POL00423693

Post Office Risk and Compliance Committee Agenda

Date
13 September 2017

Start Time	Finish Time
13.00	16.00

Location
1.19 Wakefield, Finsbury Dials

Present	In Attendance		Apologies
Jane MacLeod(Chair) Al Cameron Mark Davies Martin Edwards Kevin Gilliland Rob Houghton Martin Kirke Nick Kennett Paula Vennells	Johann Appel Richard Williams Amanda Radford Georgina Blair Deana Herley Jonathan Hill Jenny Ellwood	Sally Smith (item 3.3) Tim Armit (item 3.6) Ben Foat (item 6.1 and 6.3) Barbara Brannon (Item 6.2) Paul Blackmore (item 8.1 and 8.2) Chris Russell (item 8.3)	

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 20th July and update on actions	Chair	
3. Key Operational Risks **3.1** FS Conduct **3.2** Change* **3.3** Financial Crime* **3.4** IT Controls Framework & DR **3.5** Finance Controls **3.6** Business Continuity	Discussion & approval	✓ *paper to be discussed at ARC (others for noting)	To review the management of key operational risks.	 Jono Hill Jenny Ellwood Sally Smith Rob Houghton Amanda Radford Tim Armit	13.05 – 14.05 (60 minutes)
4. Annual Report and Accounts **4.1** Executives' Declaration and Risk section for ARA	Approval	✓	To approve the risk section for the 2016/17 Annual Report and Accounts including top risks and executive declaration.	 Deana Herley / Richard Williams	14.05 – 14.25 (20 minutes)

POL00423693

Post Office Risk and Compliance Committee Agenda (cont.)

Agenda Item		Action Needed	For ARC	Purpose	Lead	Time
5.	**Risk** **5.1** LRG Placemat **5.2** Finance & Operations Placemat	Questions & Noting	✓	To note results of roll out of placemat in LRG and Finance and Operations.	 Chair Alisdair Cameron	14.25 – 14.45 (20 minutes)
6	**Compliance** **6.1** Regulatory Framework **6.2** Procurement Compliance reporting **6.3** Criminal Finances Act	Questions & Noting	✓	 To discuss the legislative and regulatory framework applicable to Post Office. To review the Procurement compliance report To note the requirements of the CFA	 Ben Foat Barbara Brannon Ben Foat	14.45 – 15.20 (35 minutes)
7.	**Audit** **7.1** Internal audit report **7.2** Camelot lessons learned	Questions & noting	✓	 To note the Internal Audit Report. To note Camelot lessons learned	 Johann Appel Kevin Gilliland	15.20 – 15.40 (20 minutes)
8.	**Policies** **8.1** AML & CTF **8.2** Whistleblowing **8.3** Data Protection **8.4** Code of Business Standards	Approval	✓	To approve new and updated policies for onward submission to the appropriate non-executive body for final approval.	 Paul Blackmore Paul Blackmore Chris Russell Martin Kirke	15.40 – 15.55 (15 minutes)
9.	**Noting papers** **9.1** Horizon Scan **9.2** POMS RCC minutes **9.3** Insurance Renewal	Noting	✓		 Chair Nick Kennett Al Cameron	15.55 – 16.00 (5 minutes)
10.	**Any Other Business**					
	CLOSE					16.00

POL00423693

Risk and Compliance Committee (R&CC)		**Reference: R&CC July 2017**
Date: 20 July 2017	**Venue: 0.03 Moorgate, 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
Mark Davies (MD)	Group Communications, Brand & Corporate Affairs Director	Member
Martin Edwards (ME)	Group Strategy Director	Member
Rob Houghton (RH)	Group Chief Information Officer	Member
Nick Kennett (NK)	Chief Executive – Financial Services	Member
Martin Kirke (MK)	HR Director	Member
Paula Vennells (PV)	Group Chief Executive	Member
Attendees:		
Richard Williams (RW)	Senior Risk Manager	Report (Paper 4.1)
Elena Nistor (EN)	Audit Manager	Report (Paper 5)
Deana Herley (DH)	Senior Assurance Manager	Report (Paper 4.1)
Georgina Blair	Risk Business Partner	Secretariat
Jonathan Hill (JH)	Head of Risk, Banking Regulation and Strategy	Report (Paper 3.1)
Jenny Ellwood (JE)	Head of Transformation Risk and Assurance	Report (Paper 3.2)
Amanda Radford (AR)	Financial Controller	Report (Paper 3.6)
Martin Hopcroft (MH)	Head of Health and Safety	Report (Paper 3.7)
Sally Smith (SS)	Head of Financial Crime	Report (Paper 3.3)
Roger Gale (RG)	Sales and Trade Marketing Director	On behalf of Chief Executive Retail
John Whitefoot (JW)	Employee Relations and Policy Director	Report (Paper 6.5)
Rebecca Barker (RB)	Head of IT Risk and Compliance	Report (Paper 3.5)
Apologies:		
Kevin Gilliland	Chief Executive Retail	Member
Alwen Lyons	Company Secretary	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.		

POL00423693

Agenda Item 2, RCC minutes and actions

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

The Committee noted there had been some confusion over the description of AP 1776 'Camelot Audit Lessons Learned' and that it was not necessary for the current Camelot Audit to complete before preparing a summary of lessons learned.

For points (i) & (ii) the JML update and audit, the Chair explained there was ongoing activity. MK gave an update on (iii) the data cleanse activity underpinning regulatory training, noting that this was much improved and that a process to update the data for new joiners had been developed.

Agenda Item 3, Key Operational Risks

3.6 Finance Controls

AR updated the Committee on the investigation into an unsupported £0.5m debit balance discovered relating to the now-closed Merlin Cash Centre (incident initially reported in May 2017). Investigation had revealed control gaps in POLSAP processes, and remediation had been implemented, including a manual authorisation process for POLSAP journals, and further remediation was planned.

3.1 FS Conduct Risk

JH introduced the paper noting that there were no issue of particular regulatory concern. JH noted that a review of red video mystery shop results had shown that some Customer Relationship Managers (CRMs) strayed from the approved regulatory wording during their customer discussions. JH briefly explained the training and monitoring processes for CRMs to explain how such incidents were resolved.

The Committee observed the putative training requirements included in FCA's Insurance Distribution consultation paper (which include 15 hours of CPD annually) and discussed the burden of regulatory training which falls on branches as result of selling regulated products. The Committee noted that there was a limit to how much training branches could absorb. The Committee requested a further briefing on the potential training requirements of the Insurance Distribution Directive in order to consider the future compliance burden against capacity in the branch network (**AP 1781**). JM explained that the legal team had developed a regulatory framework in response to an ARC action which would help inform the discussion, and the Committee requested that the regulatory framework be brought to the September RCC meeting for discussion (**AP 1782**).

The Committee discussed the POMS scorecard and requested that it be developed to make it more similar to Bank of Ireland's scorecard & include some commentary **(AP 1783)**.

3.2 Change Risk

JE introduced the paper. The Committee discussed the report and requested that the report be developed to give more information about benefits realisation **(AP 1784).**

3.3 Financial Crime

SS introduced the paper and summarized the regulatory updates. The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 came into force on Monday 26th June 2017 but the eKYC (electronic know your customer) requirements were still unclear. Post Office would find it difficult to retain copies of ID documents the in branch, either electronically or physically, and work was underway to clarify the requirement with the regulator. **Action: ME to discuss with SS whether the eKYC requirements could be met through the identity proposals that ME's team were working on. (AP 1785)**.

The Committee briefly discussed the branch registration process, noting that a new process was now in place. SS noted that with the increase in concern around terrorist financing, it was

POL00423693

important that this risk be considered as part of the screening requirements for new agents. SS confirmed that there was work currently underway to assess the risk of unintentional terrorist financing through the branch network.

SS noted that during August identity checking would be introduced at lower transaction levels; a likely consequence would be an increase in transactions that needed to be investigated and depending on levels, POL's monitoring capability to deal with increased volumes would need to be kept under review.

3.4 Annual Gifts & Hospitality Report

SS introduced the annual gifts and hospitality report, explaining that the existing process suffered from gaps and a lack of enforcement. SS explained that a new gifts and hospitality reporting tool had been developed, which would allow quarterly reporting for each business function, and which was expected to be implemented during August. The Committee will be presented with an interim gifts & hospitality report in November to demonstrate the outputs of the new reporting system **(AP 1786)**.

The Committee briefly discussed the reporting limits and approved the proposed increase in the hospitality reporting limit from £100 to £200 and the decrease in the gift given reporting limit from £200 to £100.

3.7 Health and Safety

MH presented the H&S update. The Committee noted the increase in Supply Chain accidents and the preponderance of parcel related incidents, and queried whether there was any single cause. MH noted that no particular reason for the spate of accidents had been found. The Committee discussed the age profile in Supply Chain, noting that the risk of back strain and similar injuries is more likely in an aging workforce. AC noted that some offices had several members of staff off at the same time which was affecting quality of service targets. MK noted that Royal Mail had the same issue with regards to many of its operational staff.

MH noted that an annual Health & Safety 'deep dive review' had recently been undertaken by the GE H&S Sub Committee (Safety Board) and focused on the three areas of property, security and road risk for commercial and business drivers. The Committee briefly discussed the issue of cladding around buildings and any potential fire risk. AC explained that relevant buildings in the property estate were being tested.

MH also explained that mental health first aiders were to be rolled out across the business. OH Assist would train up to 60 people across the business to act as 'first responders' to sign post help to any members of staff showing signs of suffering from mental health issues. The Committee approved of this initiative and noted that suitable comms should accompany the roll out to explain the role of the mental health first aiders.

3.5 IT Controls and IT Tube Map

RB presented the IT Controls Update, explaining that development of the IT Controls Framework, based on COBIT5, was on track and that all 11 priority Cobit 5 processes had been reviewed and the core suppliers' controls identified, and gap assessments completed. The Chair queried whether appropriate documentation processes were in place and RB noted that policies, processes and standards were being developed as part of the framework.

RH presented the IT Risk Update, including the IT Tube Map. The Committee discussed the rate at which IT risks were expected to reduce and noted that the tube map was helpful in displaying changes in expected control status over time but because of scale was not able to show a gradual diminution of risk.

