P1 0 P2 3 P3 4 Total 7	This audit has found that generally POL manages its VAT affair effectively. The tax team are consulted on a regular basis and are involved in the decision making process to ensure that VAT is applied and managed correctly. VAT risk is managed proactively and the controls in place operate effectively. POL has a good relationship with HMRC and as evidenced through transparent communication and documentation. The following control weaknesses were reported: • There was no documented tax strategy, governance and control framework. Incomplete documentation of tax processes was identified by HMRC prior to this internal audit - this was disclosed to the ARC and remedial actions are underway. • VAT processes and controls are not well documented and is to a large extent reliant on the knowledge and experience of the two individuals in the VAT team, both who are leaving the business imminently. The delay in finding a suitable replacement may adversely impact the proper handover of the process and transfer of knowledge **Update:** A replacement VAT manager was appointed and handover has begun. • Some known system and process issues require ongoing manual intervention to ensure compliant VAT treatment. The manual adjustments are generally low in value, however, makes for an inefficient process.

Management have accepted the audit findings and corrective actions have been agreed.

8. Reviews In Progress

	Review	Status / Remarks
1	IT Controls Framework (Advisory)	Ongoing – providing challenge and input to the project.
2	IT Security Transformation (Advisory)	Ongoing – providing challenge and input to the project.
3	Mails Process - Phase 1	Report being drafted – Employing data analytics to consider the robustness of the RMG mails segregation processes and procedures, as well as the appropriateness and application of their sampling methods.
4	SAP SF Payroll Migration (Change)	Fieldwork – Nearing Completion

9. Reviews In Planning

We request management's cooperation in agreeing the scope and timing of the following reviews that are being planned for delivery in Q2 and Q3:

	Review	Timing (start of fieldwork)
1	Lottery Pay-out Verification (design effectiveness review)	July
2	Branch Cash Forecasting	Aug
3	Compliance with Banking Framework	July - Aug
4	MoneyGram: AML Compliance	July
5	Cyber Security - Phase 1	Aug
6	Branch Technology - EUC Transition (Change)	Sept
7	IT Networks (Change)	Sept - Oct
8	EUM (Change)	Aug
9	Integrated Change Plan and Dependencies (Change - to be delivered as a peer assist review (advisory))	Aug
10	PCI Compliance (Change)	Oct
11	Back-office Transformation (Change)	Aug - Sept
12	Chameleon (Thin Client Solution) (Change)	Sept
13	Network Development PIR (Change)	Aug - Sept
14	Gating Process – Effectiveness (Change)	Sept

10. Updates on Internal Audit Overdue Actions

Audit Action Status:	BAU	Change	Total
Open (not yet due)	48	8	**56**
Overdue (<30 days)	1	5	**6**
Overdue (>30 days)	0	2	**2**

Total	49	15	**64**

Audit actions are generally being completed on time. Following is a summary of overdue actions, estimated revised completion dates and latest status update:

Description of action	Due date	Revised Date & Comment
Information Security Review (Change) (Rob Houghton / Jane MacLeod)		
Restriction of copy, transfer and paste functionalities on Office 365.	30/06/17	30/09/17 Controls through this are being implemented onto Mobile devices as phase 1 which are due to be completed in July 2017, the implementation of controls for laptops/desktops will be implemented in August 2017. Once implemented, the team will look at further controls around O365 access. This will be September 2017.
Implementation of a multi-layered approach to prevent data leakage.	30/06/17	30/09/17 New controls through BYOD are being introduced throughout July/August. Further consideration will form part of the ongoing Security Roadmap.
Review contracts with third party suppliers to ensure compliance.	30/06/17	30/09/17 IPA 'House Position' for Information Security has been drafted. IPA and Legal are now planning the approach to review all significant contracts against the House Position.
Provisioning of a Security Operations Centre (SOC) to manage firewalls.	30/06/17	30/09/17 Solution design is complete and implementation partners have been down-selected to two, with preferred bidder being selected at end July. The aim is to get the initial service live in September 2017 with rollout to full SOC capability by the end of 2017.
Consideration of Information Security clauses in employee contracts.	31/12/16	31/07/17 ISC has been re-launched and will take a decision at its next meeting whether to include the information security clauses in employee contracts.
Provision of "Information Security and Data Protection Manual" to all new employees upon joining.	31/03/17	31/07/17 IPA will consider if this action is the most effective solution to mitigate this risk and will make a decision on how to proceed.
Expenditure Approval Process (Change) (Al Cameron)		
Reiteration of spend commitment process.	30/06/17	31/07/17 Finance are drafting supporting comms – it will be added to the minimum standards once it's agreed and issued.
Data Protection (Jane MacLeod)		
Issue communication around the use of BYOD for	30/06/17	31/07/17 Preparing a Branch Focus document to remind all branches, including agencies and Multiples of

accessing PO related information.		their responsibilities in relation to Data Protection (including BYOD).

11. Internal Audit Reporting SLA

At the May ARC meeting, the committee expressed their concerns about the time it takes to finalise audit reports. Unfortunately slow response to audit reports (both from operational management and GE) often delays the completion of audits and reduces the effectiveness of the audit process in addressing control weaknesses in a timely manner. The introduction of an internal SLA between Internal Audit and the business was supported by the ARC and will establish the expectations for preparing and clearing audit reports.

Activity	**Proposed Timeline**
Prepare draft report (IA)	10 working days post fieldwork closing meeting
Operational management to review and comment	5 working days post issuing the draft report
GE Sponsor clearance	5 working days post agreement by operational management of the draft report
Final Report (Total)	**20 working days post closing meeting**

The reporting timeline will be explained at the start of each audit in order to set the expectations.

END OF REPORT

POST OFFICE

RISK & COMPLIANCE COMMITTEE

Vulnerable Customer Policy

Author: Jonathan Hill Sponsor: Kevin Gilliland & Nick Kennett Meeting date: 20th July 2017

Context

Post Office's vulnerable customer policy is currently in draft only. Whilst we have a long tradition of identifying and supporting customers that need extra help to access our products and services; we have not articulated our approach in a formal policy.

Purpose

1. This paper sets out the proposed policy, which aims to:
   - Articulate Post Office's expectations as to how the business and its staff and agents identify and help customers, who might be vulnerable, during their interactions with Post Office, its products and services.
   - It outlines the types of vulnerability customers may face and our responsibilities whether this be through laws and regulation or just by 'trying to do the right thing' by our customers.
   - It will also be a useful reference point for stakeholders who ask to see our documented approach to vulnerable customers.
2. It also presents proposals to implement and roll out the policy across the Post Office.

Conclusion

1. We have drafted a Vulnerable Customer policy that is practical and requires little immediate change.
2. Post Office is already assisting vulnerable customers in a wide variety of ways, both physically (access to services through branches) and through providing clear information about products and services.
3. The implementation plan is based around a simple risk assessment that each business area needs to undertake during 2017/18 to enable Post Office to identify any gaps in its services to support vulnerable customers.
4. Regulators are becoming increasingly focused on supporting vulnerable customers and are looking to firms to set out how they are doing so.

Input Sought

The R&CC is asked to agree the policy and the implementation plan prior to this going to the Post Office ARC for approval.

The Report

The Policy

1. The proposed Vulnerable Customer Policy is attached in Appendix A.
2. The policy is set out over three sections:
   - Section 1 sets out an overview of the Policy, its purpose, core principles and legislative/industry sources.
   - Section 2 provides a high level risk assessment of the main identified vulnerabilities and the minimum control standards Post Office aims to have to support customers.
   - Section 3 explains how people can raise concerns and where to seek further information.
3. Increasingly, activities and policies to support vulnerable customers are becoming more of a focus for regulators, in particular the FCA and Ofcom. Ofcom has asked if we would share our policy when it is finalised.

Implementation and roll out

4. The working assumption is that we are broadly compliant with the policy which has been set at 'high level' principles.

   There are indicators where MI relating to our vulnerability performance can (and have been) reviewed to assess compliance. These include;
   - Complaints
   - Pressure group feedback and complaints
   - Compliance monitoring by FS&T Risk including video mystery shopping
   - BoI monitoring and other feedback
   - Risk incident management information
   - Telecoms "Dunning" MI (vulnerable customer bad debt information)
   - As part of our wider risk assessment work, we will identify more sources of information (see below)
5. We would expect the policy to be communicated in the usual way through team talks and 'One' communications, emphasising that this is a continuation of the approach we already have at Post Office. FS&T Risk and Retail will agree the content of these communications, working with Group Communications.
6. To support our approach to customer vulnerability the FS&T and Retail teams will undertake a vulnerable customer risk assessment and gap analysis to be completed by the end of Q4 2017/18. The format will be guided by FS&T Risk, working with Group Risk. The risk assessment will include vulnerable customer identification, risk assessment and mitigation plans broken down into product/service/channel. We will, wherever possible aim to use existing work to populate this assessment, for example, existing product risk assessments.
7. The outcome of the risk assessment and the associated recommendations should be communicated to relevant staff as guidance as to best practice.

8. To ensure that any new initiatives to be taken forward are aligned, a vulnerability harmonisation team comprising relevant business area representatives will be formed. It would be the joint responsibility of the policy owners to establish and chair this group.

9. We would not expect the harmonisation group to be a formal committee and it would meet on an ad hoc basis but would include;
   - A representative from each area impacted.
   - Project Portfolio Manager from the lead team (main business area impacted).
   - Network gateway team will be engaged for all initiatives potentially impacting on the branch network.
   - A representative from Post office Group Risk to review the risk assessment and to provide an independent check on Post Office wide inclusiveness.

10. The harmonisation group would review whether any new proposal was aligned with wider Post Office activity and that this was not duplicating other work. This group would need to support any new business case for change.

11. Any proposed new initiative or business change would need to be agreed and budgeted with the approval of the relevant business unit, who would need to sponsor the initiative.

12. New (and existing) initiatives will be recorded and reported to the Policy Owners. This will be a useful indicator of progress made and to communicate to our stakeholders.

Jonathan Hill
Head of Risk and Regulation, FS&T

Vulnerable Customer Policy

Version – v0.2.1

Customer Policy July 2017 v0.2.1

POL00401625

Group Oversight Committee:	Audit and Risk Committee
Sign-off Authority:	Risk and Compliance Committee
Policy Sponsor:	Kevin Gilliland and Nick Kennett
Policy Owner:	Tom Weschler and Jonathan HIll
Policy Author:	Paul Beaumont and Jonathan Hill
Approved by:	
Approved:	TBC
Next review:	TBC

1. Overview

1.1. Introduction by the Policy Owner

At the Post Office we are committed to providing quality products and services for all our customers. We work in an open and responsible way that builds the trust and respect of all our customers. Post Office seeks to ensure that all customers are provided with good product and service choices, so that they can make good buying decisions and have a positive experience when dealing with us.

Addressing the needs of vulnerable customers is core to Post Office's social purpose and is aligned to our objectives to be 'Better for Customers' and a 'Great Place to Work'. There are countless examples of how we assist customers when they need us most. This policy outlines the policy approach so that we continue to ensure that we are able to look after the needs of vulnerable customers.

1.2. Purpose

To articulate Post Office's expectations as to how employees and agents identify and help vulnerable customers during their interaction with the Post Office its products and services. This will also be an important document and source of information on Post Office's policy approach for many of our stakeholders.

1.3. Core Principles

Much of consumer protection legislation is underpinned by the notion of the average or typical consumer, and what they might expect, understand or how they might behave. Some consumers may be significantly less able to represent their own interests, and more likely to suffer a greater risk of customer detriment than the average consumer, with regard to achieving the most appropriate price, service, product or quality available to them. This may be for a variety of reasons, as outlined below (this list is not exhaustive).

Vulnerability can impact in many ways and these categories are examples. The Post Office recognises that these customers may have additional needs and may be described as 'vulnerable' although it is important to note that these customers may not regard themselves as such. It is core to Post Office's rationale and purpose to ensure that appropriate respect and care is taken of all types of customer, including vulnerable customers.

Categories include:

A. Restricted Mobility	E. Mental Capacity
B. Communications Needs	F. Age Related Vulnerability
C. Low Basic Skills	G. Life Event Vulnerability
D. Low Financial Capability	e.g., bereavement, critical illness, redundancy
	H. Financial Difficulties

1.4. Application

There are already many examples of how Post Office assists vulnerable customers these include:

- Improving disabled access and fitting hearing loops
- Team talks on vulnerability
- Financial Services and Telecoms training on vulnerability e.g., "Delivering a Great Customer Experience", "General Compliance" training modules and the "Compliance Training Manual for Broadband and Phone"
- Training on mental health awareness risk
- Participation in National Police initiatives to mitigate frauds on vulnerable customers
- Rolling out the Banking framework to ensure financial access to communities including the vulnerable when bank branches are closing
- Our response to the Grenfell Tower fire and ensuring we could support customers in time of emergency
- Working with partners such as BoI who give case by case exceptions to the 'terms of conditions' for customers, for example customers in hospital unable to read banking correspondence and statements, or those that have suffered a bout of mental illness.

Post Office provides advice and guidance to customer-facing staff and those involved in the design of products and services and the processes that support their distribution and sale, regarding the legal requirements, regulatory guidance and relevant industry body recommendations, as well as Post Office recommended best practice.

It is the responsibility of those staff to ensure that they comply with and observe those requirements or guidance, and where there is any uncertainty, to seek clarification from relevant Post Office subject matter experts.

1.5. Risk

By not addressing the needs of vulnerable customers, the impact could be significant for those customers that depend on us to deliver our products and services. These risks are included in the minumum control standards section below but could include customers not being able to access our products or services, inappropriate purchases and not being able to understand the features or terms and conditions of a product or service.

It could also cause reputational damage undermining Post Office's achievement of its social purpose. Under both Ofcom and FCA rules there could be regulatory interventions for not treating vulnerable customers fairly.

1.6. Legislation

- Ofcom duties under the Communications Act
- Disability Discrimination Act 1995
- Equality Act 2010
- Mental Capacity Act 2005 and guidance
- Power of Attorney Act 1971
- Disability Discrimination Act (Northern Ireland) 2005.
- Adults with Incapacity (Scotland) Act 2000.
- Consumer vulnerability regulation detailed within the FCA Handbook for CONC and Mortgage Conduct of Business (MCOB).

1.7. Industry Guidance

- FCA website including 2016 Thematic Review on vulnerable customers
- ABI/BBA Codes of Practice
- Age UK advice line
- Money Advice Service
- Pensions Advisory Service

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 businesses transactions. It therefore defines the boundaries of activity and levels of exposure that the Group are willing and able to tolerate.

Post Office's risk appetite is **averse** for:

- non-compliance with law and regulations or deviation from its business conduct standards, and
- 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.

The Group acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sits outside the agreed Risk Appetite. In exceptional circumstances a Risk Exemption waiver may be granted.

2.2. Policy Framework

Post Office's Board has 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 vulnerable customer matters by reports from its committees including its Audit and Risk Committee.

It is the responsibility of the policy owners to review this policy at least once a year and on an ad hoc basis as necessary to ensure the policy remains effective and up to date.

This policy will be reviewed by The Post Office Risk and Compliance Committee at least once each year from the last date this policy was determined effective.

2.3. Who must comply?

Compliance with this policy is mandatory for all Post Office employees. We will work with our Agency network, Principals and key commercial partners to ensure that where we can the spirit of our approach to vulnerable customers is applied.

2.4. Minimum Control Standards

A minimum control standard 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 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 minimum control standard for the vulnerable customer policy is 'directive' and will be communicated to staff through staff communications and intranet.

We should maintain the existing training requirements that we have in place (for example this is covered in the annual Horizon FS handbook training, Team Talks and the 'Delivering a Great Customer Experience module' on Success Factors) and aim to build on this where we can to ensure that our approach is regularly communicated.