3.8 Business Continuity

The Committee noted the paper

POL00423693

3.9 DR Testing

The Committee noted the paper.

Agenda Item 4, Risk Update

4.1 LRG Placemat

The Chair introduced the LRG Placemat using some slides (added to meeting records as Paper 4.1.1.1). The Committee discussed the placemat and the presentation of risks and controls. The Chair explained that work was ongoing and that the September meeting would include a refined LRG placemat, the first results from Finance and Operations. Work would now commence on the roll out of the Placemat to Retail and FS&T business units.

4.2 Risk Incidents

RW gave the Committee a summary of the reported risk incidents since the last meeting. The Committee discussed the categorisation of incidents, noting that fraud, theft and robbery should be categorised as one category as incidents often changed appearance as an investigation proceeded.

Agenda Item 6 Policies

6.2 & 6.3 Financial Crime and Anti-Bribery and Corruption Policies

The Committee approved the Financial Crime and Anti-Bribery and Corruption Policies.

6.2 Protecting Personal Data

The Committee noted that this policy was a necessary part of the preparations for GDPR. RH had some comments on the policy and agreed to send them to the Chair. This policy remains in draft.

6.1 Vulnerable Customer Policy

The Committee discussed the Vulnerable Customer Policy at length.

The Committee approved the Vulnerable Customer Policy.

6.5 Code of Business Standards

JW explained the approach taken to updating the Code of Business Standards. The Committee discussed the revised Code and requested further work. The Committee requested that JW gather feedback and update the policy and recirculate it for approval.**(AP 1787)**.

Agenda Item 5.1 Internal Audit Report

The Committee noted the paper.

Agenda Item 7 Noting Papers

The Committee noted the following papers

7.1 Horizon Scan

7.2 POMS RCC minutes

The meeting closed at 16.35

Next Meeting – Wednesday 13 September 2017, Room 1.19 Wakefield, 13.00 – 16.00

POL00423693

POL Risk and Compliance Committee
Action List

Status Report as at: 06/09/2017

Meeting Date	AP ref	ACTION	Action Owner	Due Date	STATUS	Open/ Closed
20/07/2017	**1787**	**Code of Business Standards -** Update report and circulate for feedback	John Whitefoot	13/09/2017	Sept Agenda item 8.4	To close
20/07/2017	**1786**	**Interim Gifts and Hospitality report** - Committee to review interim gifts and hospitality report demonstrating the outputs of the new reporting system	Sally Smith	08/11/2017		Open
20/07/2017	**1785**	**eKYC** - Discuss with Sally Smith whether eKYC requirements could be met through the identity proposals that ME's team is working on	Martin Edwards	13/09/2017	SS and ME have discussed. ME to provide verbal update if required.	To close
20/07/2017	**1784**	**Change risk -** Develop change risk report to focus on benefits realisation	Jenny Ellwood	08/11/2017	In September update have focused on the key themes we have concerns about which include benefit realisation. A wider review and revision of the risk report will be completed for November	Open
20/07/2017	**1783**	**POMS compliance scorecard -** Develop POMS compliance scorecard to make it more similar to Bank of Ireland's scorecard & include some commentary	Jonathan Hill	08/11/2017	Work is under way with POMS to identify possible improvements	Open
20/07/2017	**1782**	**Regulatory framework -** Discuss regulatory framework created in response to ARC action at RCC prior to discussion at September ARC	Jane MacLeod	13/09/2017	Sept Agenda item 6.1	To close
20/07/2017	**1781**	**Insurance Distribution Directive -** Provide a briefing on the potential training requirements of the IDD in order to consider the future compliance burden against capacity in the branch network	Jonathan Hill	08/11/2017	JH can provide verbal update in Sept meeting	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 September RCC	Kevin Gilliland	13/09/2017	Sept Agenda item 7.2	To close
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	13/09/2017	Superceded by placemat reporting	Closed
09/03/2017	1773	**RCC Terms of Reference** - to be reviewed and updated based on changes in PO structure	Jane MacLeod	09/11/2017		Open

POL00423693

09/03/2017	1770	**GE accountabilities map** - to be refreshed / updated based on the new structure following discussions	Jane MacLeod	13/09/2017	Will be an output of the development of the regulatory framework (see AP1782)	Closed

POL00423693

Financial Services Conduct Risk Update

Author: Jonathan Hill
Meeting date: 13 September 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) relates 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.

POL00423693

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 8th August there were 511 CRMs. The majority of these are active and digital tablet enabled. During July a new Telecoms tablet journey was enabled, allowing CRMs to engage with customers on Post Office Homephone, broadband and fibre products. It is planned that the CRM programme will pause at this number of CRMs for a period allowing the knowledge and processes of all the product journeys to bed in.

8. We have a more positive engagement with customers (on an introductory basis) on FS products through CRMs, which is carried out within a Training and Competence ("T&C") scheme that FS&T Risk oversee and monitor. Nevertheless as we seek to innovate the CRM network, we need to ensure that the conduct and operational controls in place remain appropriate.

9. The latest Video Mystery Shopping results for July were positive with only 3 out of 29 shops graded red. In each of the three red VMS the CRM did not provide an overview of the full range of savings accounts and in two instances the customers were not encouraged to read the application pack and consider the information before making an application.

10. The T&C Framework outlines the process Senior/ Support Managers need to follow when dealing with red VMSs. The actions are completed, documented and reported back in the monthly BOI Regulatory Review VMS Report.

11. The weekly ASPM/RSDM development call includes a VMS performance update. This includes a broadcast of the weekly results, the main causes of red & amber grades and the actions ASPM's and CRM's need to undertake.

12. We will monitor the next round of mystery shops at the respective BoI and POMS Committees.

Advertising breaches and issues

13. BoI repeated a concern that had been previously raised in relation to ensuring that marketing materials passed their approval 'sell by' date are re-reviewed and re-submitted for approval. Recent recruitment in the marketing team should make these incidents less likely. The Head of Marketing has been asked to provide a written response ahead of the next BoI Customer and Conduct Risk Committee.

14. On a related issue BoI monitoring has raised an issue in relation to a worsening trend of out of date literature in branches. From its monitoring activity (April-June) c60% of branches have been found to have out of date literature available to

POL00423693

customers either on display or behind the counter. FS&T Risk will work with the Retail Network team to ensure customers are given the appropriate literature and review what more can be done to improve compliance in this area.

Branch Regulatory knowledge

15. 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.

Future issues

16. There are a number of significant regulatory initiatives on the horizon that impact on Post Office and POMS:

    a. General Data Protection Regime (GDPR) - February 2018. This project is being led by the DPO and we are working with the team to assess and implement the requirements

    b. Vetting and 'Fit and Proper' - this is becoming an increasing priority for many of our regulators (e.g., FCA and HMRC). There is a new vetting process in place, but we need to risk assess new requirements (e.g., from HMRC) and assess whether the scope of checks needs to increase.

    c. Senior Managers and Certification Regime (SMCR) - extension to all regulated firms by 2018. This will have a direct impact on POMS. POMS is leading a project to implement this, which POL FS&T Risk is supporting, as it is the company directly impacted. The FCA has confirmed, as expected, in its latest Consultation Paper that Appointed Representatives such as Post Office will not be directly subject to SMCR. However, further guidance on the approach to SMCR for Appointed Representatives will follow.

    d. Insurance Distribution Directive, one of the proposed key requirements is increased CPD training for counter staff. POMS is leading a project to implement this by February 2018, working with the Post Office Training and FS&T Risk teams.

    e. Payment Services Regulations (Payment Services Directive 2) rules were finalised in July 2017 to be implemented in January 2018. As well as impacting on the conventional payment business these are of significant strategic impact as these regulations will open up access to the personal banking market for new types of payment firms and also allow third party firms to perform aggregation functions on behalf of and with the permission of consumers.

    f. Vulnerable customers: This is an FCA/Ofcom priority area. A vulnerable customer policy was agreed at the July RCC. We will shortly instigate risk assessment work together with the Retail Business Unit to assess whether we have any significant gaps in our approach.

Jonathan Hill
Head of FS&T Risk & Regulation

POL00423693

BOI Post Office Money branch distribution - August 2017

Risk ratings

July risk ratings and how they compared to June

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 July

Risk ring and overall performance rating



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

Green rated KRIs



Amber rated KRIs



Red rated KRIs



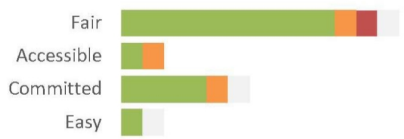
This month we were within tolerance for 19 out of the 20 KRIs we measured. 16 of our KRIs were rated green and 3 of our KRIs were rated amber. One of our KRIs was rated red. In comparison, in June we exceeded tolerance in 2 of our KRIs and in May we exceeded 3 of our tolerances. On average, in each month between February and July, we were within tolerance in 18 of the KRIs we measured and exceeded tolerance in 2.

July v June ratings

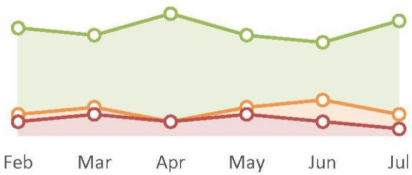
◀▶	13
◀▶	2
◀▶	1
▲	3
▲▼	1
▼	0

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

Performance against our FACE commitments



Distribution of KRI risk ratings between February 2017 and July 2017



Exceptions and key trends

CRM mystery shops - the CRM credit card pilot, which resulted in a number of red-rated mystery shops, has now ceased. CRM savings shops have improved, with 12 out of 70 (17.1%) being red rated in the 3 months to the end of July. Only 3 out of 29 shops were graded 'red' in July. 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.

Advertising breaches and issues - Two material financial promotion breaches were recorded in July and related to in-branch current account leaflets remaining in the public domain after their withdrawal dates. POL have confirmed that the reapprovals 'were' missed' as a result of the impact of the organisational restructure on the Marketing function. This is the third month in a row that there have been such material breaches and, as such, this has been followed up with Post Office.

Branch regulatory knowledge - 2 out of 54 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. There were no red rated branches in July.

Quality of Mortgage Advice - An improvement in 'C' grade cases from 9 to 2 in July and only 1 'D' case, improved the proportion of initial case checks passing QAT file checks, with 95.9% (89%) achieving an 'A' or 'B' grade. The 'D' grade related to advice which was considered unsuitable based on conflicting file notes. The QAT team continue to work with POL to mitigate these errors.

Please note, reporting in relation to a number of new KRIs will commence in September.

◀▶ 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

POL00423693

CONDUCT RISK SCORECARD

		Rating Criteria			Current						
Area	**Measure**	**Green**	**Amber**	**Red**	**Jul-17**	**Jun-17**	**May-17**	**Apr-17**	**Mar-17**	**Feb-17**	**Jan-17**
Complaints	Number of Opened complaints	0-1,000	1,000 - 1,500	1,500 - 2,000	399	395	345	299	314	264	321
	Percentage of upheld complaints	0% - 20%	21% - 30%	31% - 100%	38.3%	50.6%	34.0%	33.7%	36.8%	31.3%	27.5%
	No of FOS cases upheld	0 - 3	4 - 7	8 +	0	0	0	1	0	1	1
Mystery Shopping/VMS	Proportion of shops rated red in the month	0% - 10%	11% - 20%	20% - 100%	20.8%	11.8%	7.0%	5.0%	0.0%	13.0%	20.0%
	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+		1	5	8	7	5	1
Call Monitoring (Travel)	Percentage of red rating calls in the month	0% - 10%	11% - 14%	15% - 100%	25%	42%	40%	24%	19%	20%	15%
Call Monitoring (Life)	Percentage of red rating calls in the month	0% - 10%	11% - 14%	15% - 100%	12%	15%	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%	4.1%	3.5%	3.6%	4.1%	2.9%	2.8%
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%
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%	5.7%	7.6%	4.9%	5.2%	6.1%	4.6%	4.6%
Training & Competence	Percentage of POMS staff completed mandatory training	100% - 95%	95% - 90%	89% - 0%	100%	100%	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	75%	76%	77%	77%	77%	82%	88%
Net Promoter Score (NPS)		35	34-30	>30	41	38	38	38	42	42	40
Financial Promotions	Financial Promotions right 1st Time	50%+	35-49%	-35%	78%	87%	75%	51%	45%	65%	52%
Incidents	Number of Severe Incidents (rated 1 or 2)	0	1	2	12	3	1	1	3	1	1
	Number of unresolved Incidents	0 - 15	16 - 20	20+	13	15	13	17	21	20	14

POL00423693

3.2 Change Risk Update

Author: Jenny Ellwood Sponsor: Angela Van Den Bogerd Meeting date: 13 September 2017 (RCC)

Executive Summary

Context

This report provides an update on the delivery status of the Change Portfolio, the key risk themes under management and the current highest scoring risks, referred to as the 'top risks' within the Change Portfolio.

Questions addressed in this report

- What is the current delivery status of the Change Portfolio and key delivery challenges?
- What are the key risk themes being managed at present and mitigation plans?
- What are the current 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?

Conclusion

1. The current delivery status is Amber and the EUM and Success Factor Programmes are experiencing some significant challenges.
2. The key risk themes we continually push against are: 1) what does the next 12–18 months change activity look like and can we do it all, 2) what is the impact on the network and is it manageable, 3) Why do we continue to underspend and 4) what impact does this have on our benefits profile?
3. In terms of current top risks these are EUM Effectiveness, Delivery of 2017/18 Plan and IT Vendor Renegotiations. Work is underway on the mitigation activities to move these risks to their target risk score position. An approved revised plan and business case for EUM is expected by October, a review of the 2017/2018 change activities is underway with a detailed update scheduled for the Executive Change Group (ECG) by the end of September and work is progressing well with IT Vendor renegotiations with a Letter of Intent with Atos being signed and an agreement secured to proceed with SISD contract changes to reflect a service cost reduction and the transfer of some work in-house.
4. The type and mix of the portfolio remains broadly unchanged in this reporting cycle. Key MI to evidence this is shown within the appendices. The new integrated plan being developed, along with parallel capacity work, is also driving discussions on potential risks and dependencies and progressing well. For this reporting period the Portfolio risks have reduced to 25 and remain consistent with the nature and complexity of the individual projects and the timeline.
5. 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.

Input Sought

The ARC are asked to note the progress made since the last ARC, the top risks being faced, how they are being managed and mitigated and to advise on any additional areas/topics that should also be taken forward.

POL00423693

The Report

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

1. At the end of August 2017, the overall Post Office change portfolio status remained Amber, this is taking into account the individual status of each programme.

2. In terms of the Portfolio delivery status, we are currently reporting Amber. Key delivery challenges include:
   - Capacity: We are currently in the process of assessing (at project level) capacity constrained areas' ability to support all change. The output of this review will be used to reassess the assumptions in the Strategic Plan.
   - 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 ongoing difficulties such that the current migration planned for October/November 2017 (which itself reflected an earlier 3 month's delay) is under threat. A root cause analysis exercise has been undertaken which suggests that issues have arisen with the payroll data load particularly where employee records have needed amendment during the period of upload thereby constraining payroll comparison testing.
   - Ongoing testing capacity: Constraints 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.

What are the key risk themes being managed at present and mitigation plans?

3. In terms of key risk themes, we continually face challenges which are: 1) what does the next 12–18 months change activity look like and can we do it all, 2) what is the impact on the Network and is it manageable, 3) why do we continue to underspend and 4) what impact does this have on our benefits' profile?

4. To address the challenge of what the next 12-18 months looks like and the impact on the Network, an extensive review of the Change Portfolio is underway. This work has been led by the People and Change Director and has included consideration of the impact of change on a number of key areas: IT, Network Operations, HR Service Centre and Finance Service Centre. A full update on activities is shown in paragraphs 14 to 15.

5. Additionally, work continues to try and establish the true impact and requirements to meet the General Data Protection Regulation (GDPR). The programme has recently confirmed that:
   - 17 out of 114 projects that have already gone live were concerned with the use of personal data; and,
   - 45 out of 199 project that are still in-flight have been identified as involving the use of personal data. 20 of these have been classified as 'high priority'.

POL00423693

6. The project team has contacted 13 of the 20 high priority projects to confirm their current lifecycle stage and the extent of the use of personal data. At this stage the true impact of the work required to meet the GDPR is still unclear and clarificatory work continues this month.

7. In terms of the Portfolio cost underspend, which currently stands at 7% at P4, Finance are working closely with the Programme Finance Directors to establish root cause and re-forecasts. Within period 4 we did see the cost spend increasing gradually, however, they still remain significantly under both the original budget and the current re-forecast. The current reason for variances are as follows:
   - Telco (Newcall) costs - are £3m above forecast as the next tranche payment is sooner than anticipated, this is not an underspend, but a timing issue.
   - Network Development (ND) costs - are down IRRELEVANT. ND re-forecast was planned for P5 reporting. P4 costs are in line with the re-forecast.
   - IT & Digital - are down IRRELEVANT on reforecast: i) IT Networks IRRELEVANT, ii) EUC Branch Deployment IRRELEVANT), iii) Risk & Resilience IRRELEVANT), iv) Other IT Projects IRRELEVANT.

8. In terms of benefits we have continued to deliver the total value of benefits anticipated each year. However, this has not necessarily derived from the original Programme projected benefits specified, i.e. some Programmes have delivered more which has compensated for those Programmes that have experienced difficulties. The Change Finance Director is assessing what forum is best to review and regularly challenge both costs and benefits tracking and a proposal is to be made to the People and Change Director this month. Discussions are already underway on the benefits MI we require reporting by each Programme. The approach will be that Programme benefits tracking will be consolidated into a central view via the Finance Directors. A review of the approach taken in each Steering Committees will also be undertaken to ensure it allows an appropriate level of monitoring and challenge.

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

9. There are currently 25 open risks being managed at a Portfolio level, a net reduction of -1 from the last ARC report in July 2017. The current top risks are:
   i) EUM Effectiveness
   ii) Delivery of elements within the 2017/18 Plan
   iii) IT Vendor Renegotiations

10. The EUM programme is continuing to manage a number of challenges that must be overcome to ensure full and effective deployment of the new Horizon system access model. These include the need to obtain accurate data from agents, an ability to communicate training requirements and to enable access to training material to agents, agents' assistants and PO Branch employees, 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.

11. Retail will now take the lead on the deployment phase of the project and work is underway to develop an appropriate and scalable implementation plan. Additionally, an Inflight Review has been undertaken to support Retail and looks

POL00423693

to answer the question on whether we can be confident that the Programme will deliver from where we are now. Recommendations from both the Inflight and the Network Operations Review were presented to the EUM Steering Committee on 5 September and a plan and revised Business Case is now being produced for approval in October.

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 • being unable to collate accurate data from our agents (all of which is being provided by branch staff) • POL staff/agents not having an individual email address which can be used to communicate logins and training information, and • agents not being able to access SuccessFactors via the internet/browser solution and therefore not being able to access training material and test. This all leads to our inability to address the key business goal, which is for POL to prove to its client that persons transacting on its behalf are suitably qualified and vetted.	**16** **I/L** **4:4**	1. Identify gaps within the SF/EUM design – 7 June 17 (all actions) 2. Developing end to end process maps with risks and controls 3. Identifying the key business decisions that still remain outstanding 4. Explore alternative options to meeting the business outcome (i.e. using Horizon for agents' training, building an interface between Horizon and SuccessFactors) 5. GE workshop to make required decisions (decision on Action 4 outputs) 6. To clarify the 'burden of proof' by our FS clients and RMG on how much evidence they require for us to provide on transacting/selling on their behalf 7. Explore with Network the genuine reasons when Dual Login is used and whether this needs to remain or a workaround can be put in place 8. Revised business case and replan 9. Model office and pilot completion 10. Deployment approach proposal to SteerCo	1. Ongoing 2. Ongoing 3. Complete 4. Complete 5. Complete 6. Complete 7. Complete 8. Oct 17 9. Complete 10. Complete	**9** **I/L** **3:3**

12. With regard to IT vendor renegotiations, since the last ARC the Post Office has signed a Letter of Intent with Atos. Agreement has also been secured to proceed with SISD contract changes to reflect a service cost reduction, the transfer of some work in-house. A new Client Executive has also been appointed. Work is underway on reforming ways of working and restructuring the governance framework.