The table below sets out some of the key relationships between identified risk, the considered Risk Appetite, and the required minimum control standards:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible
Physical access to the branch network is difficult	**A) Restricted Mobility** A customer may be particularly vulnerable because they have mobility restrictions; this means that it might be difficult for them to gain physical access to our premises.	• We will seek to, where it is possible to do so, make 'reasonable adjustments' to our business premises to allow customers with mobility restrictions to access our business premises. • Where we are not able to make such adjustments we will seek, where it is reasonable to do so, to provide the customer with an equivalent service through other means.	Kevin Gilliland / Al Cameron
Customer engagement with products and services is not possible or limited because of a vulnerability	**B) Communications Needs** A customer may be particularly vulnerable because they have a hearing or sight impairment, which means they require specially adapted methods of communication.	• We will look to make 'reasonable adjustments' to the way in which we are able to communicate with our customers. For instance for sight impairment, we will seek to ensure that our customer documentation is available in a range of formats to help them understand our product material and product-life cycle communications • For hearing impairment, we will seek to provide hearing loops, and for our telephony staff, training in use of telephone relay technology.	Kevin Gilliland / Nick Kennett Al Cameron / Kevin Gilliland
	C) Low Basic Skills A customer may be particularly vulnerable because they have a low level of basic skills (including not having English as a first language) and therefore require additional or specialised assistance to	• We will seek to work positively and constructively with customers that have, or appear to have, a low level of basic skills. • We will seek to ensure that the use of jargon is minimised within our	Kevin Gilliland / Nick Kennett

	effectively make use of our products and services or, during the course of the product life-cycle, interact with us and manage their financial position effectively.	documentation. Where it is used we aim to ensure that there is an easy to understand explanation of the term. • We will look to provide sign-posting to free independent sources of information and support that the customer can access in relevant documentation and sections of our websites. • We will seek to explore how to simplify the information that we provide to customers, for example, through the standardised terms and conditions to highlight parts that matter. If appropriate we will engage with government and industry initiatives	
	D) Low Financial Capability A customer may be particularly vulnerable because they have a low level of financial capability (e.g. a specific lack of the maths skills and knowledge of financial products or matters) and therefore may require more straight-forward explanations.	• We aim to be clear and fair and not misleading in communications with customers, and wherever possible we will seek to avoid 'jargon'. We will strive to explain our products and services, including associated risks to customers, in a manner which is easily understandable. • We will seek to take reasonable steps to ensure there is sufficient 'sign-posting' across our product and service proposition to charities and other not-for-profit organisations that provide independent advice and guidance on financial issues	Kevin Gilliland / Nick Kennett
	E) Mental Capacity A customer may be particularly vulnerable because they have a mental capacity	• Be aware of the Power of Attorney requirements where applicable (refer to Horizon Help)	Kevin Gilliland/ Nick Kennett

	limitation (for instanced dementia, a learning disability, a development disorder, a neurological disability) that may restrict their ability to appropriately engage with us or make an informed and responsible borrowing decision.	• We aim in our dealings with a customer who we know, or reasonably suspect has a mental capacity limitation, to act sympathetically and positively. • We seek to allow a customer sufficient time to weigh-up the information and explanations we have provided and defer a decision to a later date. We will seek to provide all the information required to enable a customer to do this. Where possible we should ask if the individual would like to consider this decision with a family member or trusted person.	
	F) Age Related Vulnerability A customer may be particularly vulnerable as a consequence of the effects aging can have on an individual; this includes potential memory loss, dementia or the potential for the customer to be 'overwhelmed' by a particular situation.	• Be aware of the Power of Attorney requirements where applicable (refer to Horizon Help) • Post Office should not automatically assume that a customer is vulnerable by virtue of their age. We seek to provide appropriate products and services to customers of different ages. However, it is appropriate in some circumstances to explain clearly risks which relate to ageing customers e.g., for end of life planning products. • We aim in our dealings with a customer who we know, or reasonably suspect has a mental capacity limitation, to act sympathetically and positively. • We seek to allow a customer sufficient time to weigh-up the information and explanations we have provided and defer a decision to a later date. We will provide	Kevin Gilliland / Nick Kennett

		all the information required to enable this. • Where possible we should ask if the individual would like to consider this decision with a family member or trusted person.	
	G) Life Event Vulnerability A customer that has or is experiencing a specific adverse 'life event' (for example, redundancy, a bereavement, critical or terminal illness, or a marriage breakdown) could be particularly susceptible to making poor judgements. (Although these triggers may not always have a negative impact on the individual)	• We should aim to treat these customers fairly and with a level of sympathy and positivity. We aim to ensure, throughout our businesses, that when we become aware of these life events we have the ability to respond flexibly and deliver an outcome that is appropriate.	Kevin Gilliland / Nick Kennett
	H) Financial Difficulties Customers that are in financial difficulties (for instance high levels of debt or low levels of income) may be particularly vulnerable to financial detriment.	• Be conscious of customers in financial difficulties when designing or introducing products and services that require a regular financial commitment • Be able to manage expectations e.g., declines or alternate payment methods if applying for a product or service • Where feasible signpost Money Advice Service, Citizen's Advice Bureau, Pensions Advisory Service and/or other similar independent advice/helplines	Kevin Gilliland / Nick Kennett

3. Where to go for help

3.1. 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

3.2. How to raise a concern

Any Post Office employee who is concerned about the application of this policy should:

- Discuss the matter fully with their Line Manager; or,
- Report their concerns to the policy owner.
  If you wish to do this anonymously you should contact the 'Speak Up' line on GRO

3.3. Who to contact for more information

If you need further information about this policy, please contact Tom Weschler or Jonathan Hill

3.4. Company Details

Post Office Limited registered in England and Wales. Registered numbers 2154540. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.

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.

Version Control

Date	Version	Updated by	Change Details
July 2017	Draft 0.1	Jonathan Hill / Paul Beaumont	1st draft in revised template
11th July 2017	Draft 0.2.1	Jonathan Hill / Paul Beaumont	2nd draft in revised template

POST OFFICE
RISK & COMPLIANCE COMMITTEE

POLICY REVIEW

6.2 Financial Crime Policy

Author: Sally Smith   Sponsor: Jane MacLeod   Meeting Date: 20th July 2017

Executive Summary

Context

This paper sets out the updates and revisions to the Financial Crime Policy as part of the annual review process for the Risk and Compliance Committee to consider and approve.

Questions addressed in this paper

- What changes to the policy do we propose and why?
- What are the implications of these changes?

Conclusion

1. The Financial Crime Policy has been amended to reflect new legislation and clarifies minimum control standards, roles and responsibilities.
2. There are some minor changes to the requirements and minimum standards of controls which will be communicated to relevant stakeholders, and monitored on a business as usual basis by the Financial Crime team.

Input Sought

The R&CC is asked to approve the updated Financial Crime Policy.

The Report

Why do we need to review this policy?

3. The policy was last reviewed and approved by the R&CC in July 2016. The terms of the policy require it be reviewed annually

What changes to the policy do we propose and why?

What are the key features that we propose and why?

4. The policy template and format has been redesigned. This helps ensure that the purpose, core principles and impacts are understood. It sets out clear minimum control standards and responsibilities for application of those standards.
5. Key changes include:
   - We have updated the definitions of Financial Crime and included updates to reflect recent changes in regulations and laws that are applicable. We have also included the sources of industry guidance available in order to provide greater clarity.
   - We have updated the policy framework and the key linked and associated policies to provide greater clarity to individuals and stakeholders.
6. Risk Assessment methodology and Product Information Packs that have been developed over the last 12 months are now referenced for the first time.
7. A new section has been included clearly mapping minimum control standards, responsibilities and timescales.

How did we develop these recommendations?

8. The policy has been developed by reviewing recent legislation changes including the Criminal Finance Act 2017 and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.
9. Policy queries and issues that have arisen over the previous 12 months have been reviewed to ensure that these concerns are addressed.

What are the implications of these changes?

What will we need to do and by when, to implement and embed these policy changes?

10. Internal communications and training – once the policy has been approved, there will be a One communication to advise all employees of the changes and provide a link to the updated document on the Post Office Intranet. A series of workshops for product managers in Financial Services and Telecoms and Retail will be run by the Financial Crime Team during the second half of 2017/18 to provide training on 'business as usual' risk assessment methodology and use of the Product Information Pack and Risk Assessment tools.
11. The risk assessment tool for new products and services currently available on the Post Office Intranet is being enhanced, and when completed during Q3 2017/18, a communication will be sent to product managers with revised guidelines. It is not anticipated that any additional training will be required as this is an existing tool.

12.The Financial Crime team will monitor adherence to the minimum control standards set out in the policy on an on-going basis through their review of risk assessments, project business readiness and incidents. Any control gaps identified will be reported to the R&CC as required.

What will the impact be on our wider business?

13.The identification through documented risk assessment of potential or inherent and residual Financial Crime risks is not mature across the business and more needs to be done culturally to embed the methodology. Significant progress has been made over the last 18 months, and a number of high risk products and services have been formally assessed and documented. Additionally, the introduction of the Risk and Controls Matrix and Placemat methodology across the business is improving controls.

14.Design of compliance oversight monitoring to test the Groups controls and confirm effectiveness and adherence to Financial Crime policies, is not yet finalised. Work is planned by the Financial Crime team over the next 12 months to address this'

15.All business units are required to test the adequacy and effectiveness of key controls and key risk indicators in their areas relating to financial crime.

16. All business units are required to ensure that they consider financial crime risks in their area when developing their own Risk and Controls Matrix.

17.Financial crime control forms part of the half yearly Executive Declaration.

18.Although Post Office has an 'adverse' risk appetite, it is accepted that we cannot be 100% effective in preventing all losses and risk exposures. At this stage we have not tried to establish the 'tolerances' that are acceptable, as these should be considered on a case by case basis, however there are implicit tolerances in terms of budgets for losses, etc., across the business. Material issues are reported to the GE on a weekly basis, and also monitored through the Losses, Fraud and Crime Forum.

What would the impact be of delaying approval?

19. Post Office Limited is required to maintain up to date policies to support contractual requirements with clients and suppliers (e.g. MoneyGram and the Partner Banking Framework) and failure to do so may result in a breach of contract, and whilst not material, could have commercial and reputational impacts.

20.Post Office Limited is required to maintain up to date policies under its regulatory obligations, and failure to do so may lead to regulatory sanctions or penalties.

Post Office Limited provides Post Office Management Services with its policies suite in the form of "Group Policies". POMS is required under its regulatory responsibility to the Financial Conduct Authority to have up to date policies and failure to do so may lead to regulatory sanctions or penalties.

GROUP POLICIES

Financial Crime Policy

Version – V1.3

Chief Executive's Endorsement
The Post Office Group is committed to doing things correctly. Our Values and Behaviours represent the conduct we expect. This policy supports these to help us ensure the highest standards of financial crime prevention, detection and management are maintained.

1. Overview

1.1. Introduction by the Policy Owner

The General Counsel has overall accountability to the Board of Directors for the design and implementation of controls to prevent or deter Financial Crime. Financial Crime is an agenda item for the Audit and Risk committees 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 design and implementation of controls to prevent or deter Financial Crime throughout the Group[1]. 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 mitigation of risk across the Group. Compliance with these policies supports the Group in meeting its business objectives and to balance the needs of shareholders, employees[2] and other stakeholders.

1.3. Core Principles

The governance arrangements described in this Policy are based upon the following core principles:

- The interests of stakeholders are protected by ensuring that excessive powers are not delegated to individuals;
- Decisions taken by management are consistent with the Group's strategic objectives and Risk Appetite, which are approved by the Board;
- Appropriate conduct is demonstrated in executing the requirements contained within the Policy;
- Every member of staff is responsible for understanding and managing the risk they take on behalf of the Group;
- Clear accountabilities are delegated by management to people who have the right level of skill, competency and experience;
- All employees are required to comply with Group Policies.

1.4. 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.

In exceptional circumstances, where risk sits outside of the Group's accepted Risk Appetite a Risk Exception can be granted. For further information in relation to the risk exception process please see the Risk Exception process found here.

[1] In this policy "Post Office" and "Group" mean Post Office Limited and Post Office Management Services Ltd.

[2] In this policy "employee" means permanent staff, temporary including agency staff, contractors, consultants and anyone else working for or on behalf of Post Office.

While Post Office does not tolerate events that are criminal in nature and which may give rise to unacceptable and illegal behaviour, it recognises that despite its many endeavours, it is not possible to eliminate all risk of internal and external Financial Crime and as a result Post Office may incur losses, and therefore takes a risk based approach to Financial Crime.

Failure to comply with the requirements of this policy by any employee will be regarded as a significant breach impacting on the Group's risk and control environment and may lead to disciplinary action up to and including dismissal and possible prosecution.

The risk to the Group in relation to Financial Crime is reviewed by the board on a regular basis.

1.5. Financial Crime Risk

"Financial Crime" is any offence involving: fraud or dishonesty, misconduct in, or misuse of information or handling the proceeds of crime. It can be internal (by individuals within an organisation) or external (by criminals using an organisation to facilitate financial crime). Financial Crime is commonly considered as including the following offences:

- fraud
- electronic crime
- money laundering
- terrorist financing
- bribery and corruption
- information security

Failure to manage Financial Crime risks and incidents appropriately could result in financial loss, customer impact, regulatory breaches, fines, prosecution, prevention from selling a particular product, loss of existing or future contracts/relationships and damage to reputation.

These risks include, but are not limited to, the following:

External Financial Crime:
The risk of external events due to acts of a type intended to defraud, steal or misappropriate assets/ property, or which seek to circumvent the law, by a third party. Examples would include:

- Any dishonest or fraudulent act,
- Theft of assets from an organisation or its customers,
- Card or account abuse or account takeover by a third party,
- Counterfeit payment instruments (cards, cheques, etc.) and identity documents,
- ATM fraud and theft,
- Online or mobile fraud, and
- Social engineering fraud.

Internal Financial Crime

The risk of internal events due to acts of a type intended to defraud, steal or misappropriate assets/property, or which seek to circumvent regulations or the law applicable to an organisation or its contracts or internal policies or procedures. Examples would include:

- Any dishonest or fraudulent act circumventing regulations or law,
- Profiteering as a result of insider knowledge of an organisation's activities,
- Theft of assets from an organisation or its customers,
- Manipulation of transactional data at point of sale,
- False expense or payroll claims,
- Manipulation of accounts or financial statements, and
- Breach of internal processes or controls for personal gain.

The Group takes the above internal risks and Financial Crime seriously and will take appropriate action against any person including disciplinary and dismissal of anyone involved in such events.

1.6. Legislation

There are a number of relevant UK legal and regulatory requirements which describe financial crime including (but not limited to):

- The Fraud Act 2006
- The Bribery Act 2010
- The Theft Act 1968
- Common Law Offences of Fraud in Scotland
- The Proceeds of Crime Act 2002
- The Criminal Finances Act 2017
- Policing and Crime Act 2017
- The Terrorism Act 2000
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (known as Money Laundering Regulations 2017)
- Forgery and Counterfeiting Act 1981
- Identity Documents Act 2010

The group has regard for guidance and other assistance offered by regulatory, industry and other specialist bodies, for example UK Finance (which incorporates BBA, UK Payments and Financial Fraud Action UL), Link, etc., publish trends and analysis on current threats and issues.

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 businesses 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[3]:

- **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 ligation in relation to Financial Services matters
- **Averse risk appetite** for not complying with law and regulations or deviation from business' conduct standards for financial crime to occur within any part of the organisation
- **Averse Risk Appetite** in relation to unethical behaviour by our staff.

The Group also has a zero tolerance policy to criminal tax evasion and the facilitation of tax evasion.

The Group acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sit outside the agreed Risk Appetite. In this situation, a risk exception waiver will be required (See section 1.4 for further details).

2.2. Policy Framework

Post Office has established a suite of Financial Crime policies and procedures, on a risk sensitive approach which are subject to annual review. The policy suite is designed to combat money laundering, terrorist financing, bribery and corruption, fraud and ensure adherence to relevant sanctions regimes. They have been developed to comply with applicable legislation and regulation and cover the following specifically:

- The identification through documented risk assessment of potential or inherent and residual Financial Crime risks and the effectiveness of controls associated with them,
- Completing compliance oversight monitoring to test the Groups controls and confirm effectiveness and adherence to Financial Crime policies,
- On a risk sensitive basis, performing due diligence upon our employees, agents and third parties,
- Where the Group has primary or contractual responsibility for the customer relationship ensuring Customer Due Diligence, Enhanced Due Diligence and Sanctions checking are set at any appropriate level commensurate with the risk,

[3] The Risk appetite was agreed by the Groups Board January 2015

- Establishing and maintaining standards for Management Information on Financial Crime. This includes, but is not limited to, record keeping, customer identity documents, reporting of suspicious activity[4] and details of staff training.

[4] For more information in relation to the completion and submission of a Suspicious Activity Report please see the AntiMoney Laundering and Counter Terrorism Policy.

This policy provides an overview of the Financial Crime risk and governance framework and the effective system of internal control for the mitigation of Financial Crime risk required across the Group. The Key Financial Crime policies covering the major risk areas to the Group include:

- Anti-Bribery and Corruption Policy
- Anti-Money Laundering and Counter Terrorist Finance Policy
- Whistleblowing Policy

Associated Policies and Processes include:

- Information Security Policy
- Investigations Policy

Each of the above policies should be considered and read in conjunction with any other policy where relevant. These policies are supported by the Risk Exceptions process.

2.3. Who must comply?

Compliance with this policy is mandatory for all Post Office employees and applies wherever in the world the Groups 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 or have their own equivalent policy.

Where non-compliance is identified the matter must be referred to the Policy Owner. Any investigations will be carried out in accordance with the Investigations Policy. Where is it identified that an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary offence.

All Post Office employees are required to report any knowledge or suspicions (internal or external) in relation to Financial Crime please see 3.2.

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. The subsequent pages define the terms used in greater detail:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Proposed product or service	Products, services or relationships with third parties may rely on systems or processes where prevention or detection of financial crime has not been considered in the design, resulting in financial loss (whether to the Group, its customers or suppliers), reputational damage and/or regulatory sanctions.	Preventative Control: As part of the design of a new product or service: • A Product Information Pack (see 2.5 below) must be completed. • Product or service risks must be considered and documented using the Risk Assessment Tool (see 2.5 below).	Product Manager	During design phase
		Prior to launch the Product Information Pack and the Product and Service Risk Assessment must be reviewed and approved by the Financial Crime Team.	Financial Crime Team	Prior to Launch

Risk Area	**Description of Risk**	**Minimum Control Standards**	**Who is responsible**	**When**
Existing products and services	Due to changes in law, regulation, incidents, threats or practices over time, there is a risk that the controls to prevent and detect financial crime are no longer adequate.	Preventative Control: Where the product or service has had an initial Risk Assessment completed this must be reviewed and reassessed annually, or when there is a proposed change to the product or service. This reassessment must include a review of the Product Information Pack, a review of the existing controls and a re-evaluation of residual risk.	Product Manager	Annually, or at any time there is a change
		Where no initial risk assessment was undertaken, product management must agree a timescale with the Financial Crime Team to complete an assessment and a Product Information Pack.	Product Manager	Any time there is a change
		Where the reassessed risk is considered by the Financial Crime Team to rest outside of the Groups Risk Appetite, then the risk exception process must be followed.	Product Manager	Any time there is a change
		Corrective Control: Additionally, risk assessment must be undertaken where an issue is highlighted by monitoring or an incident occurs.	Product Manager	When there is a material issue or incident

Risk Area	**Description of Risk**	**Minimum Control Standards**	**Who is responsible**	**When**
Human Resources	Due to inadequate screening, there is a risk that the Group employs individuals who do not have the legal right to work in the UK or are unfit to undertake the role.	Preventative Control: To minimise the risk of financial crime by employees, Post Office completes employee screening prior to employment. In addition to this, on a regular basis (proportionate to the role) additional checks will be completed to ensure that there is no risk of internal collusion by any of our employees. For further information please see the employee vetting policy.	Director of Human Resources	Pre-employment and ongoing where required
Operations	Inadequate building and systems access controls may lead to financial crime that results in financial loss (whether to the Group, its customers or suppliers), reputational damage and/or regulatory sanctions.	Preventative Controls: Relevant business areas including the property and security teams must assess and assure risks relating to employee and customer access to sites, secured areas, systems and software, recommending and implementing additional controls where appropriate.	All employees	Ongoing
		All business areas are responsible for maintaining documented processes and procedures and deploying adequate monitoring and control to prevent and detect unauthorised access to sites, secured areas, systems and software to prevent financial crime.	All employees	Ongoing
		Detective Control: Audit trails must be maintained so that building and system access can be monitored.	Chief Information Officer and Physical Security	Ongoing
		To ensure that the Group's controls remain effective the Group undertakes internal audits to test and assess their effectiveness.	Internal Audit	Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Financial settlement and reconciliation	Inadequate controls and audit trails relating to financial settlement and reconciliation may result in financial loss (whether to the Group, its customers or suppliers), reputational damage and/or regulatory sanctions.	Preventative Controls: Relevant business areas must assess and assure risks relating to financial settlement and reconciliation and are responsible for maintaining documented processes and procedures and deploying adequate monitoring and control to prevent and detect financial crime.	Chief Financial Officer	Ongoing
		Detective Control: Audit trails must be maintained so that system access can be monitored.	Chief Information Officer	Ongoing
		To ensure that the Group's controls remain effective the Group undertakes internal audits to test and assess their effectiveness.	Internal Audit	Ongoing

2.5. Product and Service Risk Tools

Risk Assessment Tool
The Risk Assessment Tool has been created by the Financial Crime Team to assist Product Managers to determine the level of risk exposure and engagement required for new products and services. The Risk Assessment Tool takes into account inherent risks (e.g. payment method, channel, customer demographic etc), UK regulations and legislation and industry best practice.

The Risk Assessment Tool can be found here.

Product Information Pack
The purpose of the Product Information Pack (PIP) is to provide an overview of the product or service, including customer/transactional journey, parties involved, any contractual responsibilities, monitoring and control requirements. It should consider the inherent risks the product is exposed to from a Group and customer perspective and the framework for the effective risk mitigation of the product.

The existence of detailed operating policies, procedures and processes may be referred to throughout this document and is to be used to illustrate how the risks associated with the product are reduced.

The Product Information Pack can be found here.

3. Where to go for help

3.1. 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

3.2. 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 0845 603 4004; or,
- Report the matter directly to the Money Laundering Reporting Officer (MLRO)
- staff can contact the Post Office's General Counsel, currently Jan e MacLeod who can be contacted by email at: whistleblowing GRO or by telephone on: 07900 216851.
- Alternatively staff can use the Speak Up service available on 0800 0484531
- or via a secure on-line web portal: http://www.intouchfeedback.com/postoffice

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 financial.crime GRO

4. Governance

4.1. Governance Responsibilities

The policy sponsor, responsible for overseeing this policy is the General Counsel of Post Office Limited.

The policy owner is the Director of Risk and Compliance who is responsible for ensuring that the Financial Crime Team conducts an annual review of this policy and tests compliance across the Group. Additionally the Director of Risk and Compliance and the Financial Crime Team are responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee.

The Audit and Risk Committee are responsible for approving the policy and overseeing compliance.

The Board is responsible for setting the groups risk appetite.

5. Control

5.1. Policy Version

Date	Version	Updated by	Change Details
November 2016	1	Georgina Blair	Roll out of Final version
April 2017	1.1	Thomas Richmond	Review and update **in line with** updated regulations and new policy design
June 2017	1.2	Thomas Richmond	Updated in line with comments from stakeholders

5.2. Policy Approval

Group Oversight Committee: Risk and Compliance Committee and Audit and Risk Committee

Committee	Date Approved
POL RCC	
POMS RCC	
POL ARC	
POMS ARC	

Policy Sponsor: Group Director of Legal, Risk & Governance

Policy Owner: Director of Risk and Compliance

Policy Author: Head of Financial Crime

Next review: July 2018

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 an d Customs (HMRC), REF 12137104. Its Information Commissioners Office registration number is Z4866081.

6.3 Anti-Bribery & Anti-Corruption Policy

Author: Paul Blackmore and Thomas Richmond Sponsor: Jane MacLeod Meeting Date: 20th July 2017

Executive Summary

Context

This paper sets out the updates and revisions to the Anti-Bribery and Anti-Corruption (ABC) Policy as part of the annual review process for the Risk and Compliance Committee to consider and approve.

Questions addressed in this paper

- What changes to the Policy do we propose and why?
- What are the implications of these changes?

Conclusion

1. The ABC Policy has been amended to reflect new legislation and clarifies the minimum control standards, roles and responsibilities
2. The updated Policy reflects all recommendations made as part of the external risk assessment of the ABC framework completed by Thistle Initiatives
3. The ABC Policy has been updated to include reporting guidance, clarification of amounts and line manager or GE approval limits.

Input Sought

The R&CC is asked to approve the updated ABC Policy.

The Report

Why do we need to review this Policy?

4. The Policy was last reviewed and approved by the R&CC in July 2016. The terms of the Policy require it be reviewed annually.

What changes to the Policy do we propose and why?

What are the key features that we propose and why?

5. We have redesigned the Policy template and format but the substance and obligations have not changed materially. The new format helps ensure that the purpose, core principles and impacts are understood. It sets out clear minimum control standards and responsibilities for application of those standards.
6. The Policy has been updated to reflect the recommendations made by the external Risk Assessment completed by Thistle Initiatives. The key recommendations include:
   - Governance and oversight should be clarified and ownership evidenced through the half yearly executive declarations in respect of their business areas.
   - The Policy document needs to be updated to consider the new Policy implementer, the requirement on staff before engaging with any member of government, the businesses stance on sponsorships and grants and a clear definition of a facilitation payment.
   - A simplified ABC Policy should be published on Post Office public website (See Appendix A)
   - The ABC Policy reflect the roles and responsibilities of first, second and third lines of defence.
   - Implementation of enhanced monitoring procedures to ensure quantifiable data to be analysed in relation to Gifts and Hospitality.
7. The Gifts and Hospitality Tool has been developed to make it easier for employees to accurately record the offering and acceptance of gifts and hospitality throughout the Group. The introduction of this tool will be communicated to relevant stakeholders and monitored on a business as usual basis by the Financial Crime Team.
8. The thresholds have been amended owing to a large number of hospitality being recorded at above the agreed thresholds without corresponding Line Manager/GE approval.
9. We have updated the Policy framework to provide greater clarity to include minimum reporting requirements and timescales. The framework also covers minor changes to the requirements in relation to reporting.

How did we develop these recommendations?

10. The Policy has been developed following the Risk Assessment undertaken by Thistle Initiatives during 2016/17.
11. Policy queries and issues that have arisen over the previous 12 months have been reviewed to ensure that these concerns are addressed. The definitions have been updated to clarify queries and issues raised by key stakeholders.

What are the implications of these changes?

What will we need to do and by when, to implement and embed these Policy changes?

12.No material changes are required to comply with this updated Policy.

13.All employees need to ensure that they accurately report all instances of gifts and hospitality using the new tool.

14.Internal communications and training – once the Policy has been approved, there will be a One communication to advise all employees of the changes and provide a link to the updated document and the Gifts and Hospitality Tool on the Post Office Intranet.

15.The Financial Crime Team will monitor adherence to the minimum control standards set out in the Policy on an on-going basis through their review of the Gifts and Hospitality Tool and any other reported issues. Any control gaps identified will be reported to the R&CC as required.

16.The Financial Crime Team will provide quarterly reports to Group Executive members.

17.Every six months, as part of the Group Executive declaration the members will be required to confirm that the Policy has been correctly applied in their business area.

What will the impact be on our wider business?

18. Increased transparency of the ABC framework to include minimum control standards and control responsibility.

19.Design of Compliance oversight monitoring to test the Groups controls and confirm effectiveness and adherence to ABC Policy, is not yet finalised. Work is planned by the Financial Crime Team over the next 12 months to address this.

20.Public transparency of Post Office's adherence and commitment to ABC will be demonstrated through the publication of a simplified ABC Policy on the Post Office website (see Appendix A).

21.Increased oversight of all Gifts and Hospitality being offered and received throughout the group.

22.All business units are required to ensure that they report gifts and hospitality and ensure that reporting and acceptance of Gifts and Hospitality complies with the Policy.

23.Clarification that the failure to comply with the requirements of ABC Policy by any employee will be regarded as a significant breach impacting on the Post Office's risk and control management environment and may lead to disciplinary action up to and including dismissal and possible prosecution.

What would the impact be of delaying approval?

24.Risk that the group breaches the Bribery Act 2010 by not having up to date policies and procedures to prevent bribery by any person or company who operates on our behalf.

25.Post Office Limited is required to maintain up to date policies to support contractual requirements with clients and suppliers (e.g. MoneyGram and the Partner Banking Framework) and failure to do so may result in a breach of contract, and whilst not material, could have commercial and reputational impacts.

26. Post Office Limited provides Post Office Management Services (POMS) with its policies suite in the form of “Group Policies”. POMS is required under its regulatory responsibility to the Financial Conduct Authority to have up to date policies and failure to do so may lead to regulatory sanctions or penalties.

Appendix A

Simplified ABC Policy for publication on the Post Office website

Post Office (Post Office Limited and Post Office Management Services Limited) are committed to high standards of ethical behaviour and have zero tolerance towards bribery and corruption. Post Office requires compliance with all anti-bribery and corruption laws in all markets and jurisdictions in which it operates. These laws include the UK Bribery Act 2010 and the Criminal Finances Act 2017.

Post Office's Anti-Bribery and Corruption (ABC) compliance programme and policies are overseen by the Board. Policies incorporate the results of regular risk assessments and emphasise that all employees, including the Board of Directors and Associated Persons, must comply with the principles in these policies in the performance of their services for or on behalf of Post Office. We also expect that outsourcers and other companies providing services to Post Office will adhere to equivalent standards.

At Post Office, we aspire to be at the very heart of customers' choice by becoming the most trusted provider of essential services to every person in the land. It recognises that over and above the commission of any crime, any involvement in bribery will also reflect adversely on its image and reputation. Post Office therefore aims to limit its exposure to bribery by:

- Setting out a clear Anti Bribery & Corruption Policy;
- Training employees so that they can recognise and avoid the use of bribery by themselves and others;
- Encouraging its employees to be vigilant and to report any suspicion of bribery, providing them with suitable channels of communication and ensuring sensitive information is treated appropriately;
- Rigorously investigating instances of alleged bribery and assisting the police and other appropriate authorities in any resultant prosecution;
- Taking firm and vigorous action against any individual(s) involved in bribery.

Based on the above, the ABC Programme imposes the following requirements:

- All individuals are required by policy to ensure that appropriate due diligence and controls are applied, to any individuals they engage with, to ensure that they comply with the letter and spirit of applicable anti-bribery legislation and regulation; and
- Gifts, Hospitality and Charitable giving: All individuals are required by policy to avoid offering, accepting or permitting any gift, entertainment, charitable giving, sponsorship or other advantage to be offered or accepted without the appropriate controls being applied.

As part of the prevention, identification and remediation of ABC issues, mandatory training is conducted throughout Post Office and the Financial Crime team carries out regular, risk based assessments, monitoring and testing of its AB&C programme.

Post Office also maintains a clear Whistleblowing Policy and processes to ensure that individuals can confidentially, with no fear of retribution, report concerns to be investigated and remediated appropriately.

GROUP POLICIES

Anti-Bribery and Corruption Policy

Version – V1.2

Chief Executive's Endorsement
The Post Office Group is committed to doing things correctly. Our Values and Behaviours represent the conduct we expect. This Policy supports these to help us ensure the highest standards of financial crime prevention, detection and management are maintained.

1. Overview

1.1. Introduction by the Policy Owner

The General Counsel has overall accountability to the Board of Directors for the design and implementation of controls to prevent or deter Bribery and Corruption. Anti-Bribery and Corruption is an agenda items 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 our Bribery and Corruption risks throughout the Group[1]. 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 across the Group. Compliance with these policies supports the Group in meeting its business objectives and to balance the needs of shareholders, employees[2] and other stakeholders.

1.3. Core Principles

To offer a bribe is a criminal offence; bribery is an offer, promise, payment, request, or agreement to receive anything of value from any person or entity in order to induce that person to perform their roles improperly.

In order to prevent Bribery and Corruption the governance arrangements described in this Policy are based upon the following core principles:

- The Group is committed to and oversees the implementation of a Policy of zero tolerance, recognising that bribery is contrary to fundamental values of integrity, transparency and accountability and undermines the Group's effectiveness;
- Post Office has devised a robust Policy and associated procedures (set out in this document) which are proportionate to the risks and complexity of the Group;
- A bribery risk assessment is an integral part of our Group's overall and ongoing risk management process;
- Post Office must assess the risk associated with entering into joint ventures, partnerships or contracting arrangements with other entities and must carry out periodic due diligence based on that risk assessment. This includes ensuring that these organisations have policies and procedures which are equivalent to the Group's own procedures;
- The Group undertakes a training and awareness program to ensure employees are aware of the potential risks, how bribery might affect them, what they should do if they are offered a bribe, and the consequences should they be found to have made or received a bribe;
- The interests of Policyholders and other stakeholders are protected by ensuring that excessive powers are not delegated to individuals;

[1] In this Policy "Post Office" and "Group" mean Post Office Limited and Post Office Management Services Limited.