13. Revenue baseline and principles agreed with Fujitsu. Now drafting supporting Memorandum of Understanding for signature by end of September 2017. Ways of working (including behaviours and collaboration) being monitored formally at monthly governance board.

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**	1. Establish Legal support to assist in vendor contract renegotiations 2. Hire negotiation and procurement expertise 3. Contract Managers in place to manage transition and ensure Vendor SLAs and commitment is maintained	1. Complete 2. Complete 3. Ongoing	**9** **I/L** **3:3**

POL00423693

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
			4. Provide support and guidance to Senior Stakeholders (IT & other Business Areas) regarding any high level strategy discussions with any of the impacted Vendors. Short Term Actions: 5. Enforcement of clear relationship management governance on vendors, everything will go through the vendor manager, internal comms to be issued to provide structure around the vendor manager engagement and key contacts 6. Stand up relevant vendor management governance forums 7. Renegotiation of Atos contract (Project Armada) (Atos proposal now approved) 8. Fujitsu (Project Everest) scope obtained with a view to understand ownership of key activities (post in-house move) Long Term Actions: 9. Decision regarding Atos (maintain/exit)	4. Ongoing 5. Ongoing 6. 30 Sept 17 7. 30 Sept 17 8. 30 Sep 17 9. Mar 18 / Sep 18	

14. The People and Change Director hosted a capacity review workshop on 8 August 2017 where all 76 projects within the current change portfolio were presented to the 5 capacity constrained areas (IT, FSC, Retail, Network Ops and HRSC) for an initial impact assessment. A follow up workshop was held on 29 August 2017 at which it was concluded that:
    - IT and Network Operations are the main areas where capacity will cause impact on delivery. Additionally Network Operations, HR Service Centre and Finance Service Centre will require appropriate early engagement from the projects and sufficient lead-in time to uplift resource to accommodate any increased activities;
    - There are still unknowns that will impact ability to deliver e.g. GDPR; and,
    - Recommendations to include need for prioritisation of all projects to make priority calls where capacity constraints exist and ongoing demand management by constrained areas.

15. It is scheduled to present the findings and next steps to GE/ECG on 18 September 2017.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
Delivery of elements of the 2017/18 plan	There is a risk that we will not be able to deliver all of the 2017/18 plan due to multiple capacity constraints.	16 I/L 4:4	Completion of a review to understand the implications of major programmes on a wider range of constrained resources to establish the feasibility of programme delivery.	ECG – Sep 2017	9 I/L 3:3

16. A full list of the 25 portfolio risks is shown as an Appendix.

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

17. At the last ARC meeting there were 26 portfolio level risks. The current total is 25 which, however, has been subject to churn in the intervening period in that 4 risks were closed namely:

POL00423693

- Capacity of IT Key Suppliers: There was a risk that key IT suppliers cannot meet our change demands due to the pace of change and the concurrency of activities resulting in delays to our "Change Portfolio" delivery plans. This was closed on the basis that it was deemed that elements of this risk were captured and managed under another risk ('Complex Portfolio Planning & IT Management'.
- Resourcing Risk (Payroll Legislation): There was a risk that HMRC legislative changes that came into effect in April 2017 could cause significant impact to Change resourcing model and the way that it uses contractor staff. The risk was closed on the basis that it had been managed down to target.
- Unintended consequences on Operational Performance (People): There was a risk that staff departures as a result of change being implemented may impact the effectiveness of the control environment increasing likelihood of new operational risks. The risk was closed through merger with a similar portfolio risk ('Op Performance – Process').
- Delivery (Integrated Plan Delivery Performance): There was a risk that our delivery is all back ended and we hit business with too much change all at once. Closed on the basis of replacement with risk on our ability to deliver the 2017-18 change plan due to multiple capacity constraints.

18. The 3 new risks opened are:
    - GDPR: see paragraphs 5 to 6.
    - Delivery of 2017/18 Plan: see paragraphs 14 to 15.
    - Model Office Testing Capacity/Resilience: The Model Office is designed to test counter releases and services in a live environment. There is a risk that the introduction of new network routers and platforms (HNGA) introduces complexity and additional time as testing needs to cover different branch types, network routers and platforms (HNGX and HNGA). An additional risk is that the Model Office has limited visibility of change projects in the pipeline, which results in an ability to effectively plan and prioritise activities within Model Office. We will monitor the demand from the integrated planning activity and consider the capacity of the Model Office as a constraint during this transition.

19. 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
August 17	0	3	13	9	0	25
July 17	0	3	14	10	0	27
June 17	0	2	15	9	0	26
% of total (current period)	0%	8%	58%	35%	0%	100%
Number of New Risks						4
Number of Emerging Risks						6
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,

POL00423693

Appendix: Change Portfolio risks and supporting metrics

The Portfolio

	Risk Title	May ARC	Jul Arc	Sep ARC	Grid Ranking CURRENT	Grids Ranking TARGET
1	EUM Effectiveness		✓	✓	16	9
2	Delivery of 2017/18 Plan			✓	16	9
3	IT Vendor Renegotiations	✓	✓	✓	16	9
4	Complex Portfolio Planning & IT Management	✓	✓		16	8
5	IT Delivery Capability	✓			16	6
6	Operational Impact of Generic Training Expiry Dates		✓		16	6
7	IT Change Operating Model				12	8
8	Data Risk				12	8
9	GDPR			✓	12	8
10	Financial Risk – Insufficient Funds to deliver Transformation				9	9
11	Transformation Delivery oversubscribed				9	9
12	Unintended consequences on Operational Performance – Process				9	6
13	Availability of Key Skills and Knowledge				9	6
14	Adverse Impact of Change / Organisational Change on Agents				9	6
15	Accounting & Reconciliation				8	8
16	Financial Risk – Benefits/Revenue Realisation				8	6
17	Deployment of Non-Compliant Solutions/Systems				8	4
18	ITNBA Incumbent Supplier Proactive Engagement – BT				9	4

POL00423693

	Risk Title	May ARC	Jul Arc	Sep ARC	Grid Ranking CURRENT	Grids Ranking TARGET
19	Responsible use of public funds				9	1
20	Strategy & Design: Conflict between current BaU and Transformation activities				6	3
21	Reputational Damage - Media risk				6	4
22	Reputational Damage - Political stakeholder risk (local government)				6	4
23	Reputational Damage - Political stakeholder risk (national government)				4	4
24	Poor coordination of communications about change activity with stakeholders and employees				4	4
25	Model Office Testing Capacity / Resilience *NEW*				4	2

POL00423693

The Churn

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



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

Risk Weighting

Each portfolio risk has a weighting score calculated by multiplying their impact/probability scores. When added together this provides a cumulative portfolio score which currently stands at 242.

The overall risk severity score has reduced by around 9% 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.

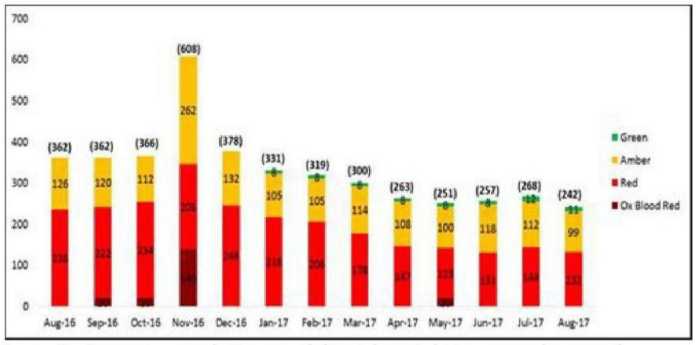


Figure 3: Current cumulative portfolio risk weighting score by month

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

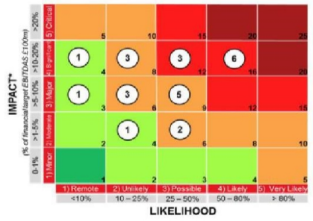


Figure 4: Current portfolio risk weighting (Aug 2017)

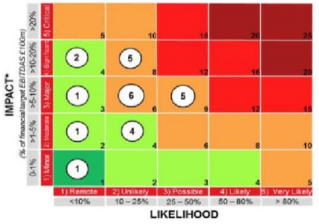


Figure 5: Projected portfolio risk weighting (Feb 2018)

POL00423693

3.3 Financial Crime Risk Update

Author: Sally Smith | Sponsor: Jane MacLeod | Meeting Date: 13th September 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. Regular meetings are being held with HMRC and the HMRC audit action plan is on track. The penalty notice in respect of historic premises registrations has now been received and paid (IRRELEVANT). HMRC are still considering the regulatory position relating to Bill Payments and potential penalty for regulatory breaches relating to Bureau de Change.
2. Risk Assessment work has progressed well and will be 'business as usual' by the end of the current financial year. The Financial Crime Team are to support and deliver workshops to product managers to embed the methodology across the business.
3. Post Office continues to work with HMRC to understand the implications of the new Fit & Proper test regime and for HMRC to clarify their interpretation and guidelines in respect of eKYC and retention of identity documentation.

Input Sought

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

POL00423693

The Report

HMRC Audit status

4. Further meetings have been held with HMRC on the 26th July 2017 and the 23rd August 2017. An updated Bureau de Change action plan was presented by the project team in July, with improved timescales for delivery, and this has been accepted by HMRC and is currently on track:

   - New customer data capture and identification/address verification thresholds and data capture improvements delivered into the Network on 30th August 2017
   - A daily feed of all Bureau de Change activity into a central Post Office data depository, with appropriate tools for rules based exception reports together with the ability to undertake ad-hoc and holistic transaction monitoring is scheduled for delivery at the end of January 2018
   - Subject to procurement timeframes, PEPs and Sanction screening is expected to be delivered by end February 2018 and eKYC by end April 2018.