[2] In this Policy "employee" means permanent staff, temporary including agency staff, contractors consultants and anyone else working for or on behalf of Post Office.

- Decisions taken by management are consistent with the Group's strategic objectives and risk appetite, which are approved by the Board;
- Appropriate conduct is demonstrated in executing the requirements contained within the Policy;
- Every member of staff is responsible for understanding and managing the risk they take on behalf of the Group and for ensuring that they act within accordance to them;
- All employees are required to comply with Group Policies.

1.4. 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.

In exceptional circumstances, where risk sits outside of the Group's accepted Risk Appetite a Risk Exception can be granted. For further information in relation to the risk exception process please see the Risk Exception process found here.

While Post Office does not tolerate events that are criminal in nature and which may give rise to unacceptable and illegal behaviour, it recognises that despite its many endeavours, it is not possible to eliminate all risks of internal and external Bribery and Corruption. As a result Post Office may incur losses, and therefore takes a risk based approach to Bribery and Corruption.

For definitions please see section 3.1.

The risk to the Group in relation to Bribery and Corruption is reviewed by the board on a regular basis.

1.5. Types of Bribery and Corruption Risk

Post Office is exposed to a number of the above risks relating to Bribery or Corruption. These risks include, but are not limited to, the following:

1. **Payment Risks** –for example, facilitation payments, gifts & hospitality, client training programmes, charitable or political donations, ex-gratia payments/ legal settlements. This would also include the offer of sponsorships or grants.
2. **Third Party/Associated Party Risks** –third parties who provide services on behalf of the Post Office Group engaging in bribery or corruption while performing such services. The scope of this could include agency operators within the Post Office network and suppliers procured through the business or through the Procurement Team. Examples of Associated Parties include agents, consultants, suppliers, introducers, and intermediaries.

3. **Employment Risks** –Post Office employees requesting or receiving something of value from a third party in exchange for providing employment or work opportunities at the Post Office or offering or providing work opportunities, paid or unpaid, to Connected Individuals[3], or otherwise using employee connections to improperly obtain business or secure an advantage for Post Office. Employment opportunities (including work experience, secondments, etc.) have a value to the recipient and/or their close family members and may be considered to be bribes if used to improperly obtain or retain business or secure an advantage for Post Office.

4. **Inducement Risks -** Post Office must take reasonable steps to ensure that it, and any person acting on its behalf, does not:
   - Offer, give, solicit or accept an inducement; or
   - Direct or refer any actual or potential business in relation to another person on its own initiative or on the instructions of an associate; if it is likely to conflict to a material extent with any duty that Post Office Management Services owes to its customers in connection with an insurance mediation activity or any duty which such a recipient firm owes to its customers in connection with an insurance mediation activity.

5. **Gifts & Hospitality** –The Group has a process for reporting Gifts & Hospitality (both received and offered) details of this can be found here.

1.6. Legislation

The Group seeks to comply with all relevant UK legal and regulatory requirements including (but not limited to):

- The Bribery Act 2010
- The Criminal Finances Act 2017
- Financial Conduct Authority (FCA) Rules and Guidance (to the extent that these apply – see 1.8 below)

Under the Bribery Act, it is an offence to:

- Directly, or indirectly offer, promise or give a financial or other advantage with the intention of inducing any person to perform a business activity improperly or to reward any person for doing so;
- Request, agree to receive or accept a bribe, i.e. to receive a financial or other advantage with the intention of performing a business activity improperly;
- Bribe a foreign public official;
- Fail to prevent bribery by any person who perform services for or on behalf of a company ("corporate offence").

Post Office is subject to the Bribery Act 2010 (Bribery Act) and could become criminally liable as a result of an act of bribery or corruption by its employees or a third party operating on our behalf.

The Bribery Act has extra-territorial effect which means that the actions of Post Office or a third party operating on our behalf outside of the UK may fall within the scope of the Act. In the context of Post Office, this could apply in scenarios such as where a Post Office contractor or supplier resides outside the UK.

[3] Connected Individuals means those individuals who are known to have close connections to existing or prospective clients or suppliers, Public Officials, Politically Exposed Persons (PEP) or using employees' connections to improperly obtain business or secure an advantage for Post Office.

The Criminal Finances Act also includes a 'failure to prevent' (strict liability) offence on the Group, where failure to prevent criminal facilitation of a tax evasion offence, by a taxpayer, takes place and there are no reasonable procedures put in place to prevent such facilitation, or it cannot show that these procedures would have been unreasonable.

Post Office can be held liable unless it can demonstrate that it has in place "adequate procedures" designed to prevent this type of misconduct. The controls outlined in this Policy, including appendices, assist Post Office in preventing and detecting corrupt conduct and form an essential component of Post Office's adequate procedures.

1.7. FCA Rules

Post Office Limited is an Appointed Representative of the Bank of Ireland and P ost Office Management Services Limited (POMS) and is contractually required to comply with certain regulatory requirements. As such the Group as a whole is obliged to ensure there are adequate systems and controls are in place to mitigate Financial Crime risks.

POMS is a directly regulated firm with the FCA is directly exposed to regulatory fines and censure if the FCA determine that the systems and controls associated with this Policy are not effectively implemented.

This Policy contributes to Post Office's compliance with these regulatory and contractual obligations.

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

Risk Appetite is the extent to which the Group will accept that a risk might happen in pursuit of day to day businesses 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 [4]:

- **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 ligation in relation to Financial Services matters
- **Averse risk appetite** for not complying with law and regulations or deviation from business' conduct standards for financial crime to occur within any part of the organisation
- **Averse Risk Appetite** in relation to unethical behaviour by our staff.

The Group acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sit outside the agreed Risk Appetite. In this situation, a risk exception waiver will be required [5].

2.2. Policy Framework

Post Office has established a suite of financial crime policies and procedures, on a risk sensitive approach which are subject to an annual review. The Policy suite is designed to combat money laundering, terrorist financing, bribery and corruption and adh ere to relevant Sanctions regimes. These have been developed to comply with applicable legislation and regulation and covers the following specifically:

- The identification of potential financial crime risks
- On a risk sensitive approach, performing due d iligence at on-boarding, periodic basis and payment on third parties who perform services for or on behalf of us.
- Maintaining appropriate records for at least the minimum UK prescribed periods.
- Completing compliance oversight monitoring to test the Group's controls and confirming effectiveness and adherence to financial crime policies.
- Establishing and maintaining Standards for Management Information on Financial Crime. This includes, but is not limited to, record keeping, reporting of suspicious activity and details of staff training.

The Anti-Bribery and Corruption Policy is a key Policy under the Financial Crime Policy framework and should be considered and read in conjunction with the overarching Financial Crime Policy where relevant.

[4] The Risk appetite was agreed by the Groups Board January 2015
[5] For more information in relation to Risk Exception waivers found here

2.3. Who Must Comply?

Compliance with this Policy is mandatory for all Post Office employees and applies wherever in the world 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.

All Post Office employees are required to report any knowledge or suspicions in relation to Bribery or Corruption to Grapevine. As such all business units are required to have a process in place for reporting Bribery or Corruption incidents to Grapevine by telephone on 0845 603 4003. For more information in relation to reporting knowledge or suspicions please see section 3.2.

The next page sets out the minimum control standards that the Group has implemented to control these risks.

2.4. Gifts and Hospitality Tool

The purpose of the Gifts and Hospitality Tool is to make it easy for our employees to accurately record the offering and acceptance of gifts and hospitality throughout the Group. For more information in relation to the tool and how to use this, please see the below links:

The Gifts and Hospitality Tool can be found here.

Instructions upon how to complete the tool can be found here.

The procedure for completing the Gifts and Hospitality Tool can be found here

2.5. 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 defin ed Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum con trol standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensu re 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:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Appointment and Activities of Consultants and Contractors	Failure to ensure that Consultants and Contractors comply with the Group's anti-bribery and corruption policy may lead to criminal prosecution and damage to the Post Office brand or reputation.	Preventative Control: Our contracts require Consultants and Contractors to comply with the Group's anti-bribery and corruption policy. A clause is included within Consultants and Contractors contracts requiring them to comply with the Group's anti-bribery and corruption policy.	Procurement	Ongoing where required
Charity Donations	Insufficient controls may lead to the donation of money to an unregistered charity, which could be interpreted as bribery and result in reputational damage.	Preventative Control: Where the Group, a team or an individual has selected a particular charity to support, they are required to validate that charity against the Charity Commissions website. More information can be found here.	All employees	Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		Where a supplier or third party requests that Post Office makes a charitable donation, Post Office ensures that the donation is not linked to any business or services provided to or by that supplier or third party.	All employees	Ongoing
Conflicts of Interest	The acceptance of hospitality or gifts from third parties could lead to bias or undue influence, or the perception of such, in how individuals exercise their duties and responsibilities.	Preventative Control: The Group operates a procedure to ensure Gifts and Hospitality may not be offered or accepted where they could bias or influence how individuals exercise their duties and responsibilities. All employees are made aware of and are expected to comply with the gifts and hospitality procedures.	All employees	Ongoing
Employment Risks	Failure to identify employees requesting or receiving something of value from a third party in exchange for providing employment or work opportunities may result in the loss of Group stakeholder support.	Preventative Control: Any form of employment or work opportunities (paid or unpaid) must be reviewed and approved prior to employment.	All employees	Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Gifts	Inadequate controls may lead to employees accepting gifts that are not appropriate, proportionate or within policy resulting in reputational damage or criminal prosecution.	Preventative Control: All employees must report correctly any gifts or hospitality which they receive or offer using the Gifts & Hospitality tool. No employee may accept cash (or cash equivalent) gifts. Corrective Control: Where an issue is identified, the reason for this is reviewed and action is taken. Action includes disciplinary and dismissal.	Each employee is responsible for ensuring that all gifts offered or received are recorded. Line manager for approving or declining the acceptance of a gift Group Executive is responsible for approving or declining any offers over £100 Financial Crime Team is responsible for reviewing the Gifts and Hospitality register. Human Resources is responsible for reviewing any incidents where further action is required	Ongoing Ongoing Ongoing Ongoing Ongoing
Hospitality	Inadequate controls may lead to employees accepting hospitality that is not appropriate, proportionate or within policy resulting in reputational damage or criminal prosecution.	Preventative Control: All employees must report correctly any gifts or hospitality which they receive or offer using the Gifts & Hospitality tool. Before accepting or giving hospitality an employee must receive written approval from their line manager.	Each employee is responsible for ensuring that all hospitality offered/received are recorded Line manager for approving or declining the acceptance of hospitality	Ongoing Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		The hospitality must be reasonable (not lavish or extravagant), proportionate to its purpose and must ordinarily be below £200 per person in value.	Group Executive is responsible for the approving or declining of any offers of hospitality over £200	Ongoing
			Financial Crime Team is responsible for reviewing the Gifts and Hospitality register	Ongoing
			Human Resources is responsible for reviewing any incidents where further action is required	Ongoing
Payment Risks	Offering facilitation payments, gifts & entertainment, client training programmes, charitable or political donations, ex-gratia payments or legal settlements that are not justifiable or proportionate may result in reputational damage or criminal prosecution.	Preventative Control: All employees are required to comply with the conflicts of interest policy which can be found here.	Each employee is responsible for ensuring that all hospitality and gifts offered or received are recorded	Ongoing
		All employees are required to comply with the Gifts and Hospitality procedure which can be found here.	Line manager for approving or declining the acceptance of a gift or hospitality.	Ongoing
		The acceptance of discounted or complimentary training courses which would usually incur a cost are classified as Gifts and Hospitality and employees are required to report these using the Gifts & Hospitality Tool.	Group Executive is responsible for the approving or declining of any offers of gifts or hospitality over the agreed amounts	Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		The payment of ex-gratia payments or legal settlements are strictly controlled and must be submitted to the Group Legal Director for approval.	Financial Crime Team is responsible for reviewing the Gifts and Hospitality register Group Legal Director is responsible for reviewing and signing off as required any ex-gratia payments or legal settlements as requested from the Business.	Ongoing Ongoing
Political Donations/Lobbying	Employees making or soliciting political donations on behalf of Post Office may result in criminal prosecution.	Preventative Control: Before giving or offering Hospitality to or from a political party, approval must be obtained from a GE Member. The giving of political donations or gifts on behalf of the group to a Politician or a Political Party are strictly prohibited.	Each employee is responsible for ensuring that all Gifts & Hospitality offered or received is recorded Group Executive is responsible for the approving or declining of any offers of hospitality by a political party Financial Crime Team is responsible for reviewing the Gifts and Hospitality register	Ongoing Ongoing Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Procurement/Third Party Risk	Inadequate monitoring may lead to third parties engaging in bribery or corruption while performing services on behalf of the Post Office Group. This could result in criminal prosecution, loss of key contracts or reputational damage.	Preventative Control: Post Office ensures that any fees paid are proportional to the services being rendered or consistent with the market. New and existing contracts are reviewed on an ongoing basis to ensure that there is no risk of conflicts of interest. This includes ensuring that all parties involved are aware of Procurement Lockdowns.	Chief Financial Officer Procurement	Ongoing Ongoing

The Group completes Annual Risk Assessments reviewing its bribery and corruption exposure and its compliance with the above key risk areas.

3. Definitions

3.1. Definitions

Bribery
Bribery is defined as the offer, promise, payment, request, agreement to receive anything of value whether directly or indirectly to or from any person or entity in order to induce that person or entity to perform their roles improperly or, in the case of a Public Official, in order to influence them with the intention of obtaining or retaining business or an advantage in the conduct of business.

Examples include an offer or promise to give anything of value to anyone to obtain or retain business for or on behalf of the Post Office or to obtain or fulfil a legal or regulatory requirement in furtherance of the Group's business. A bribe can take the form of a "reward" and be paid after the improper performance of the relevant duty or obligation.

Corruption
Corruption is defined as the misuse of entrusted power or public office for private gain.

Educational courses/conferences
Events that are offered by third parties without charge do not amount to hospitality. However, free places to attend courses or conferences that would otherwise attract a charge are covered by this procedure.

Facilitation Payment
A Facilitation Payment is a type of bribe and should be seen as such. A common example is where a government official is given money or goods to perform (or speed up the performance of) an existing duty. Within the UK these are strictly prohibited.

Gifts
Gifts refers to a physical gift and includes the offer to a specific individual or team with the exception of low value promotional items costing under £20 each, such as pens, calendars, diaries, notepads and paperweights.

Hospitality
Invitations to attend events which have a social element (whether or not th ey are at the same time as or linked to a business meeting) and where the cost of a 'ticket' (participation) is free of charge or reduced in price when otherwise there would be cost attached to it. This would include things such as tickets to a sporting ev ent, tickets to a concert or a corporate dinner.

Inducement
An inducement is a benefit offered to a firm or any person acting on its behalf, with a view to that firm, or that person, adopting a particular course of action. This can include, but is not limited to, cash, cash equivalents, commission, goods, hospitality or training programmes.

Third Party funded trips
Travel/accommodation that is funded by third parties is covered by this procedure as a form of 'hospitality'.

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 suspects that there is a breach in this Policy should report this without any undue delay.

In case of bribery or corruption concerns or whistleblowing, staff may contact:

- their line manager,
- a senior member of the HR Team, or
- if either or both are not available, staff can contact the Post Office's General Counsel, who can be contacted by email at: whistleblowing@postoffice.co.uk or by telephone on: 07900 216851.
- Alternatively staff can use the Speak Up service available on 0800 0484531
- 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 bribery or corruption 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 the Policy sponsor or Policy owner.

5. Governance

5.1. Governance Responsibilities

The Policy sponsor, responsible for overseeing this Policy is the General Counsel of Post Office Limited.

The Policy owner is the Director of Risk and Compliance who is responsible for ensuring that the Financial Crime Team conducts an annual review of this Policy and tests compliance across the Group. Additionally the Director of Risk and Compliance and the Financial Crime Team are responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee.

The Audit and Risk Committee are responsible for approving the Policy and overseeing compliance.

The Board is responsible for setting the Group's risk appetite.