5. HMRC advised they are considering a penalty in respect of breaches of Regulations 19 and 20:

   - Regulation 20 (Risk Based Approach) – HMRC cited 'behavioural' failures relating to the lack of up to date Bureau de Change risk assessments and processes, and failings in relation to AML/CTF policy documentation (the 2012 version was current until 2016, with no evidence of review).
   - Regulation 19 (Record Keeping) – HMRC cited observation of a lack of knowledge as to where and how data was stored (no data dictionary maintained), there were delays in data provision and that missing transactional and due diligence data was identified during the audit. As such HMRC believe POL was in breach of the requirements to maintain due diligence information for a minimum of five years.
   - The starting penalty is £5,000, although turnover and gross profit are also taken into consideration. Based on financial information provided by the Bureau de Change product team, HMRC estimate a penalty in the region of IRRELEVANT, although they are IRRELEVANT the collaborative and proactive approach by Post Office to date. The financial information provided is still under review by forensic accountants within HMRC, and the pre-penalty notice will not be received until this work is complete, and a decision about Bill Payments is made as this may impact apportionment of costs of premises registration (see point 7. below). These IRRELEVANT per annum and currently all costs are allocated to the Bureau de Change business - if Bill Payments are ruled as in scope for HMRC regulation, this will increase the Bureau de Change gross profit calculation and could increase amount of penalty calculation.

6. HMRC confirmed that whilst there were previous historic failings relating to Staff Training (Regulation 21), they had evidence that throughout the audit Post Office had been continually improving their AML/CTF communication plan to address this. Additionally, in relation to Due Diligence (Regulation 7) breaches, although Post Office was unable to monitor the IRRELEVANT had

POL00423693

been entered into, HMRC had not identified many specific failures. Therefore Post Office will not be fined for breaches to regulations 7 & 21 but are likely to receive a warning.

7. After the meeting un the 26th July 2017, Post Office wrote formally to HMRC in relation to the legal view that it was not directly regulated for Bill Payment services. This is being considered by HMRC as part of a sub-sector review and is still with the HMRC Policy and Legal teams for a decision. Until a decision is reached, HMRC will not audit the Post Office in respect of this activity.

8. The penalty notice relating to historic premises registration issues was received on 10th August 2017 (IRRELEVANT) and has been paid.

Financial Crime Risk Assessment Update

9. The action plan in Appendix A gives full updates, but in summary:

   - Drop and Go, MoneyGram, Gift Cards, Travel Money Card, International Payments and Postal Orders are complete and will be tracked for annual review going forward.
   - Bill Payments work is due to be completed at the end of August and will be issued to the product manager for review and sign-off. The Bureau de Change control strength and residual risk scores are being re-evaluated as the remediation solutions are delivered.
   - Of the remaining products and services, the following approach will be adopted:
     i. Residual risk was last calculated in October 2016 by Thistle Initiatives, this is now being reviewed in line with business changes and controls identified from the high risk re-assessments completed. Current assessment is that there are no high risk products and services remaining that require remediation work, but this will be confirmed at November R&CC once the work is complete.
     ii. Product Manager risk assessment workshops will be rolled out from the end of September 2017 in conjunction with the proposed Product Manager training by Cranfield School of Management – attendees will complete the Product Information Pack for their products and services after these workshops. The Financial Crime Team will check these completed documents against the existing risk assessment, and amend residual risk calculations, as appropriate. These will then be diarised for annual review going forward, along with the 8 high risk products and services.

10. Non-conformance issues in the Network in July and August 2017/18 include 30 incidents identified at 24 branches:
    - 17 branches are on the non-conformance watch list and manually monitored monthly
    - 1 branch has been added this quarter
    - 1 branch has been removed this quarter

11. The volumes of suspicious activity reports (SARs) have reduced by c.20% in July and August and this appears to be in relation to MoneyGram. MoneyGram implemented new identification requirements from 20 June 2017 to meet new requirements under the money laundering regulations and all transactions now

POL00423693

require identification to be presented and recorded. Customers sending or receiving £800 or more have to present ID at the counter and upload an image of their ID direct to MoneyGram via a dedicated upload portal in order for the transaction to be completed. MoneyGram then check these against the details captured at POS before they release the funds. At this stage we are not sure if the reduction is because suspicious activity is being driven elsewhere, or staff fail to be suspicious because they have taken identification. A branch focus article is planned 14 September 2017 to raise awareness of the need to report all suspicions. We will continue to monitor.

Anti-Bribery and Corruption (ABC) Risk Assessment update

12. The following has been completed since the last update in July:
    - ABC policy – being submitted to September 2017 ARC for final approval.
    - Gifts and Hospitality reporting tool launched.
    - ABC training launched 8th September 2017.

AML/CTF training update

13. HR have confirmed that a process has been established to ensure that all new back office staff and contractors complete training within 30 days of joining. Financial Crime Team have established ongoing compliance checks.

14. As at the time of writing there are c. 130 branches that have not completed training as required and the Branch Standards Team are working through appropriate intervention options with the Contracts Team and the Network Team to ensure completion.

POMS MLRO report

15. A report on POMS activity has been produced by the Financial Crime Team and MLRO and is being presented to the September 2017 POMS R&CC and ARC. No material weaknesses have been identified and the governance framework is currently considered to be effective in managing and overseeing the AML risks within the POMS business.

16. From the risk assessment undertaken in April 2017, there were only minor recommendations made and POMS evidenced a clear reporting structure in which financial crime concerns are escalated efficiently to senior management. The policies, procedures, monitoring, controls and both internal and external audits to mitigate exposure to financial crime are in place and communicated effectively to third parties. The risk assessment evidenced that all insurance products within POMS remit were within the risk appetite set by the business.

Regulatory updates

17. eKYC – HMRC advise that they have not reached a decision internally regarding the adequacy of eKYC for customer due diligence and the interpretation issues between themselves and the JMLSG. We understand that a number of organisations are raising queries with HMRC regarding this issue and Post Office is to write formally to HMRC to request response and guidance regarding this issue

18. Fit & Proper test – HMRC is still undertaking internal analysis of the interpretation and application of the requirements, in conjunction with discussions with the top 11 organisations directly regulated by them. Following the meeting on 26th July, Post Office provided to HMRC some detail around the due diligence undertaken at

POL00423693

on-boarding. We are expecting further guidance and clarification by the end of 2017. Post Office have until the date of our next annual registration (1st June 2018) to comply with these new requirements.

19. 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.

External threats

20. There have been no new issues since the July 2017 report.

POL00423693

Appendix A – Action Plan

PROJECT / SPECIFIC TASK	STATUS	COMPLETION DATE	WEEKLY UPDATE
AML/CTF Branch Training Failures Review	In Progress	30/09/2017	01.09.17 Data received from Branch Standards Team confirming the number of individuals who took more than five attempts to pass the AML/CTF training. We are at present reviewing the findings which will be drafted into a high level report.
Risk Assessment Tool	In Progress	30/09/2017	04.09.2017 The tool has been reviewed and its question bank updated to reflect regulation changes. We are also in the process of creating a new portal to make it more user friendly.
RAT Ref 2015/7 - Digital Passport/ Digital Check & Send	In Progress	28/02/2018	04.09.17 Product Owner has confirmed that service will only be available to branches with AEI. The project is currently in design and test stage, and is expected to go live in February 2018. No financial crime concerns at this stage.
Branch Premises Registration Policy & Procedures Review	In Progress	15/09/2017	01.09.17 Updated Policy and Procedures have been drafted and circulated to stakeholders for review.
Santander Business Deposits/Time Saver Deposit Project	In Progress	30/09/2017	01.09.2017 A report setting out the risks and concerns in relation to the existing and proposed service has been created and circulated to stakeholders for comments.
EUM Project	In Progress	30/09/2017	18.08.17 The project team have confirmed that they are looking for potential alternatives or better controls around RUID. They also advised that passwords would be managed at branch level. Financial Crime Team has advised that if passwords are not controlled centrally, there is a potential risk that if a staff member leaves, there ID could be passed on to new members of staff.

POL00423693

PROJECT / SPECIFIC TASK	STATUS	COMPLETION DATE	WEEKLY UPDATE
Bureau de Change Product Information Pack (PIP) Update	In Progress	30/09/2017	31.08.2017 PIP has been updated in line with the changes made to the product. This at present is with the product manager for review.
Postal Orders - Monitoring and Controls	In Progress	30/09/2017	04.09.17 The Financial Crime Team are working with the product manager to review and improve existing monitoring.
JMLIT Section 7 Requests Policy and Procedures Review	In Progress	15/09/2017	18.08.17 Process guide has been drafted and circulated to stakeholders for review
Product and Service Residual Risk Reassessment (From TI Asessment in October 2016)	In Progress	30/09/2017	04.09.2017 A reassessment of previously completed risk assessments is underway to review if generic business changes have changed any of the key risk areas.

POL00423693

3.4.1 IT Controls Update

Author: Rebecca Barker Sponsor: Sharon Gilkes, Rob Houghton Date: 13th September 2017

Executive Summary

Context

The purpose of this paper is to update the RCC on the status of the IT Controls Framework (ITCF); the most recent remediation plans; any emerging issues or developments; and the next steps of the project.

Questions addressed in this paper

1. What is the current status of the ITCF?
2. What are the latest control/remediation results & what does this mean?
3. How will the controls reduce our risks?
4. What are the next steps?

Conclusion

1. Of the 193 controls in the ITCF, 108 are implemented, 64 are partially in place (they do not fully mitigate the risk) and 21 controls are missing. Compared to other IT Control Framework projects, the level of control gap is not unusually large for this stage in the transformation. However, the issues highlight control gaps that would not be expected at similar large and high-profile organisations, and provide a particular challenge for the Post Office as a result of the extensive levels of outsourcing.

2. We are marginally below our forecast of the key controls being implemented. This is because a number of remediation activities are reliant on key programmes including the Security Operations Centre (SOC) and the implementation of the new Service Integrator Target Operating Model. Remediation activities will be implemented as these programmes deliver during 2017/18 and we are adjusting our plan to reflect this.

3. We have reviewed the Manage Security and Manage Security Services RACM and identified a number of controls that will reduce the overall risk severity on the IT Risk Register; we are prioritising these.