6. Control

6.1. Policy Version

Date	Version	Updated by	Change Details
November 2016	1	Georgina Blair	Roll out of Final version
June 2017	1.2	Thomas Richmond	Updated in line with comments from stakeholders

6.2. Policy Approval

Group Oversight Committee: Risk and Compliance Committee and Audit and Risk Committee

Committee	Date Approved
POL RCC	
POMS RCC	
POL ARC	
POMS ARC	

Policy Sponsor: Group Director of Legal, Risk & Governance

Policy Owner: Director of Risk and Compliance

Policy Author: Head of Financial Crime

Next review: July 2018

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.

6.4 Protection Personal Data Policy

Author: Chris Russell Sponsor: Jane MacLeod Meeting Date: 20th July 2017

Executive Summary

Context

This paper sets out the introduction of the Protecting Personal Data Policy for the Risk and Compliance Committee to consider and approve.

Questions addressed in this paper

- What is the need for a Protecting Personal Data Policy and why now?
- What are the implications of these changes?

Conclusion

1. The Protecting Personal Data Policy has been created to bestride our obligations under the current Data Protection Act 1998, and the General Data Protection Regulation (GDPR) which will come into force in May 2018.
2. The Policy introduces the mandate needed to meet the Group's legal requirements.
3. The Policy sets out minimum standards of controls which will be communicated to relevant stakeholders, and monitored on a business as usual basis by the Data Protection Function.

Input Sought

The R&CC is asked to approve the Protection Personal Data Policy.

The Report

Why do we need to review this policy?

4. This is a new business Policy and the terms of the policy require it be reviewed by the R&CC.

What is the need for a Protecting Personal Data Policy?

5. The policy has been created to ensure the Group meets its obligations under Data Protection Laws.
6. The regulatory landscape is changing, in May 2018 the GDPR comes into force and will put further obligations on the Group. The Policy has been designed in a manner to ensure compliance with current regulation, but to begin to embed our obligations under the GDPR, and meet the deliverables of the GDPR Programme.

How did we develop these recommendations?

7. The policy has been developed by reviewing current legislation (Data Protection Act 1998) against the incoming legislation changes General Data Protection Regulation).

What will be the impact of the Policy and will there be a need to implement further business processes to meet the Policy requirements?

8. A number of Standard Operating Procedures, as mandated by the Policy, will be created in order document operating procedures to allow the exercise of individual rights.
9. Membership of the Data Breach Emergency Response Team, as mandated by the Policy, will need to be scoped.
10. Data Retention Schedules will need to be reviewed and updated.

How will the Policy be communicated and implemented?

11. Internal communications and training – once the policy has been approved, the GDPR programme Steerco will be engaged, and a multi-channel communication plan developed, in order to meet the programme deliverables against education, awareness and accountability.
12. The revised Data Protection Impact Assessment Tool, is being embedded into the business with the Gating Community, and further by introduction into the Information Security and Data Protection Corporate Training, and multi-channel communications piece.
13. The Data Protection Function will monitor adherence to the minimum control standards set out in the policy on an on-going basis through their review of risk assessments, project business readiness and incidents. Any control gaps identified will be reported to the R&CC as required.

GROUP POLICIES

Protecting Personal Data Policy

Version – V1.1

Chief Executive's Endorsement

Post Office is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

POST OFFICE®

1. Overview

1.1. Introduction by the Policy Owner

The General Counsel has overall accountability to the Board of Directors for in ensuring that the requirements of this Policy are maintained, for introducing any change programs that may be required as a result of this Policy and ensuring ongoing compliance programs are managed appropriately.

1.2. Purpose

Trust is at the heart of the Post Office brand and protecting the Personal Data we use is fundamental to maintaining that reputation. Data Protection legislation protects the fundamental rights and freedoms of individuals, in relation to the use of their Personal Data.

As such, this Policy sets out the expected behavior of Post Office Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of Personal Data.

1.3. Core Principles

Post Office has adopted the following principles to gover n its collection, use, retention, transfer, disclosure and destruction of Personal Data:

1. Lawfulness, Fairness and Transparency

Post Office must Process Personal Data lawfully, fairly and in a transparent manner.

- Post Office must tell the Data Subject what Processing will occur (transparency),
- Processing must match the description given to the Data Subject (fairness), and
- Processing must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

2. Purpose Limitation

This means Post Office must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

3. Data Minimisation

The Personal Data Post Office collects must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are Processed.

This means Post Office must not collect or store any Personal Data beyond what is strictly required.

3. Accuracy

The Personal Data Post Office collects must be accurate and, kept up to date.

This means Post Office must ensure that processes for identifying and addressing out -of-date, incorrect and redundant Personal Data are introduced and maintained. This will ultimately have a business benefit to the business by removing contacts that are no longer using Post Office products or services.

4 Storage Limitation

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed.

This means Post Office must, wherever possible, introduce mechanisms and procedures into their systems and processes that limits or prevents identification of the Data Subject (eg Anonymisation).

5 Integrity & Confidentiality

Post Office must Process Personal Data in a manner that ensures appropriate security of the Personal Data, including:

- Protection against unauthorised or unlawful Processing,
- Protection against accidental loss, destruction or damage.

We must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

6 Accountability

Post Office must demonstrate these Data Protection Principles are met for all Personal Data for which it is responsible.

It shall be the responsibility of the GE to ensure that all processes for which they are responsible, are conducted in a manner which can be be subject to either internal audit or external regulatory scrutiny, and can demonstrate their compliance with this Policy, its corresponding Standards and Procedures and Legal Requirements.

1.4. Application

This Policy is applicable to all areas within the Group and defines the minimum standards to control the risks associated with non-compliance of Data Protection regulations.

All Third Parties engaged to process Personal Data on behalf of Post Office (Data Processors) must be aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, prior to granting them access to Personal Data controlled by Post Office.

The risk to the Group in relation to breaches of Data Proteciom regulations are reviewed by the board on a regular basis.

Any non-compliance may expose Post Office to complaints, regulatory action, fines and/or reputational damage. Therefore any breach of this policy will be taken seriously and may result in disciplinary action or business sanctions being applied.

1.5. Data Protection Risk

Failure to appropriately manage risks and incidents relating to Data Protection could result in punitive penalties, regulatory breaches, fines, prosecution, and prevention from processing personal data and damage to reputation.

The GE must ensure that all Data Protection risks are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes.

A Data Protection Impact Assessment (DPIA) must be conducted, in cooperation with the Data Protection Function for all new, and/or revised systems or processes.

Where applicable, Information Protection and Assurance (IPA) and IT Security, will cooperate with the Data Protection Function to assess the impact of any new technology uses on the security of Personal Data.

1.6. Legislation

The Group seeks to comply with all relevant UK legal and regulatory requirements including (but not limited to):

- Data Protection Act 1998
- Privacy & Electronic Communications Regulations 2003
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998

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 businesses 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 responsivities 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
- **Adverse risk** appetite for litigation in relation to high profile cases/issues
- **Adverse risk** appetite for not complying with law and regulations or deviation from business conduct standards
- **Adverse risk** appetite for data loss/leakage that can lead to customer, commercial or reputational damage
- **Adverse risk** appetite for inaccurate and unreliable processing of data

The Group acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sit outside the agreed Risk Appetite. In this situation, a risk exception waiver will be required.

2.2. Policy Framework

Post Office has established a suite of Data Protection policies and standard operating procedures (SoPs), which are subject to annual review. The policy suite is designed to set out how the business aims to comply with Data Protection regulations.

The SoPs mandated by this Policy covers the following:

- The identification through documented risk assessment of potential or inherent Data Protection risks and mitigating actions (Data Privacy Impact Assessments)
- Documentation of operating procedures to allow the exercise of individual rights, including:
  - Information access.
  - Objection to Processing.
  - Objection to automated decision-making and profiling.
  - Restriction of Processing.
  - Data portability.
  - Data rectification.
  - Data erasure.
- On a risk sensitive basis, performing due diligence upon our employees, agents and third parties,
- Data Breach escalation and management plans

2.3. Who must comply?

Compliance with this policy is mandatory for all Post Office employees and applies wherever in the world the Group's business is undertaken. All third parties who do business with the Group, including consultants, suppliers and business will be required to agree contractually to this policy or have their own equivalent policy.

Where non-compliance is identified the matter must be referred to the Policy Owner and the Data Protection Function. Where is it identified that an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary o ffence.

2.4. Minimum Control Standards

A minimum control standard 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 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, the considered Risk Appetite, and the required minimum control standards. The subsequent page defines in greater detail terms used:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Proposed Product or service	A new system uses Personal Data, however potential privacy risks have not been considered in the design, which results in a Personal Data Breach, accompanied by punitive penalties, reputational damage and a loss of licence to process personal data.	Preventive Control: 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 using the DPIA before completion of the design phase. • Prior to launch the DPIA must be reviewed and approved by the Data Protection Function.	Product Manager Data Protection Function	During design phase
Existing Products and services	Due to changes in regulation there is a risk that current controls will no longer be adequate to meet our Data Protection obligations	Preventative Control: Where a product or service has undergone a DPIA, it must be reviewed annually, or when there is a proposed change to the product or service affecting Personal Data. If it is found that no DPIA has been agreed, one must be undertaken, in an agreed timescale, with the Data Protection Function.	Product Manager Product Manager	Annually, or at any time there is a change Annually, or at any time there is a change

POL00401625

		Corrective Control: DPIAs must be carried out where an issue is highlighted or incident occurs.	Product Manager	When there is a material issue or incident
Employees	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.	Preventative Control: All staff must undertake annual Data Protection training. Employees who operate in areas with high exposure to Personal Data will, in addition to this, on a regular basis, receive bespoke training to reflect their on-going needs.	Data Protection Function All employees	Annually, and when a need is identified
Data Processing	Personal Data is Processed in a way that is incompatible with the reason it was collected, resulting in customer complaints due to unsolicited marketing, resulting in ICO investigations, enforcement action including, punitive penalties, loss of licence to Process Personal Data.	Preventative Control: Assessment of Processing activities through DPIAs. Governance of Processing activities through Processing registers Internal auditing and review of Processing activities and qualifying legitimate purposes for Processing; including marketing permissions.	Data Protection Function All business functions Data Protection Function	Ongoing Ongoing Ongoing
Breach Management	Due to malicious behaviour, customer or employee records are accessed resulting in punitive penalties, reputational damage and a loss of licence to process personal data	Preventative Control: The Group has an Information Security Policy which sets out the minimum technical security measures the Post Office employs to protect the Business against malicious behaviour. The Group has a breach management plan with an Emergency Response Team, to	Information Security Data Protection Function	Ongoing Ongoing

		investigate and manage the potential impacts from a Personal Data Breach To ensure that the board and senior managers are aware of issues and concerns a Weekly GE Incident Reporting process is in place.	Data Protection Function	
Third Parties	Failure to follow due process set out in contractual clauses, statements of work and operating procedures by the Third Parties may incur a data breach affecting PO customer data	Preventative Control: Third Parties must adhere to the processing arrangements as specified in the data processing contractual provisions. Processing Provisions and liability arrangements are in place to ensure Post Office has a remedy against Third Parties who are in breach of contract and Data Protection Laws. Contract Owners must ensure that there is appropriate oversight of Processing activities undertaken by the contracting third party.	Legal and Data Protection Function Legal and Data Protection	Ongoing Ongoing
Information Security	Inadequate access controls may lead to unauthorised access, deletion, loss, damage or unauthorised alteration of Personal Data.	Preventive Controls: Business areas must assess and assure risks relating to employee access to systems and files containing Personal Data.	All employees I.T.	Ongoing
Data Retention	Customer Data is retained when there is no longer a legitimate purpose for doing so, which may lead to customer complaints resulting	Preventative Control: The Group has a Data Retention Policy which sets out appropriate procedures for the	Data Protection Function	Ongoing

	in punitive penalties, reputational damage and a loss of licence to process personal data	retention and destruction of Personal Data. (Under review)		

3. Tools

3.1. Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) must be conducted, in cooperation with the Data Protection Function for all new, and/or revised systems or processes.
The DPIA Template can be found here (link)

.

4. Where to go for help

4.1. Additional Policies

This policy is one of a set of policies and standard operating procedures, which can be found:

insert link

4.2. How to raise a concern

Any Post Office employee who wishes to raise a concern can:

- Discuss the matter fully with their Line Manager; or,
- Email the Data Protection Function- data.protection@ GRO
- Report the matter directly to the Data Protection Officer.

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 data.protection@ GRO

5. Control

5.1. Policy Version

Date	Version	Updated by	Change Details
May 2017	1	Sophie Dalby	
July 2017	1.1	Sophie Dalby	Updated in line with comments from stakeholders

5.2. Policy Approval

Group Oversight Committee: Risk and Compliance Committee (RCC) and Audit and Risk Committee (ARC)

Committee	Date Approved
POL RCC	
POMS RCC	
POL ARC	
POMS ARC	

Policy Sponsor: Group Director of Legal, Risk & Governance

Policy Owner: Director of Risk and Compliance

Policy Author: Data Protection Officer & Senior Data Protection Manager

Next review: July 2018

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.

POST OFFICE
RISK & COMPLIANCE COMMITTEE

DECISION PAPER

Review of Code of Business Standards

Author: Martin Kirke Sponsor: Martin Kirke Meeting date: 20 July 17

Executive Summary

Context

At the RCC in March it was agreed that the above would be reviewed and updated to be issued alongside the EVP work "Our Post Office". The latter answers the question "Why is Post Office a great place to work? "and the former answers the question "What are the dos and the don'ts?" *

The RCC is asked to approve the revised version which follows.

Extensive input and review has been undertaken by many particularly in IT and LRG. Some of the changes requested have been at odds with each other. For example the need to have legally tight wording to help us win an employment tribunal versus the need for simplicity.

There was also a concern that for new recruits the wording was too negative or directive (theory X). However our experience, and HR professional research, suggests that candidates are positive about organisations which take compliance seriously and act on bad conduct. Awareness of the potential career damage of a toxic organisation name on your CV has increased in recent years.

Thanks to Kelly (Employment Policy and previously Comms) for most of the work.

Questions addressed in this report

1. Does the RCC approve it?
2. If so what happens next?
3. How do we know colleagues have read and understood it?

Conclusion

1. We recommend approval
2. The document will be sent to all colleagues who have been issued a Post Office E mail address. For those who have not it will be printed and sent to them. Commas direct to colleagues and through line managers will be issued including material to discuss in team meetings. It will be issued to all new recruits and explained in their induction.
3. We are developing E learning which will be mandatory and this will also enable us to measure understanding. The training will be launched in November rather than immediately after the launch. This will improve the validity of measurement.

.

Input Sought and Received

1. As above

The Report

What is the need or opportunity and why now?

1. Covered above

What do we propose to do and why?

1. Covered above

What options did we consider?

1. Covered above

What do we need to do next to progress?

1. Covered above

What resources are required? Will any further approvals be required?

1. No additional resources are required.

What would the impact be of delaying or rejecting the decision to progress?

1. Covered above

**There are different views on the correct use of apostrophes in this phrase and Comms can decide*

POL00401625

Working at Post Office
The dos and the don’ts

Contents (to be added once document complete)

POL00401625

Dear Colleagues,

Post Office is unique. A commercial business delivering an important social purpose. We believe in the importance of connecting communities and enhancing the powerful role they play in all our lives. We stay true to this commitment by meeting customer needs through carefully designed, high quality products, and maintaining an unrivalled local presence across the UK.

Generations of hard work and honest achievement have made Post Office a name that elicits trust. This is due in no small part to an unwavering commitment to ethical behaviour and doing the right things in the right way. This commitment and integrity is critical to achieving great business performance.

I expect everyone at Post Office to read this document carefully and thoroughly and to think about how it applies to their work. Consider how your behaviours, actions and decisions may affect others, including customers and colleagues. The way that we conduct business has never been more important.

Thank you for your trust in Post Office. And, most importantly, thank you for your commitment to ensure our customers and everyone we do business with continue placing their trust in us.

Paula

Paula Vennells

Introducing our Code of Business Standards- The Dos and the Don'ts

The Post Office has thrived at the heart of high streets and local communities across the UK for over 370 years. We're one of the country's most trusted brands and we take our commitment to providing essential services to customers across the UK very seriously. We're the UK's largest retail network and provide unrivalled access to banking and financial services, with more branches than all the UK's banks and building societies put together.

We are committed to doing business the right way. That means we act lawfully. It also means that how we conduct ourselves is more than just a matter of policy and law; it's a reflection of our core values: Care, Challenge and Commit. By aligning our behaviours to our core values, we help maintain the trust and support of our customers, shareholders, communities and others with whom we work.