4. We have set a target to close the remaining gaps in the ITCF by March 2018. 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.

POL00423693

Input Sought

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

POL00423693

The Report

What is the current status of the ITCF?

1. We are proceeding with the 11 processes in Tranche 1 (Priority 1 – see Appendix 2) included in the original scope of the ITCF. These are currently going through remediation assessment: ensuring that controls owners are being identified and remediation actions are being assigned. Remediation is being monitored by IT Risk Management and KPMG.
2. We have reviewed and have full remediation plans for 4 Processes: Incident Management, Change Management, Manage Security and Manage Security Services.
3. The number of controls has slightly decreased from 215 in July to 193 in August. This is due to consolidation and removal of several controls to better match the control environment with the needs of the Post Office. We have reviewed these controls with the Control Owners and Internal Audit, and actioned their feedback.
4. Of the 193 controls, 108 are implemented, 64 are partially in place (i.e. they address some but not all of the risk), and 21 are currently not in place. For all the controls which are not implemented, we have identified and graded the severity of gaps. This assessment has been refreshed to include likelihood (see Appendix 1 for the new criteria).
5. Out of the 193 controls we have categorised 114 as Key Controls. These have been assessed by the level of risk to the business i.e. "What is keeping us awake at night?" The Key Controls will be remediated as a priority.
6. Following remediation workshops we have identified that the design of 108 controls is implemented. These controls have not been subject to detailed testing and we may identify that the remediation activity is insufficient. Further information on testing can be found below.
7. To enable ongoing monitoring of ITCF and controls self-assessment, we have been developing test scripts for each individual process. This will include sample testing and review of evidence retained as a result of ITCF controls operation. The main purpose of test scripts is to enable testing of controls found to be already in place and overall operating effectiveness of controls as gaps are remediated.
8. We have discussed the requirements for the upload of the RACMs into TrAction with Internal Audit. We have submitted 2 RACMs to the TrAction team, and we are investigating the cost and timescale required to upload the 11 RACMs.
9. Incident Management, Business Continuity and Managed Security Services have the highest number of controls not in place. This is because a number of the controls are reliant on the implementation of the Security Operations Centre (SOC), which is expected to be in place in Q4 and also the delay of the target

POL00423693

operating model with our Service Integrator and staff resource within the Service Delivery team.

What are the latest control/remediation results?

10. The results of August 2017 remediation activities are summarised in the table below

Across 11 processes				
Design of Control	Actuals (%)	no of controls	Actuals on key controls	key controls
Implemented	56%	108	49.12%	56
Partially in place	33%	64	37.72%	43
Not in place	11%	21	13.16%	15
	Total	193		114

All controls

Per RACM	CM	IM	PM	MCAT	MS	MSS	MSA	MSP	MAC	MO	MC
1	5	1	0	3	4	5	4	4	3	17	2
2	2	5	5	8	2	8	2	6	5	7	10
3	6	11	5	9	2	14	4	2	5	2	4
4	1	1	1	1	0	7	2	1	1	2	4
Total	**14**	**18**	**11**	**21**	**8**	**34**	**12**	**13**	**14**	**28**	**20**
Implemented	50%	33%	45%	52%	75%	38%	50%	77%	57%	86%	60%
Partially in place	43%	61%	45%	43%	25%	41%	33%	15%	36%	7%	20%
Not in place	7%	6%	9%	5%	0%	21%	17%	8%	7%	7%	20%

Key controls

Per RACM	CM	IM	PM	MCAT	MS	MSS	MSA	MSP	MAC	MO	MC
1	2	0	0	2	3	3	2	3	0	7	0
2	1	4	4	4	0	8	0	2	2	3	6
3	4	7	3	4	2	11	2	2	4	1	3
4	0	0	0	1	0	6	1	1	1	1	4
Total	**7**	**11**	**7**	**11**	**5**	**28**	**5**	**8**	**7**	**12**	**13**
Implemented	43%	36%	57%	55%	60%	39%	40%	63%	29%	83%	46%
Partially in place	57%	64%	43%	36%	40%	39%	40%	25%	57%	8%	23%
Not in place	0%	0%	0%	9%	0%	21%	20%	13%	14%	8%	31%

	April	May	June	July	August	September	October	November	December	January	February	March
Target (key controls)	45	50	55	60	65	70	75	80	85	90	95	100
Actuals			50.39%	56%	56%							

11. We are marginally below our forecasted target of controls being remediated, because a number of controls owners have been on leave. The August actual remains the same against the July Actual as a result of challenges back from the project and remediation examples not being evident. We expect the actuals to increase rapidly upon implementation of the Security Operations Centre and also when the governance has been restructured to align to the Target Operating Model with our service integrator.

How will the controls reduce our risk?

12. We have reviewed the Manage Security and Manage Security Services RACM and identified a number of controls (see table below) that will reduce the overall risk severity on the IT Risk Register; we are prioritising these.

POL00423693

- Effective Incident Management/Change Management controls would have reduced the overall risk of a Severity 1 incident which occurred on the 30th April 2017 and resulted in lack of connectivity to the live service for multiple branches. In this case, back-end maintenance was not managed via the correct Change Management channels and this resulted in an engineer accidently shutting down the system. If the correct controls had been in place to ensure that all maintenance/ prerequisites/ benign changes were visible to the Service Integrator and Post Office the impact may have been reduced. Human error cannot be prevented but the controls around Incident Management/Change Management would have reduced the overall likelihood and impact.
- Effective Manage Change and Acceptance controls would have reduced the overall risk of an incident which occurred in June which resulted in customers being unable to make Metrobank cheque deposits. The issue was the result of a change that had taken place within the clients' domain which had not been tested correctly. We have several controls with the Manage Change and Acceptance process which will reduce this risk going forward. One of the key controls to support this will be that a model test environment is in place which is representative of current and future production environments. The remediation is currently being identified.

POL00423693

High Risks from the IT Risk Register			Tier 1 Controls from Manage Security Services RACM (part of IT Controls Framework)
Risk Title	**Risk Description**	**Control Remediation/Action Log**	**Tier 1 Controls and Remediation Action**
Vulnerability Testing	Failure by Post Office to ensure there is adequate security to prevent attacks both on the infrastructure and end point across all services that accept, process, store or transmit personal data maintain a secure environment, may lead to legal and regulatory breaches, Resulting in fines/sanctions. financial loss / Service Loss and reputational damage.	**Lenovo BIOS Vulnerabilities R213 -** As a result of recent acknowledgement from Lenovo, it has come to light that a major vulnerability exists with the BIOS of the Lenovo device. The BIOS is built in software that directs the Operating System when starting up the device. There is a Risk unauthorised parties might gain access to Post office information by exploiting this the vulnerability that exist with BIOS. Unauthorised users might take control of the machine and infect the device with malware, disable or bypass security controls in place when the machine is rebooted. It should be noted that the malicious user would need physical access to the device in order to exploit the vulnerability. Which will result in loss of credibility within the Post Office both with Employees, Customers and Governmental Departments as well as financial consequences. At this time POLISAG accept the Risk.	**Control MSS-C1.1** Malware protection tools have been installed on all equipment used for PO business, and updates performed regularly. **Remdiation MSS-C1.1** Malware control is in place. The Control Owner in Micke Ebsworth' team needs the support of CC to run this report biannually. **Control MSS-C2.3** Network filtering mechanisms have been implemented, such as firewalls and intrusion detection software, with appropriate policies to control inbound and outbound traffic. **Gap MSS-C2.3a** There is no monitoring of data centre traffic by PO, and no logs are stored for any intrusions or threats. There is no coordinated communication procedure of attacks across the multiple data centres hosting PO information. **Gap MSS-C2.3c** There is no visibility over how often vulnerability and intrusion scans are performed and the outcomes of such exercises. For example, the logs of security related events are kept by CC, however they are not reviewed on a periodic basis, only if an incident occurs (CC). Additionally, Verizon note that no intrusion software has been implemented currently and they are in discussions with PO regarding this. **Remediation MSS-C2.3a & MSS-C2.3c** MSS-C2.3a We get reports on a monthly basis but not in a timely manner. We also don't have a clear visibility of the remediation that's taking place. There is remediation action taking place now to address this by 30 Oct 2017. Going forward, the control around the process will be reviewed on a monthly basis.
SOC and supporting technology controls (Provision of Security Operations Centre IT Security)	Failure by POL IT to introduce a Security Operations Centre may lead to increased Cyber attacks, lack of enhanced visability, lack of prompt detetion of threats. Resulting in loss of service, financial loss and reputational damage.	**Network Access Control Solution** Hardware assets that are not on the register on the EUC Admin network can access the network via LAN cables at the Post Office sites	**Control MSS-C2.1** Only authorised devices (including Laptops, desktops, Mobiles and Tablets) are given access to corporate information and the enterprise network. **Gap MSS-C2.1a** Network access is partially restricted within PO. However, 1.5 factor authentication in place which means users can only access Office 365 when connected to the PO network externally. **Remediation MSS-C2.1a** All laptops (except BYOD) must have a valid certificate and this process is already in place. Control Owner in Mick Ebsworth's team is in the process of arranging to receive a monthly report from CC demonstrating compliance by 30 Oct 2017. Going forward, the control around the process will be reviewed on a monthly basis. **Control MSS-C7.1** The PO have configured systems and network devices to log suspicious or anomolous behaviour, such as invalid logon attempts, out of hours failed access attempts, network penetration attempts and other security activity. **Gap MSS-C7.1a** Currently no Service Organisation Controls (SOC) in place with third party suppliers. **Remediation MSS-C7.1a** The services are currently completed by 3rd parties providers but not centralised into PO. PO review monthly reports on activities and advise on any incidents and risks. Current work is in progress to centralise this into the SOC Service Organisation Controls by 31 Dec 2017 with monthly reviews to take place after this date.