All colleagues must read and ensure they understand the code. If in doubt ask your manager or HR.

Do help serve the community

Each Post Office plays a key role in the communities they serve and all colleagues are expected to get to know their local Post Office through visits. You may also be asked to help customers at Christmas in a branch. More information can be found (link)

Do support charities

The Post Office 'Your Charity' scheme encourages teams across our business to select and support worthy causes, with the opportunity for matched funding and a payroll giving scheme for colleagues. We also encourage teams to get directly involved with the charities over and above their fundraising efforts.

> Established in 1882, the Rowland Hill Fund is our very own in-house charity open to all Post Office colleagues, past and present. For more information (link)

Do promote our brand and demonstrate our behaviours

Our brand experience, for employees, customers and all we do business with, needs to be shaped by our core values of **Care, Challenge and Commit**.

We make that happen by having a set of straightforward business behaviours which inform the way we do things.

It's how we do things in this business so we deliver our brand consistently to customers.

We care by always thinking customer

Care is the cornerstone of our business. It means valuing people and their time; and putting our customers first. It means making it personal; listening and understanding; being guided by our conscience and expertise; and keeping our word. In short, it means doing right by people. This is what sets us apart and gives us our competitive edge.

We strive to make things ever better through honest challenge
Challenge conventions, challenge complexity, challenge competitors, challenge on behalf of our customers, challenge each other, challenge yourself. We've been passed the baton of this great institution. It's up to every one of us to drive it forward and create change for a successful future.

We commit to decisive delivery
We don't just work for the Post Office, we are the Post Office and we're all responsible for its commercial success. The road ahead is exciting, but not easy. If each and every one of us invests all our energy, creativity and passion we can achieve amazing things.

You can find out more about these behaviours and what they mean, in Our Post Office.

Behaviours: The don'ts

- Behaviour, which damages service to customers, or the reputation or efficiency of Post Office, is unacceptable. This includes poor attendance, lateness, dishonesty, drunkenness, use of illegal substances, bullying and harassment, violent or disorderly behaviour and abusive language
- Coming to work with an unclean or untidy appearance
- Bringing Post Office into disrepute
- Claiming money for hours you did not work, a journey you did not make or an expense you did not incur
- Discriminate on the grounds of
    - Race
    - Colour
    - Religion or Faith
    - Age
    - Sex, sexual orientation, gender, or gender identity expression
    - National origin, geographical or demographic background
    - Pregnancy or Maternity

We must continue to ask ourselves what we as individuals can do to uphold and strengthen the right behaviours. And, we must never victimise colleagues for 'calling it out' wrong behaviours.

Do deliver customer service excellence

Our customers are at the heart of everything we do.

We all know what good customer service is and there are hundreds of examples of us all delivering it every day.

Our challenge is to make sure we deliver great service for every customer, every time. The more we understand our customers and their expectations, and put ourselves in their shoes, the easier it will be to provide consistently great service.

How do we demonstrate our commitment to customer excellence?

- by listening to them first, and fully understanding their needs and expectations
- by communicating respectfully, leaving out the jargon, providing them with the best service and products that meets their expectations, to achieve their goals
- by always thinking about them and not the process
- by keeping it simple, straightforward and quick to reach us, in branch, online, on mobile

We do work to resolve grievances and disputes

- We have clear and robust policies and procedures for managing grievances, alleged breaches of discipline and resolving disputes. Visit the HR Advice and Guidance page on the intranet for more information.
  - We ensure that appropriate structures are in place to facilitate constructive dialogue for resolving individual and collective disputes with our unions
  - We have extensive collective consultation and negotiation arrangements with our unions

Do report violence, threats, bullying and harassment

Post Office operate a zero tolerance to any form of violence on any of its premises. An act of violence can take many forms, including:

- Verbal
- Written or physical threat
- Intimidation or abuse
- Physical assault

Sexual harassment incudes

- Sexually suggestive statements or actions
- Inappropriate or offensive comments, 'jokes' and nicknames

If you witness an act of violence, bullying or harassment at work, report it to your line manager right away. If the situation escalates and there is a threat to you, or your immediate safety or the safety of those around you, take action and contact a member of HR or call Grapevine on 0845 6034004.

It is in everyone's interest for individuals to raise a genuine concern they have about their treatment or the treatment of others at work. Concerns should ideally be raised with your manager first.

If the concern is about bullying and harassment, you can speak to your line manager or refer to the Bullying and Harassment policy or managers can contact My HR Help. There is also the HELP employee assistance programme, which you can find out more about here.

Do promote diversity and inclusion
We want our people to reflect the diversity of the communities in which we live and work, and the customers we serve.
We celebrate the diversity of our work force and the communities we serve by embracing diversity and inclusion and creating policies which actively promote working without fear of discrimination.

Everyone working for Post Office has a responsibility to:

- Promote a culture of inclusivity where differences are accepted, valued and celebrated
- Inform their line manager of any instances of apparent discrimination
- Comply with, and promote Post Office policy and procedures with regard to diversity and inclusion. You can view our Valuing Diversity Policy, here.

We actively support:

- Flexible working practices, which you can read more about here.
- Women in Leadership Programme to support and nurture female talent.
- Post Office Prism: a network of lesbian, gay, bisexual and transgender (LGBT) colleagues and their allies. The group supports and celebrates Post Office's LGBT community and provides advice and guidance to our business on inclusivity and diversity.
- Disability Confident Group: a network of Post Office colleagues with disabilities and colleagues who want to support them. The group provides, support, advice and helps the business to do the very best it can for employees with disabilities.

Modern Slavery

Modern slavery is a crime and a violation of fundamental human rights. It takes various forms, such as slavery, servitude, forced and compulsory labour and human trafficking, all of which have in common the deprivation of a person's liberty by another in order to exploit them for personal or commercial gain.

Post Office is committed to acting ethically and with integrity in all our business dealings and relationships and to implementing and enforcing the systems and controls set out in our Modern Slavery Statement with the aim of ensuring that modern slavery is not taking place anywhere in our own business or in any of our supply chains.

The prevention, detection and reporting of modern slavery in any part of our business or supply chains is the responsibility of all Post Office employees at all levels, as well as of its directors and officers. Our Modern Slavery statement can be found on our website, here.

If you witness any signs of modern slavery within our business or supply chains, you should raise your concerns via our Speak Up line on 0800 048 4531.

Do maintain a safe and healthy place of work

Do ensure that you are aware of all fire and emergency procedures. Do not ever use your mobile phone when driving even with a hands free kit.

- We comply fully with relevant legislation
- We ensure that the health and safety responsibilities of our employees, including managers, are clearly defined, allocated and understood
- We encourage and help all managers and employees to carry out their responsibilities through effective health and safety management systems, with safe premises, equipment and processes
- We improve our employees' capability to manage and work safely, through coaching and training
- We support and encourage our people and unions to get involved in the health and safety performance of our business
- We support and encourage our people and unions to get involved in pursuing a healthy and safe way of living and working
- We monitor and review how well we put our health and safety policies into practice

We are all responsible for health and safety. Every manager is accountable for the health and safety of their people. A full copy of the Health and Safety policy, and all associated policies, can be found on the Health and Safety intranet site.

Do make the most of our support for colleague's wellbeing

We seek to enable colleagues to achieve a positive balance between their work and their lives outside of work.

We take health and wellbeing seriously. That's why we work hard to promote a positive wellbeing culture and provide a range of services such as flexible working to help all our people stay mentally and physically healthy.

What we offer:

- Lifestyle online for colleagues and their families – to support our people to stay fit and healthy
- Monthly health and wellbeing campaigns, helping to raise awareness of what we offer and how our people can stay healthy
- Health checks – a rolling programme using kiosks and mobile kit
- **HELP** employee assistance programme for colleagues, partners and managers can provide advice and guidance on a variety of topics in full confidence.
- OH Assist Managers Portal provides advice and guidance for managing health and wellbeing
- Occupational Health Referral Portal for managers to request support for their teams during challenging times
- Training for colleagues to raise awareness on specific issues relating to health, and wellbeing

Use of Alcohol, Tobacco and Illegal Drugs

Drugs and alcohol can impair judgment and affect motor skills, placing our colleagues, customers and others at risk of harm. Tobacco may harm our own health and the health of those around us.

Possession or use of alcohol or illegal drugs while on Post Office premises or while conducting company business is prohibited. The exception is that during business dinners and events, or in designated areas, we may provide and drink alcohol in moderation, where permitted by law.

Vaping and electronic cigarettes are not allowed to be used in company premises

Do help protect the environment

Everyone has a part to play in reducing our environmental impact.

Post Office aims to comply with all relevant environmental legislation, and to promote initiatives that save on the resources we use. We recognise that our business activities and policies have an impact on the environment and we are committed to taking account of the environmental and ethical effects of our policies in our planning and operations.

In standards of design and cleanliness, we recognise our responsibility to ensure that our premises are a credit to the communities in which they are situated.

We aim to reduce our environmental impact through:

- Reduction in the use of water
- Efficient use of energy and a reduction in our CO_2 emissions
- Reduction in waste to landfill by recycling where possible
- The use of sustainable materials

Do protect our business and our brand by complying with IT security

The security of our information and IT systems is of paramount importance and essential to our success.

Many of our colleagues will have access to Post Office systems, information and devices such as laptops and mobile phones. It's really important that anyone who accesses them knows how to keep them secure by following the requirements in the 'Acceptable Use policy'. For example, these devices must not be left unattended in public areas, screens must always be locked when not in use and the use of privacy screens should be adopted to protect our information from being overseen by unauthorised people.

To help protect our systems and information, please:

- Classify information in line with our classification standard, as set out in our Information Security Handbook.
- Use complex passwords to protect your access, as set out in our Information Security Handbook.
- Only open emails when you know who they are from and don't click on unknown links or open unexpected attachments
- Don't use your Post Office email address and password for accessing 3rd party services such as LinkedIn. Use a different password.
- Only use approved data storage areas, such as onedrive. Don't sign up for cloud storage services such as Dropbox.
- Never click on links to go to a website where you expect to log on - always

go to the website directly.
- Don't store Post Office data directly onto your personal devices
- Don't become a victim: if you think an offer is too good, it probably is

If you become aware of **any** information security issue or incident you should always report it to the IT Helpdesk on 0330 123 0778 or email postofficeservicedesk GRO

We expect our colleagues, whether sending an email internally or externally, to use a Post Office email signature and to use their out-of-office when on annual leave. Similarly, personalised messages on voicemail should also be used.

As Post Office colleagues, we are allowed limited and reasonable personal use of company equipment in our own time. Payment is required for all personal telephone calls.

The following actions and or behaviours, is strictly prohibited:

- Accessing or forwarding documents or emails that allow computer viruses to infect our networks
- Using Post Office or personal equipment that interferes with customer service or productivity
- Downloading, installing or using unauthorised or banned software or modifying company provided hardware or software
- Accessing, storing, sending, posting or publishing gambling, pornographic, indecent, illegal, offensive, threatening or insulting material, or chain or "spam" emails
- Sending confidential information by email, instant messaging, or the Internet without adequate security
- Sharing of computer user IDs and passwords
- The use of mobile phones while driving

All modes of our communication are subject to the Freedom of Information Act.

Failure to comply with the Acceptable Use policy can carry profound consequences for Post Office and individuals. Breaches of the policy or the law may lead to disciplinary action up to and including dismissal.

Use social media but here are the do's and don'ts

Colleagues are free to use social and other digital media in their own time. Social media is a public forum and the boundaries between professional and personal can often become blurred – so it's important that we exercise particular care to ensure:

- Post Office brands or logos are not used or altered without prior permission
- Copyright and fair usage laws and restrictions are respected and observed
- Social media is not used to offend, harass or bully people
- We must not disclose official information relating to clients, partners or suppliers without the prior authority of the business.
    - Social media helps us work openly and connect with the communities we serve – just remember to apply common sense.
        - If in doubt, don't post it
        - Check the accuracy and sensitivity of what you are posting before

pressing 'send'

- Remember once something is posted online it's very difficult to remove it
- Ensure your privacy settings are correct and that you only share information with people you want to
- Never publically 'check-in' to locations you visit, especially when on holiday showing you are away from home
- Our Social Media team can be contacted by emailing social GRO

Don't talk to the media about Post Office unless our Press Office asks you to

Where a colleague is asked to make a comment about Post Office in a published form external to the business, such as a newspaper, magazine, journal, radio, television or a website, they must direct the request to our Press Office. They can be contacted on 0333 665 3076 or pressoffice GRO

Do remember the Post Office is politically neutral

Colleagues have the right to participate as an individual in political activities .

However, these activities are conducted as an individual and not as a representative of Post Office. The Post Office is a politically neutral organisation and our reputation must not be compromised by your interest, affiliation or activities to political party's pressure groups or other causes.

No matter what your own political beliefs are, you must not act or behave at work in a way that is determined by party political considerations, or use Post Office resources for party political purposes; or allow your personal political views to determine any advice you give or your actions.

Do watch out for conflicts of interest

We ensure that information received during our business dealings is not used inappropriately for corporate or personal gain or any other purpose except that for which it is given.

If you feel that you might have a potential conflict of interest, inform your line manager and seek their advice if you are unsure. Be open and frank about any outside activity or business you are involved in which may conflict with Post Office or your duties as an employee.

The essential principles are:

– You must not do anything which conflicts with your duty as an employee of the company, or use your official position for private advantage

– You must declare any outside employment, directorship or material shareholding and these must not be contrary to the company's commercial interest or bring it into disrepute

- Your actions as an employee must not be improperly influenced by any relationship (e.g. with relatives, friends, marriage, partners or membership of any social, religious or political association)
- or by any personal or financial consideration.
- no one should exploit their personal or family relationship with any colleague for any gain including to themselves or others
- If you receive a fee from an outside source for performing a service which forms part of your official duties or takes place in business time, e.g. giving an interview or lecture, you must report it to your manager. You will normally be expected to pay the money to Post Office or to a charity connected with it.
- If the service arises from your work but is not directly connected with it and is given in your own time, you must still report it to your manager

Do not accept gifts or sponsorship

You must not accept any gift, payment, bribe, favour or inducement that might influence (or seek to influence) your action as a Post Office employee. Equally, you must not offer any bribe or inducement to anyone else. If any such offer is made to you, you must report it to your manager.

In general, the giving and receiving of gifts is not permitted except for low value promotional items, such as pens, calendars, diaries, notepads and paperweights. You can find out more by reading the Anti-Bribery and Anti-Corruption policy.

You must not ask for or accept sporting or charitable sponsorship from an organisation that has (or is seeking) a contract to supply the company, or is in competition with it. You must declare to your manager any plan to accept sponsorship and ask if there is any conflict with company interests.

The Risk and Compliance team maintain a Register of all gifts given and received.

Hospitality and Entertainment

Hospitality may only be given and accepted where it has a clear and demonstrable link with a legitimate business purpose, e.g. an organised event or a meal at which business is to be discussed. In relation to offers of hospitality, numbers on both sides should be limited to those whose presence is necessary to progress the business in hand.

Maintaining our standards means the giving and receiving of hospitality and entertainment is subject to the following rules

- You must obtain prior permission from your line manager before accepting or giving hospitality
- The hospitality must be reasonable (not lavish or extravagant), proportionate to its purpose and must ordinarily be below £100 per person in value
- You must send details of all hospitality offered and accepted, along with written approval from your line manager, to the Risk and Compliance team at riskandcompliance GRO so they can maintain a Register of all Hospitality given and received.

You should be aware of the risk that accepting any hospitality and entertainment could compromise your performance of official business, or might reasonably appear to have improperly influenced a business decision.

Use sound judgement and exercise restraint. If you are still unsure about the standards required of you consult your manager or view the Anti-Bribery and Anti-Corruption policy.

Fraud and Financial Crime (Bribery, Money Laundering)

We seek to comply fully with relevant legislation.

We take protecting our customers and their information extremely seriously. We invest significantly in activities to detect, deter and prevent all aspects of financial crime. Through this, we aim to protect our customers, maintain value for our shareholder and assist society in combating crime by preventing criminals from benefiting from their activities and proceeds.