POL00423693

Next Steps

13. Continue to validate control designs and gaps with control owners and expand control design to include defined control operators and audit trail. Walkthroughs are scheduled to run over the next couple of weeks for the remaining 7 RACMs.
14. Test scripts will be finalised for all 11 processes by the end of September.
15. A workshop has been scheduled for 7th September to plan the operating model for ongoing controls assessment. This will also determine if 3rd party off-shore support is required.
16. Training with control owners will start in October. Following advice from the Finance Controls Project this will be carried out in a staged approach and we estimate will take 3 months to deliver.
17. Self-assessment will commence as the RACMs are rolled out and training is completed with control owners.
18. As an awareness exercise and to provide support to the forthcoming EY Finance Control Audit we will share the ITCF RACMS for Manage Change, Manage Security Services and Manage Operations with EY.
19. Appendix 2 depicts the Tranche Priority processes for the ITCF programme. Priority 2 process controls have not yet been started, these 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 and Human Resources. Gap analysis and remediation is expected to be complete by end January 2018.
20. 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.

POL00423693

Appendix 1

Step 1: Risk Assessment	Confidentiality (C)	Integrity (I)	Availability (A)	Reputational Risk (R)
	Gap impacts the privacy of sensitive data?	Gap impacts the integrity of data?	Gap impacts the availability of systems?	Gap impacts the reputation of IT internally at POL?
	High: private data exposed as a result of the gap	High: Significant volume of important data lost or corrupted by the gap	High: Downtime possible at critical systems or significant downtime of other systems	High: Significant impact on multiple stakeholders
	Medium: commercially sensitive data exposed as a result of the gap	Medium: Some deletion/ corruption may occur as a result of the gap	Medium: Gap does not impact critical systems but may cause outage of less critical systems	Medium: High impact on individual stakeholder or some impact on multiple stakeholders
	Low: no private or commercially sensitive data exposed	Low: no data loss expected	Low: No outage expected	Low: Little impact on internal stakeholders

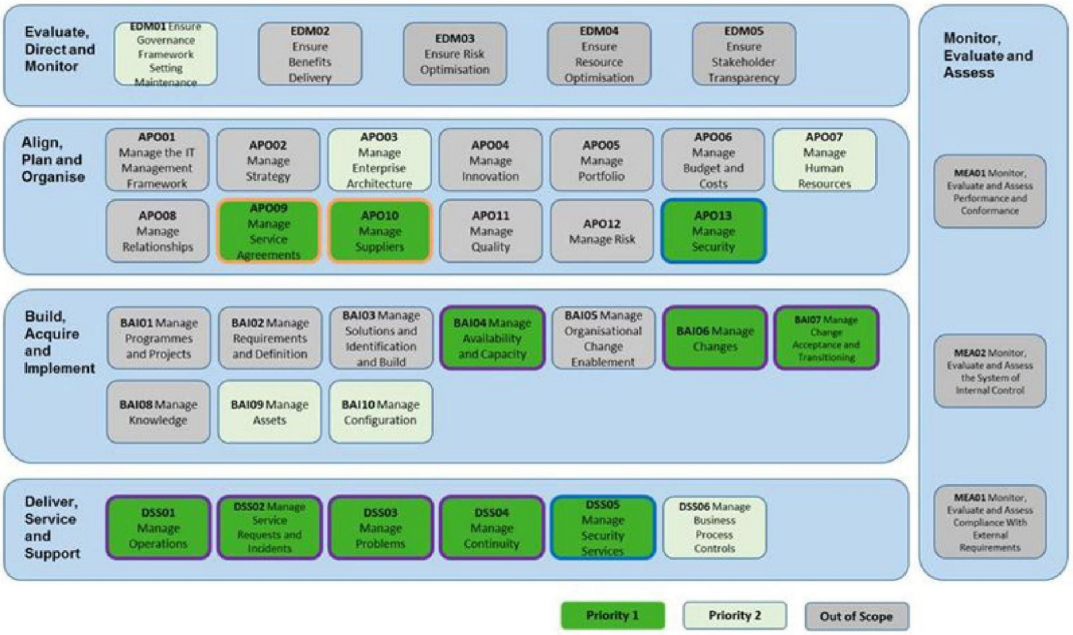
Step 2: Impact Assessment	Impact	Criteria for CIA	Additional Criteria for R	Example rating (CIAR)
	High	One or more high risk Example: HLL	Gap stays at High risk regardless of "R" if one of "CIA" is high. High reputational risk increases the overall impact from medium to high regardless of "CIA" ratings.	HLLL MMLH
	Medium	Two or more medium risk Exapmle: MML	High reputational risk increases the overall CIA impact from low to medium. If reputational risk is medium or low, the impact stays the same.	MMLL LLLH
	Low	Other Example: MLL	If reputational risk is medium or low, the impact stays the same.	MLLM LLML

Step 3: Likelihood	Key	Definition	%
	5	Very Likely	>80%
	4	Likely	50-80%
	3	Possible	25-50%
	2	Unlikely	5-25%
	1	Remote	<5%

Overall Tiering		Likelihood				
		1	*2*	*3*	*4*	*5*
CIAR Impact	*H*	T3	T2	T1	T1	T1
	M	T3	T3	T2	T1	T1
	L	T3	T3	T3	T2	T2

POL00423693

Appendix 2 – ITCF processes by Tranche Priority



POL00423693

POL Disaster Recovery Position

Authors: Mick Mitchell/Rebecca Barker Sponsor: Rob Houghton Meeting date: 13TH September 2017

Executive Summary

Context

In July 2017, the POL Disaster Recovery Position paper outlined the current Disaster Recovery (DR) position within POL and the need to implement a strong DR Policy and Framework which is regularly tested and improved. This paper provides an update on the remedial actions to date.

Questions addressed in this report

1. What is the progress since the last update?
2. What are the next steps?

Conclusion

1. We have carried out a full review of the current state of key services to understand what has been tested and the status of testing that has been carried out to date. We developed a Disaster Recovery Framework and assessed all DR services against it. 29 services are rated Gold, 10 services are Silver and 13 Bronze, based on recovery times required. We are still in the process of reviewing the Silver/ Bronze services but can confirm that 4 are compliant with the DR framework with the rest still to be determined. We have reviewed our DR plans with business and process owners to ensure that these plans align to the needs of the business.

2. We are putting action plans in place to bring non-compliant services into full compliance with the DR framework over the coming months, and will assess the costs involved to support any required contract changes. We will also review and refresh the framework, and further define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

Input Sought

We are asking the RCC to endorse the actions outlined to date and support further reviews of status at future RCC forums.

POL00423693

The Report

What is the progress to date?

1.1 We have carried out a full review of the current state of key services to understand what has been tested and the status of testing that has been carried out to date.

1.2 We have defined a robust DR framework for IT Services which provides clear definition of testing and recovery required.

1.3 Services are categorised by recovery time as as Gold (recovery time 5 hours), Silver (recovery time 24 hours) or Bronze (recovery time 96 hours).

1.4 We have assessed all DR services against the framework and 29 services are rated Gold, from 8 different Suppliers (further detail in Appendix A). Of the remainder, 10 DR services are rated Silver and 13 Bronze. We are still in the process of reviewing these remaining Silver/ Bronze services but can confirm that 4 are compliant with the DR framework with the rest still to be determined. We will prioritise this over the next few months. We have carried out a review with business and process owners to ensure that our IT DR plans align to the Business Continuity planning needs of POL.

1.5 We have implemented improved governance around the process of periodic IT DR testing from our supplier base. In future, the postponement of IT DR tests will only be permitted subject to active challenge and subsequent sign off by IT and business owners.

1.6 We have reviewed the existing IT Service Recovery report that Atos provide and made key amendments that will ensure that POL IT can give more visibility across IT and our business areas.

1.7 We have updated our risk logs to align with the above status.

What are the next steps?

1.8 POL IT will now ensure that we have the actions in place to mitigate any outstanding issues, assess the costs involved to support any required contract changes and schedule tests that have not been scheduled or aligned to contract specifications.

1.9 We will review and refresh the framework, including the need for further definitions of Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

1.10 Gain agreement with the RCC to progress the actions specified above.

1.11 We propose to include a progress update at each RCC going forwards.

POL00423693

Appendix 1. DR Framework – Gold Services Status

Provider	Summary	Service	Test Status	Comment
Fujitsu 8 Gold Services	There has been no formal Data Centre DR test of the Fujitsu environment since May 2013 due to Infrastructure Legacy issues. Component testing has been carried out on most of Fujitsu's platforms. We will initiate a project in Autumn 2017 with the objective of having a full DR test of the Fujitsu environment in 2018.	Network Banking Service (POCA/Vocalink /Santander)	Component test carried out in May 2016	
		Network	Component test carried out in May 2016	
		Debit Card	Last full test verified in May 2013	
		Horizon (Online Processing)	Last full test verified in May 2013	
		PODG	Component test carried out in June 2017	
		MDM	Last full test verified in May 2013.	*Credence & MDM platforms will migrate to a Cloud-based service platform in October 2017*
		Credence	Component test carried out in June 2017	*See MDM note*
		POLSAP	Component test carried out in June 2017	

POL00423693

BT/Verizon 1 Gold Service	The service is currently transferring to Verizon from BT.	Core Branch Network Services	Successful DR Data Centre failover carried out Feb 2017	
Atos 1 Gold Service	Atos provide IT Service Desk services to the Post Office from their two locations in Manilla, Philippines, and their Disaster Recovery Centre in Kuala Lumpur, Malaysia.	IT Service Desk	We are awaiting confirmation from Atos on their last IT Service Desk test but an account DR plan was successfully carried out in March 2017.	
HP 2 Gold Services	HP provide the Post Office with services for their card account product, including two gold services.	Card Account services - Cheque printing	All services have a DR test annually (last known test was July 2017). Currently waiting for a status update on this test.	
		Card Account services - Banking Engine	As above	
Gemalto 1 Gold Service	Gemalto provide Biometric Application, Enrolment and Identification (AEI) services to the Post Office Branch Network.	Biometric Application, Enrolment and Identification (AEI) services	Last DR test May 2017. Some issues identified and actions being put in place to resolve.	
VocaLink 1 Gold Service	Vocalink provides a payment service gateway and is protected as part of the national infrastructure. Routers	Vocalink Payment Services gateway		