We promote high ethical standards and have a zero tolerance for circumvention of our fraud and financial crime policies. Our colleagues are required to demonstrate honesty and integrity in everything they do. We do not condone, under any circumstances, the offering or receiving of bribes or any other form of improper payments. Our colleagues are supported in doing this by mandatory training to develop their understanding of financial crime risks.

We operate systems and controls designed to ensure that our products and services are not abused for the purposes of laundering the proceeds of crime. We must also comply with requirements in respect of the management of Financial Crime. For more information (link).

Line managers have some more dos and don'ts

- Promote the Code of Business Standards and work related policies
- Set a fitting example though your own behaviour
- Promote diversity and inclusion at every opportunity
- Make certain your team members know they can come to you with questions or concerns and that you'll listen to them and respond to them appropriately
- Never make promises or make commitments beyond your authority e.g. on pay, promotions or job offers. If in doubt ask HR.
- Maintain up to date job descriptions including the access to systems required for the job
- Complete performance management requirements including conducting one to one meetings, objective setting, PDRs and performance ratings. See the Performance Development Reviews page on the intranet for more information.
- Ensure that bullying and harassment is not tolerated in our workplace. See the Bullying and Harassment Policy
- Listen to and act on grievances -see Grievance Policy and Procedure for more information.
- Deal promptly and effectively with conduct, performance and attendance issues. View Conduct Policy, Performance, Attendance and Behaviour (see separate guidance for managers, colleagues and CSCs performance) and Managing Sick Absence Policy for further information.

- Hold, at a minimum, monthly team meetings which should be supported by the monthly Team Talk briefing materials which can be found on the intranet.
- Complete all mandatory compliance training and ensure your teams do the same. More information can be found on the intranet.
- Ensure that new colleagues are appropriately welcomed and inducted during their trial period. See Induction Policy and manager guidelines
- Ensure that systems access is removed for leavers
- Sharing information widely, early and often
- Involving our people in developing solutions early, giving them the opportunity to inform and influence business decisions

All line managers have access to the My HR Help service which supports managers with team management queries. Visit www.myhrhelp.co.uk.

And finally

Compliance is not optional.

It is important to remember it is everyone's responsibility to follow our Code of Business Standards. Failure to comply with the Code, company policies and the law can carry profound consequences for Post Office. It can also carry profound consequences for you. Where non-compliance with the Code, company policies or the law has been identified in accordance with established company investigatory procedures, we will take swift and decisive action against an offending party, up to and including, the termination of individual and or third party contracts as appropriate.

Post Office does not tolerate any form of retaliation against colleagues or third parties who have made reports, in good faith, of threatened, ongoing, past or suspected breaches of this Code of Business Standards

We all have a responsibility to promote the Code of Business Standards and managers should help and encourage their teams to understand and observe it.

Even with good judgement and the best intentions, we may not always know the most appropriate course of action to take. The Code, along with our other company policies, is designed to help us make proper decisions.

If you are faced with a dilemma, after reviewing the relevant parts of the Code, ask yourself a few questions to help make the right decision:

- Am I adhering to the Code, other policies and procedures?
- Am I being honest?
- What would others think of my actions?
- How might my decision affect others?
- Would I feel comfortable if my actions were reported in the media?
- How would my decision impact on Post Office reputation?

If you are still unsure as to the right thing to do, you should talk with your manager and discuss your questions and concerns.

We all share a responsibility to report concerns of actual or potential breaches of the Code of Business Standards, company policies and the law.

If you witness or otherwise learn about the company's standards and reputation being put at risk by unethical or even criminal behaviour, you must immediately, and without investigating, report it.

If you feel you can't talk to your own manager and want to speak to someone confidentially, please contact the **Speak Up** line on GRO More information can be found in the **Whistleblowing Policy**. You can also email **whistleblowing**GRO

POST OFFICE

RISK & COMPLIANCE COMMITTEE

7.1 Horizon Scanning Report

Author: Patrick Bourke   Sponsor: Jane MacLeod   Meeting date: 20 July 2017

Executive Summary

Context

As part of its remit, the Risk & Compliance Committee should consider legal, regulatory and other external developments on behalf of Post Office in order to ensure that impacts on Post Office (including its customers, staff, suppliers and stakeholders) are understood and being appropriately managed. This report highlights current developments of relevance to Post Office and the work that is being done to monitor these.

Questions this paper addresses

1. What are the material legal, regulatory and other external risks the Post Office executive and Board should currently be aware of?
2. What work is being undertaken to assess, monitor and mitigate these risks?
3. Who is accountable for this work and how will it be reported through Post Office governance structures?

Conclusion

1. There are a number of material developments which either will or could impact Post Office and details of these are set out in this summary.
2. In each case, work is being undertaken to monitor and assess the risks arising from these developments.
3. Governance structures and reporting lines will be developed to ensure there is appropriate representation from across Post Office in formulating responses to, and mitigation plans for, these developments.

Input Sought

The R&CC is asked to note these developments.

The Report

Taylor Review of Modern Working Practices

1. In October 2016, the Prime Minister asked Royal Society of Arts Chief Executive Matthew Taylor to lead an independent review into how employment practices need to change in order to keep pace with modern business models.

2. The Review, published on 12 July 2017, considered the implications of new forms of work on employee rights and responsibilities, as well as on employer flexibilities and obligations. The wide-ranging review looked at ways to ensure that the regulatory framework surrounding employment, and the support provided to businesses and workers, is keeping pace with changes in technology, the labour market and the economy.

3. Key recommendations for Government include:

   - People working for companies who have a controlling and supervisory relationship with them should be classified as '**dependent contractors**';

   - This dependent contractor category would be comprised of workers who are neither fully fledged employees, nor truly self-employed, since they exercise only limited autonomy in respect of their duties and the manner in which they are performed;

   - Dependent contractors should enjoy certain employment rights, including an entitlement to sickness and holiday pay, and the opportunity to achieve remuneration no lower than the level of the minimum wage;

   - Employers should be obliged to pay national insurance contributions in respect of dependent contractors, as part of a renewed effort to align the employment and tax frameworks to ensure the differences in tax paid for 'work', whatever the employment status of the individual performing it, are reduced to a minimum;

   - HMRC's role should be expanded to enable it to check that sickness and holiday pay entitlements, as well as those relating to the minimum wage, are being fulfilled;

   - Individuals should be able to seek a determination of their employment status for free at an expedited preliminary employment tribunal hearing, with burden of proof in such hearings reversed so that the employer has to prove that the individual is not entitled to relevant employment rights; and

   - There should be an increase in the use of Government approved digital platforms over time to reduce the incidence of cash-in-hand work, and boost tax revenue.

4. In her Statement to the House of Commons following publication of the Taylor Report, Margot James MP limited herself to a commitment that Government would respond to the Review by the end of the calendar year. Given the publicity the Government has given the Review, however, there is a strong likelihood that legislation in this area will be brought forward. However, it is unlikely that this represents grounds for immediate concern, in the context of the many other pressures on Government.

5. However, even at this early stage, it is possible to identify areas of potential impact which relevant teams at Post Office will wish to assess, in order that the organisation is as prepared as it can be to take the necessary measures to contain any areas of significant risk.

6. At the one end of the spectrum, these include:

   - Any changes required to workforce planning and management to reflect the 'dependent contractor' status envisaged by the Review;

     The effect of any reduction in the flexibility the organisation might enjoy to resource particular projects and programmes, as well the cost implications, including those relating to tax and compliance, of any such moves; and

   - The effects, both positive and negative, of a reduction in the amount of cash-in-hand work and therefore cash in the economy, and an increased demand for forms of digital payment.

7. At the other end of the spectrum is a basket of risks associated with the potential for the introduction of this new category of dependent contractor to be seized upon to create pressure for a concerted challenge to the status of our agents.

8. With the exception of our colleagues working in Directly Managed Branches, Subpostmasters currently work for us on the basis of a contract for services and we do not, therefore, consider or treat them as employees.

9. Self-evidently, any change to that position would have profound implications for our current business model:

   - were agents to be re-classified as dependent contractors under new legislation, they would acquire very substantial new rights and the costs involved would be unsustainable;

   - moreover, the National Federation of Subpostmasters (NFSP) could be in a position to mount a successful challenge to the currently applicable ruling of the Certification Officer who, in January 2014, found that the NFSP is NOT a trade union on the basis that it does not represent individuals falling within the current statutory definition of 'worker' (though noting that should NFSP revert to becoming a Trade Union, the Grant Agreement would fall away); and

- aside from the NFSP, this sort of shift also entails the possibility of our agent network, or a proportion of it, becoming subject to a membership recruitment campaign by the Communication Workers Union and/or Unite.

10. As noted above, we are some considerable way off from the point at which these risks have any prospect of crystallising. Convention would also have it that a Conservative Government would be particularly alive to the risks to business generally, and the Post Office in particular, of any precipitous move in this direction.

11. However, the turbulence in the political landscape, in which both main parties are making strenuous efforts to position themselves as the true champions of working people, and where the possibility of a General Election sooner rather than later cannot be discounted, it is important that the organisation is alive to these risks.

12. Drawing from another context, the RCC will also be mindful of the fact that a key line of attack against Post Office in the ongoing Sparrow litigation centres on the Subpostmaster contract, and whether it should properly construed as containing significant implied duties on the Post Office towards the Subpostmaster.

13. **The Employee Relations, Agents' Development and Remuneration, Legal, and Corporate Affairs teams** are working closely together to monitor and assess the situation, and to inform, and make recommendations to, senior management as the need arises over the weeks and months ahead.

14. A more detailed briefing, covering all the impacts on the business as an employer is being prepared for GE by HR teams, following the commitment given by Martin Kirke at GE on 13 July.

Information Commissioner Audit of Security of Personal Data in Telecoms Business

15. The Post Office has been asked by the Information Commissioners Office (ICO) to participate in an audit of its Telecommunications Services business. The ICO, by virtue of the Privacy and Electronic Communications Regulations (PECR), has statutory powers to conduct compulsory audits in this area but prefers, in the first instance, to try to perform these on a voluntary basis. Following discussions with the ICO, the proposed dates for the audit are the end of October/beginning of November 2017.

16. This audit forms part of a programme begun by the ICO in early 2016, as part of a commitment to audit all Communication Services Providers over a three year period. The audits last year focused on the larger players including Vodafone, BT, and Talk Talk.

17. The ICO's audit powers under the relevant legislation are limited to the Security of the Personal Data that is collected to enable us to provide the service to our subscribers. Specifically, the audit will focus on the following areas:

    - Governance and Risk Management - specifically the areas relating to Network and Information Security Governance and Risk Management;

    - Human Resources Security - The security measures taken to provide assurances to PO as to the security of personnel, such as employees, contractors and third-party users;

    - Security of Systems and Facilities – This includes the environmental and physical security elements;

    - Personal Data Breach Reporting, Management and Monitoring – Detection of, response to, and communication about Information Security Incidents involving personal data;

    - Business Continuity Management – The security measures for protecting public electronic communication services from the effects of major failures of information systems or disasters and to ensure their timely resumption; and

    - Monitoring, auditing and testing – monitoring, testing and auditing of network and Information System, facilities and security measures.

18. Under the provisions of PECR, the ICO has powers to impose financial sanctions for breaches. Under PECR, these fines are limited to up to £1,000 being awarded for failures to notify the ICO of any breaches incurred by PO Telecoms Services.

19. However, the ICO has further powers under the Data Protection Act where she can award sanctions ranging from Enforcement Notices, further audits or fines up to a maximum of £500,000 for infringements of the DPA. It is worth noting that should this audit be taking place at the same time next year, then the potential fines regime under the General Data Protection Regulation would be considerably higher with fines for these types of breaches having an upper limit of £20m in the case of the Post Office.

20. Preparations for the successful management of this audit are underway, with a small project team and working group being formed to co-ordinate across the business, working to Meredith Sharples (Telecoms Director) and Chris Russell (Data Protection Officer). The success of this audit will also, in part, depend on our relationship with Fujitsu who have already been briefed.

21. Regular updates will be made available to key stakeholders, prior to, during and post audit.

Company no. 8459718 – Strictly Confidential

RCC 17/31 – 17/40

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 27 April 2017

Present:	Susie Hayward (SH)	Head of Risk and Compliance (Chairman)
	Gerry Barrett (GB)	Head of General Insurance
	Stephen Gaines (SG)	POMS Compliance Manager
	Russell Tavener (RT)	Head of Commercial Operations
	Michael Brown (MB)	Deputy for Head of Commercial
	Ryan Griffin (RG)	Head of Protection
	Gerry Barrett (GB)	Head of General Insurance
	Francisco Couto (FC)	Head of FS Legal
In Attendance:	Elizabeth McMenemy (EMM)	Compliance Advisor
	Susan Don (SD)	Financial Promotions Officer
Apologies:	Ben Foat (BF)	Head of Legal
	Gill Craig (GC)	Deputy for Head of Travel
	Sanjeeve Thakrar (ST)	Risk Manager

RCC17/31 WELCOME, QUORUM AND CONFLICTS OF INTEREST

The Chairman declared the meeting quorate and open.

RCC17/32 MINUTES OF THE MEETING HELD ON 23 MARCH 2017

(a) The minutes of the meeting held on 23 March 2017 were approved and the Chairman was authorised to sign them as a true record of the meeting

RCC17/33 MATTERS ARISING AND ACTIONS LIST

(a) SH spoke about the need to use the RCC meetings to discuss the data in more detail and better understand what the data is telling us, thus enabling appropriate escalation to EXCO. SH requested papers to be submitted in time for review and that preparation, questions and actions are brought to the meeting.

(b) The action list to be re-circulated for updates from action owners including new actions from this meeting

RCC17/34 RISK MANAGEMENT

Action all (a) Group discussion around risk assessment, challenging our own appetite, ensuring controls are reviewed and subsequent actions followed through. Risk register to be reviewed to ensuring we are capturing the key risks to the business and emerging risks are also being captured. The new Xactium risk management system coming in soon should help drive those disciplines. In the meantime there is still the action (17/24(e)) from the last meeting for **all risk owners to revisit the risk register and update their own risks**

Action SH (b) There is a risk workshop for Board due in July, **but SH to set up a risk workshop for the senior management team in the meantime.**

Action SH (c) Risk Acceptances were reviewed and the acceptance rational for the new global payments contract risk (risk id 87) was questioned as currently showing within appetite. **SH to check with ST.**

RCC 17/35 INCIDENT MANAGEMENT

Action GB/RT/ST (a) Discussion around the incidents relating to Junction and whether we are recording incidents which are being correctly managed by third parties. Discussed the definition of incident and the levels of escalation required in accordance with the contract. **GB/RT/ST to consider defining of what constitutes an incident and update the incident management process**.

Action ST (b) The pause and resume incident is still showing as open, but this is now fixed and can be closed. **ST to close incident**

(c) Discussion around ZEUS defects and what constitutes a change request versus reporting the issue as an incident. All agreed that where the issue leads to customer detriment outside appetite or any other regulatory impact then this would be deemed an incident. All ADC incidents are captured and change requests added to the demand pipeline to be prioritised.

Action RT (d) General question as to how defects in the demand pipeline are prioritised so **RT to arrange a ZEUS incident prioritisation meeting**

RCC17/36 1st LINE COMPLIANCE REPORT

Scorecard

(a) The amended conduct scorecard was presented for discussion and further analysis. The output from the meeting will form the basis of commentary for Exco.

Action RT (b) The business recognises the need for additional MI and discussion continued around how we can obtain reporting from Hexaware, when all parts of the business are also requesting MI. Considered that an MI project needs to be instigated to prioritise business requirements **RT to discuss with Michelle**

Action SH (c) To contextualise travel complaints we need number of travel policies in force, especially now this forms part of the FCA complaints return**. SH to ask David White for travel policies in force**

(d) **Complaints**
It was noted that complaints had increased by 18% with 77% for Travel. The reasons for complaints included incorrect information, unhappy with process and refunds. Contact centre rates higher than branch.

Action RT (e) Collinsons upheld rate is also high at 40%. Discussion on the high upheld rate continues for travel for complaints, however benchmarking from FCA records suggests 50% may be industry standard. RT is conducting further analysis on the root cause for complaints with Webhelp, Collinsons and TIF. A paper will be presented to June RCCC/Exco with recommendation for our tolerance level.

(f) Discussion on the impact of new FCA renewal rules on complaints and retention, GB advised no great impact so far, but motor maybe more visible as rates are increasing for 15/4 incepts. Ogden rates likely to have a significant impact on rates and may see further complaints to follow.

Claims

(g) GB advised that the new claims outsourcing project will go live on 9th May 2017 which should enable us to improve our claims MI with an active reporting tool.

Cancellations

Action RT (h) Due to errors with the report, the life cancellation lapse curve was not available for this month. It was also noted that no travel cancellation data was available. **RT to try and obtain short term cancellations for travel from elsewhere** however it was noted that travel cancellations remain low at less than 1%

Action RT (i) Regarding Life cancellations the reasons for cancellation are captured in free text, therefore difficult to get meaningful MI from Royal London. **RT to follow up with Tom**

Quality Assurance

(j) Results of the Webhelp QA were discussed at the QBR the previous day with many of the errors due to medical questions, features and exclusions and agent errors. The competence of the agents and content of training were discussed with WH.

(k) SH advised that results of the branch mystery shopping for travel and over 50's were not particularly good and not enough is being done compared to how many policies sold. POL are to provide Compliance with an action plan to fix these issues and SH will include branch QA results into RCC pack

RCC17/37 **2nd Line Compliance Report**

Action EMM (a) SG and EM briefly presented the second line deck, the only issue to follow up was that on all O50's & Term calls monitored, the call paused at the bank details correctly, however the bank details were visible on screen. **EMM to investigate**.

EMM noted that there had been a low volume of Life calls undertaken by WH and the majority of these were the shorter FPL and O50's calls

(b) SD noted that the main reason for rejection of fin proms was the use of Post Office rather than Post Office Money

RCC 17/38 **ISAG REPORT**

(a) There was no ISAG report provided this month.

RCC 17/39 **POL REPORT**

(a) There was no POL report provided this month whilst we await POL's action plan for 17/18.

RCC 17/40 **ANY OTHER BUSINESS**

(a) There was no other business raised. There being no further business the meeting was closed.

The next meeting of the RCC will be held on 22 May 2017 at 12.30pm.

Chairman…………………………………..….. **Date** …………………

Company no. 8459718 – Strictly Confidential

RCC 17/41 – 17/49

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 22 May 2017 at 12.30 pm

Present:	Susie Hayward (SH)	Head of Risk and Compliance (Chairman)
	Gerry Barrett (GB)	Head of General Insurance
	Stephen Gaines (SG)	POMS Compliance Manager
	Russell Tavener (RT)	Head of Commercial Operations
	Michael Brown (MB)	Deputy for Head of Commercial
	Ryan Griffin (RG)	Head of Protection
	Sanjeeve Thakrar (ST)	Risk Manager
In Attendance	Ann Young (AY)	Compliance Advisor
Apologies:	Francisco Couto (FC)	Head of FS Legal
	Gill Craig (GC)	Deputy for Head of Travel
	Elizabeth McMenemy (EMM)	Compliance Advisor

RCC17/41 **WELCOME, QUORUM AND CONFLICTS OF INTEREST**

The Chairman declared the meeting quorate and open.

RCC17/42 **MINUTES OF THE MEETING HELD ON 27 April 2017**

(a) The minutes of the meeting held on 27 April 2017 were approved and the Chairman was authorised to sign them as a true record of the meeting

RCC17/43 **RISK MANAGEMENT**

(a) ST discussed the areas for concern and confirmed that there were 4 items on the risk register which were outside appetite. RT confirmed that the ISAG/ IPA position has been filled and will commence employment in July. It was agreed to reduce the risk from 4 to 2 and this will bring the risk to within appetite

Action ST (b) ST to set up a risk workshop for the POMS senior lead team for a date in June (date to be confirmed).

Action ST (c) ST confirmed that the installation of the Xactium system was nearly complete and in house training to be arranged to include the 4 main users. A date to be agreed in June.

RCC 17/44 **INCIDENT MANAGEMENT**

Action ST (a) ST confirmed to the meeting that few incidents had been reported this month. There are currently 4 incidents on the register. It was noted that the last entry on the register was 12 April. ST to check with EMM, Kenny and Nichola that there have been no incidents recorded since this date.

Action ST (b) The reporting of incidents was discussed. Third party incidents would be reported to POMS when above defined thresholds and therefore the definition of reportable incidents needs to be clarified on the incident reporting process. ST to obtain the Junction definition of an incident from Ian Coughtrey.

Action ST (c) Following any change of the incident management process, RT suggested that ST could educate the POMS staff in the involvement of incident management.

RCC17/45 **1st LINE COMPLIANCE REPORT**

Scorecard

(a) The conduct scorecard was discussed. It was noted that complaints were down by 4.8%. The upheld complaints were 30%. This was driven by travel complaints. It was noted that no data has been provided on the lapse curve. MB confirmed this is due to problems with Hexaware and David Williamson is currently working on this. The CES score was discussed and RT is in discussion with POL.

Complaints

(b) RT confirmed that BGL are not reporting on upheld or rejected claims from the contact centre. The only complaints that are reported are those from the Customer Relations Team.

(c) SG reported that the number of complaints managed by Webhelp resolved within three days had reduced significantly. The reason for the reduction could be a reflection of the resource challenges within the team and should be closely monitored.

Action RT (d) MB noted that the complaints numbers were down by 4.8% month on month and the upheld complaints remained high at 30% due to travel complaints. A review of upheld complaints is in progress and will be reported at the next RCCC.

Quality Assurance

Action RT (e) The travel quality assurance red calls has increased to 24%. The reason given for this increase is an influx of new starters and a lack of experience within the campaign. The medical screening failures had increased. RT to contact WH to ensure this is reported in earlier.

Action SG (f) The quality of the Webhelp reporting on QA was discussed and SG noted they were working with help to improve the value of the information reported and the actions being taken

Cancellations

Action MB (g) It was noted that the cancellation lapse curve report was still experiencing problems and therefore had not be reported for the second month. Noted also that the Travel lapse curve report was not able to be issued. MB to check with David Williamson on the status of the MI.

(h) The cancellation reasons were reviewed and noted that there were 26 cancellations for conduct reasons recorded for travel insurance. The

Action MB

Action SH

reason given were mainly errors made within the branches and contact centre. MB will continue to track these reasons and review for more information. It was noted that Royal London were not able to track cancellation reasons as this is a free text field and unable to collate MI, SH to check with RL.

(i) The number of complaints relating to motorcycle insurance had continued to increase. The reasons provided were issues with the service provided by Devitt's, including lack of call-backs, duplication, i.e re-requesting previously requested information and unable to get through to the contact centre. MB confirmed to the meeting that Devitt's had missed the SLA twice and this is being monitored by the operations team.

RCC 17/46 **ISAG REPORT**

Action SH (a) There was no ISAG report provided this month. It was noted that a new started was due to join the IPA team who will be POMS business partner. Agreed to invite to the next meeting.

RCC 17/47 **POL REPORT**

(a) SH provided a verbal update to the meeting on the outcomes of an earlier conduct meeting with POL. There were two RED VMS for life this month due to errors with the life provider, not providing information in all product choices and incorrect information on the appointment of a beneficiary. A further Amber VMS had been recorded for Home by not giving the customer sufficient time to read the Policy summary. POL have agreed to pull together an action plan for VMS/MS results and will share at the next meeting.

(b) It had been noted that only 366 of the 501 CRM's had completed the Hera training on the new life provider. POL are investigating and will provide further information in due course.

RCC 17/48 **MATTERS ARISING AND ACTIONS LIST**

(a) **16/45©** PCI Compliance – RT seeking to understand POMS requirements in line with the new Globalpay contract. Defer to July meeting

(b) **17/06** © Panel of Insurers – GB to provide an update with MI at the June meeting

(c) **17/37 (a)** EMM To investigate bank details visible when calls paused. C/Fwd

RCC 17/49 **ANY OTHER BUSINESS**

(a) ST confirmed that the Draft PWC Internal Audit report on Risk and Compliance report is expected this week. This will be shared with the RCCC when available.

(b) There was no other business raised. There being no further business the meeting was closed.

The next meeting of the RCC will be held on 26 June 2017 at 09.30am.

Chairman…………………………………..…. **Date** …………………

POL00401625

Company no. 8459718 – Strictly Confidential

RCC 17/50 – 17/59

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 26 June 2017 at 9.30 am

Present:	Susie Hayward (SH)	Head of Risk and Compliance (Chairman)
	Stephen Gaines (SG)	POMS Compliance Manager
	Russell Tavener (RT)	Head of Commercial Operations
	Michael Brown (MB)	Deputy for Head of Commercial
	Ryan Griffin (RG)	Head of Protection
	Sanjeeve Thakrar (ST)	Risk Manager
	Francisco Couto (FC)	Head of FS Legal
	Elizabeth McMenemy (EMM)	Compliance Advisor
	Beverley Turner (BT)	Senior Product Manager
	Alberto Zanatta (AZ)	Audit Manager
In Attendance	Ann Young (AY)	Compliance Advisor
Apologies:	Gerry Barrett (GB)	Head of General Insurance
	Gill Craig (GC)	Deputy for Head of Travel

RCC17/50 WELCOME, QUORUM AND CONFLICTS OF INTEREST

The Chairman declared the meeting quorate and open.

RCC17/51 MINUTES OF THE MEETING HELD ON 22 May 2017

(a) The minutes of the meeting held on 22 May 2017 were approved and the Chairman was authorised to sign them as a true record of the meeting.

RCC17/52 RISK MANAGEMENT

Action ST (a) ST confirmed that a risk workshop has been undertaken with the Senior Lead Team to discuss the emerging risks, new risks and risk appetite. ST confirmed that a list of the emerging risks would be circulated for discussion prior to the next workshop which is scheduled for 9 August.

Action ST (b) ST confirmed that the Risk Appetite statements will need revision before they are presented to the Board. ST also confirmed that a workshop to discuss risk appetite further is to be arranged. Date to be confirmed.

Action ST (c) ST advised the meeting that the Xactium system is due to go live this week and reports will be ready for the next RCC in July.

(d) ST confirmed that there had been a session with the Senior Lead team to discuss the implications of Brexit and the risks faced by POMS. There are to be further sessions as possible risks emerge.

Action ST (e) ST discussed the new risks facing POMS including concentration risk, investment curve, aggregators, Management information, shareholder funding and staff. ST will enter the new risks on the Risk Register and communicate to RCCC.

RCC 17/53 **INCIDENT MANAGEMENT**

Action ST (a) The ghost policy issue was discussed and RT confirmed that the root issue is being investigated, in the meantime the scale has reduced and fixes are being put in place. ST to obtain an update to the actions from the team and update the Incident Register.

Action ST (b) An incident relating to the Junction renewal letters following the new FCA requirements has been entered on the Incident Register. ST to investigate full details and check if Junction have now resolved the issue.

RCC17/54 **1st LINE COMPLIANCE REPORT**

(a) RT discussed the operational issues encountered in Webhelp. The QA results for May were reported at 40% and so far for June at 42%. There are issues with the volume of new agents, level of competence and oversight. The error are also shown in the 2nd line compliance and the complaints handling. It had been decided to implement Project Calibre to deal with the issues. This project will be overseen by Head of Operations Nichola Hazard. Actions include looking at recruitment processes and training programmes and taking significant steps to step in to the management of WH and control of the QA/Complaints team. Need to understand and improve operations quickly. This will mean a focus for the POMS team based in Glasgow to ensure solutions are imbedded quickly. RT is now receiving a data feed from WH as there were concerns over the transparency of the MI provided.

(b) BT reported that the CLUK claims project for Home is now live however only with one insurer so far and only one claim. More information will be provided at the next meeting.

(c) Travel claims are reporting higher in number due to seasonality but levels of repudiations are consistent

(d) Complaints – It was noted that no MI had been received from WH this month for complaints and concerns were mounting over the handling and reporting of complaints as discussed earlier.

Action MB (e) MB discussed the emerging trend in the Collinsons complaints relating to errors and customer services in branch. MB confirmed that the complaints are consistent with branch feedback in complaints. MB agreed to monitor and discuss with CISL

Action MB (f) MB noted that there had been a disparity in the POMS lapsed curve and the RL dashboard. There appears to be a significant gap in cancellations report. MB also noted that the dashboard appears to be more consistent with the cancellation data from Royal London. MB will discuss with David Williamson which MI to use.

RCC 17/55

Cancellation reasons were showing 38 conduct cancellations due to branch processes. No cancellation reasons had been provided by RL, SH to chase.

(g) RT presented a report on the Upheld Complaint Deep Dive. Currently the business upheld rate is 20%. However, this has not been achieved and the rate has been 32% on a 12 month average with travel being the highest in volume and upheld rate. It was also noted that POMS as a business is performing within average industry levels. It was agreed in the meeting to increase the upheld rate tolerance level in the scorecard to 35% with a 10% tolerance for Amber.

2nd Line Compliance Monitoring

(a) EMM provided a report on the 2nd line compliance monitoring undertaken at Webhelp. There were 87 variances for Travel and 36 for Life with 4 instances of potential detriment. These are reflective of the new QA agents and the lack of training and guidance, this will be picked up as part of Project Calibre. EMM also confirmed that she had undertaken training and calibration session with the new QA personnel. EMM noted that the new agents are undertaking their training in Falkirk and losing valuable hours in traveling with no compliance included in the training.

(b) AY provided an update on the 2nd line compliance monitoring undertaken in the branches and noted that there had been an increase in calls available for review. Subsequently, the number of calls reviewed for the 2nd line compliance monitoring had also been increased SH noted that the VMS process is currently out for tender and advised that the amount VMS calls for insurance should be representative of the business written. It was also noted that due to the tendering process there had been no Non-Video VMS visits to review during April or May.

(c) SG confirmed that the financial promotions approved first time continues to improve with the remainder achieving approval on the second attempt. SG also advised that there had been a review of the Financial Promotions process and confirmed a decision to remove the withdrawal forms had been undertaken.

RCC 17/56 ISAG REPORT

(a) There was no ISAG report provided this month. It was noted that a new starter was due to join the IPA team who will attend the RCC from August onwards

RCC 17/57 POL REPORT

(a) SH confirmed that the scope of the monitoring team will be widening and will be looking at other areas, including Mortgage Specialists, training, ASPM and BDM spans of control and sales behaviours (including the behaviours during customer offer days).

(b) SH advised that the final draft PWC report had been discussed and responses prepared and was now ready to go to EXCO.

(c) SH advised that Thistle has also completed two reviews, Anti money Laundering and Anti bribery and corruption. There were a few minor issues to address but both reported low risk.

(d) SH discussed the issue with the JCC and the unwillingness of the POL management to address the items raised during the monitoring reviews. Progress will be made by tackling issues and putting action plans in place.

(e) SH discussed the EUM project. The roll-out had been scheduled for June, but due to operational issues, including issues with access to Success Factors. The pilot is now scheduled for 26 July. This will involve 25 branches over a period of 3 weeks. Full rollout of 500 branches selected by POMS will commence 11 September for 6 weeks. A further rollout of another 500 branches is expected by February 2018. These rollouts will cover 75% of the top performing branches within the network. SH also advised that Michelle Downs will now look after the EUM project.

RCC 17/58 **MATTERS ARISING AND ACTIONS LIST**

(a) **16/45©** PCI Compliance – RT seeking to understand POMS requirements in line with the new Globalpay contract. Defer to September meeting.

(b) **16/92 (b)** Risk Management – Produce for control self-assessment and share with the owners – September meeting.

(c) **17/26 (**f) Cancellation reason- SH to check with Royal London for more information on cancellation reasons. Ongoing

(d) **17/37 (a)** EMM To investigate bank details visible when calls paused. Ongoing

RCC 17/59 **ANY OTHER BUSINESS**

(a) MB thanked SH on behalf of the attendees for her continuing help during her time as chairman of the RCC and wished her success in the future.

(b) There was no other business raised. There being no further business the meeting was closed.

The next meeting of the RCC will be held on 27July 2017 at 15.00 pm.

Chairman.. **Date** ....

Post Office Ltd
Risk & Compliance Committee meeting
20 July 2017

Location:

Boardroom 1.19 Wakefield , Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ, United Kingdom

ATTENDANCE LIST

ATTENDEES	SIGNATURE
MacLeod, Jane	
Alwen, Lyons	
Cameron, Alisdair	
Houghton, Rob	
Kirke, Martin	
Mark, Davies	
Martin, Edwards	
Nick, Kennett	
Paula, Vennells	

Also in attendance

CoSec	

Apologies for absence

Kevin, Gilliland

Additional access

Regan, Avene	
Smith, Debbie	