POL00423693

	are located in Fujitsu Datacentre. Vocalink switch to alternative datacentres every 3 months as they have active/active Datacentres.			
Accenture 3 Gold Services	Gold Services are Credence (Software), POLSAP (Software), Common Digital Platform (CDP) The CDP service that supports Post Office.co.uk has been classified as a Gold service with a RTO within 5 hours. This is not backed up in the contract (RTO 21.4 hours). Business decision will be required to confirm if this is acceptable and we except this risk or potentially incur costs to reduce the contractual RTO. Meeting will be scheduled in September 2017 with the process, business and service owners.	Credence (software)	Component testing of Credence infrastructure carried out by Fujitsu June 2017	*Credence & MDM platforms will migrate to a Cloud-based service platform in October 2017*
		POLSAP (software)	Component testing of POLSAP infrastructure carried out by Fujitsu June 2017	
		Common Digital Platform (CDP)	CDP platform was successfully tested in October 2016.	*See note in Summary column re RTO.*
Computacenter 12 Gold Services	A full disaster recovery test occurred in June 2017. This exercise successfully recovered in-scope services however there were issues during testing which resulted in some failures, these included Office 365, Skype, SRM, "follow me" printing, ADFS (Active Directory File	DHCP Core Network	June 2017 – see note in Summary column	
		Active Directory	As above	
		Email	As above	
		OneDrive	As above	

POL00423693

	System) and SMTP. All issues have been resolved. Meetings will be held with business owners and Atos in September 2017 to ascertain a suitable date for re-test. Atos recommendation is for a re-test within 6 months. The timing of the re-test should allow Computacenter and all 3rd parties reasonable time to investigate and remediate the root cause of issues identified during the test and facilitate a successful re-test in reasonable timescales.	SharePoint	As above	
		Skype	As above	
		Ricoh Printer Server ("Follow Me Printing")	As above	
		Admin LAN	As above	
		Firewall and DDoS	As above	
		Core Network	As above	
		Wi-Fi	As above	
		VPN	As above	

POL00423693

Financial Reporting Controls

Author: Danielle Goddard Sponsors: Amanda Radford, Al Cameron Date: 13 September 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 (July 2017), current areas of focus, and the progress made on the second phase of the project.

Questions addressed in this report

1. What is the current status of the FRC?
2. What are the latest self-assessment results?
3. How are the current control gaps being addressed?
4. What were the results of the Merlin review and balance sheet review?
5. What progress has been made on the next phase of the FRC, and what are the next steps?

Conclusions

The existing framework has continued to expand (269 controls at end July 2017 from 262 at end May 2017) as we have introduced various new controls. Monthly self-assessment is continuing in the TrAction online self-assessment tool and results are being monitored.

Of the 269 controls at end July 2017, 191 (71%) were issued for self-assessment. 184 (96% of those issued for self-assessment) were operating effectively. Of the remaining 7 controls, 3 were not performed in time but were subsequently confirmed as effective, 1 was not performed effectively but mitigating procedures were reviewed, 2 related to the change in the Fixed Assets control environment which is under review, and 1 was not self-assessed but was later confirmed as effective.

Of the 78 controls not issued for self-assessment at the end of May, 55 were not due to be operated in the period. 13 controls were in remediation, and 10 were yet to be set to live. For the 13 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 excluding Spreadsheets for which we have draft results; the results for the completed areas show that out of 80 controls tested, there were 12 amber exceptions and no red exceptions. The amber exceptions have now been

POL00423693

addressed. The draft results for Spreadsheets testing show that improvement is required (rated as amber); work is already in progress to address this.

The Merlin investigation work is complete; the investigation has identified accounting entries which could relate to missing cash. However, the cause of this potential cash loss could not be confirmed to either be accounting errors following system outages, or the theft of cash.

In response to the Merlin incident a new high risk gap was raised regarding POLSAP journals, which has since been reduced to medium risk. An interim authorisation policy has been implemented and user roles have been reduced to the minimum required. Further work is still being performed to refine and monitor this. The FRC team are working with the Back Office Transformation team to develop the longer-term solution once POLSAP processes are migrated into CFS. A review is also underway over HRSAP access and the control environment over its replacement Success Factors.

The year-end review of Accounts receivable and Accounts payable is complete; testing was performed over the material Receivables and Payables balances as at FY16/17 year end, with a focus on confirming balances had cleared (i.e. receipts or payments) after the year end, and reviewing support for any uncleared items. The review identified a number of adjustments, netting to a debit to the P&L of £65k. With the exception of the Merlin cash centre balance, the adjustments mainly relate to aged balances which are no longer required or supported, which are individually immaterial. Further work is planned to complete balance sheet reconciliation training.

A Masterdata controls analyst and a Finance Service Centre controls analyst (contractors) have now joined the FRC team. A permanent controls analyst has been recruited to start in October 2017, who will perform monthly testing of controls.

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 (July 2017) are summarised in section 2 below.

1.2 The controls framework is expanding and adapting each month. The total number of controls at end July 2017 was 269, up from 262 at end May 2017. The net increase of 7 controls related to the addition of 12 new controls, less 5 removed controls. The 12 new controls were one for each Process owner to

POL00423693

submit periodic conformation that they have reviewed the risks and controls in their process. Of the 5 controls removed, 3 were merged with similar or linked controls, and 2 were no longer relevant (one relating to the closed DB pension plan, and the other relating to an accrual which is no longer required). All control removals are reviewed before being removed from the CSA tool.

1.1. PwC have completed their independent testing of controls (excluding Spreadsheets for which we have draft results) and have provided a 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 report is shown in Appendix 2.

1.2. PwC have provided draft results of their testing over Spreadsheets controls. The control has been rated as amber, with some improvement required in order to refine the controls defined and apply them consistently. The main improvements required relate to change management and approval of changes. Work has already begun to address the detailed action points raised by PwC, including the introduction of a front sheet for each spreadsheet which requires evidence of change management and approval. This is currently being rolled out across the in scope spreadsheets (starting with those that PwC identified as requiring improvement from their sample testing). PwC are developing their comments before providing a formal report on Spreadsheets controls.

1.3. A permanent controls analyst has now been recruited, who will perform monthly cycle testing over all controls. The controls analyst is expected to join the FRC team during October 2017.

1.4. There were 13 open control gaps remaining at end of July 2017 for which workaround controls are in place or remediation is being completed. None are considered high risk; 9 are considered medium risk and 4 low risk. This includes the control gap that was raised in respect of POLSAP journals, which was classified in June 2017 as high risk, but subsequently reduced to medium risk after temporary controls have been implemented. This is further discussed in section 3.

1.5. There were 10 controls to be set to live at end of July 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 by end December 2017.

POL00423693

2. What are the latest self-assessment results?

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

July 2017 - Total controls	**269**	
Less: Controls in remediation	-13	
Controls to be set to live	-10	
Controls not due to be operated due to frequency	-55	
Total population for self-assessment	**191**	**71%**
Self-assessed and operated effectively	184	96%
Self-assessed but not operated effectively	6	3%
No self-assessment submitted	1	1%

2.2. 55 controls were not due to be self-assessed for July 2017, this is because the controls are annual, bi-annual or quarterly controls and did not fall due in the month.

2.3. 3% (6 controls) were initially assessed as not operating effectively; 3 of these were performed late, 2 related to Fixed Asset controls which are being transformed as a result of the recent Fixed Assets review, and 1 was not performed but mitigating procedures were in place. Conversations have also been held with control owners to ensure that the controls are performed effectively and on time for the next self-assessment.

2.4. 1% (1 control) had no self-assessment submitted. We have confirmed with the control owner that the control was performed effectively and there were no issues.

2.5. The August self-assessment is currently being performed and results will be assessed mid-September.

3. How are the current control gaps being addressed?

3.1. There were no high risk control gaps at end July 2017, 9 medium risk gaps, and 4 low risk gaps.

3.2. In June 2017 a high risk control gap was raised regarding lack of authorisation over manual journals in POLSAP. Under the original scope of the FRC, an authorisation process was implemented over CFS journals and it has since been identified that this should be extended to cover POLSAP. Work has been performed to mitigate the risk and the control gap has been reduced to medium.

POL00423693

3.3. Some POLSAP users require access to post manually in order to carry out various transactions (manual file uploads, transaction corrections, cash receipts and cash dispatches, treasury clearing account transactions, and client settlements). There are various controls already 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.

3.4. An authorisation process has now been implemented for POLSAP journals, this was effective from 5 July 2017. 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.

3.5. Manual postings in scope for approval in July were sample checked to ensure authorisation was provided by an appropriate authoriser; a 10% sample check was performed (52 items). Out of the 52 items sampled, 34 items were agreed to approvals sent into the POLSAP Approvals inbox, 17 items were agreed as pre-approved through the normal payment approvals process which we agreed would be out of scope for this separate approvals process. 1 item did not receive approval; this was followed up and retrospective authorisation was received. Sample testing will be extended to ensure there are no further unauthorised journals.

3.6. Separate to this, a POLSAP user access review has been performed to remove access from any users who do not have a critical requirement for access to post manually into POLSAP. This resulted in 54 out of a total of 169 roles being removed. A report is being obtained from Accenture to assess the last transaction dates for these users. The reason for the high number of roles is due to the size of the teams processing transaction corrections, settlements, and cash receipting and despatching. Of the 54 roles removed, 7 were leavers and 8 were Accenture support roles.

3.7. The Back Office Transformation (BOT) project is removing POLSAP and transitioning the processes performed in POLSAP over to CFS. Access to post manual journals in CFS is centralised and restricted to a small number of individuals who have appropriate segregation of duties. The FRC team are working with the BOT team to ensure that the CFS controls are applied to the migrated POLSAP processes where appropriate.

3.8. After the transition into CFS, all manual journals which are not high volume or time critical will be submitted centrally for processing and subject to the normal CFS journal authorisation policy. However, there are some processes where users require access to create a high volume of time critical manual transactions (for example transaction corrections and cash receipting or despatching). For these transactions, there are options which can be used in

POL00423693

CFS including value restrictions on the maximum value a user can transact, and workflow approval based on defined approval limits. We will be defining appropriate controls with the BOT team.

3.9. A review is underway over HRSAP access and the control environment in Success Factors.

4. What were the results of the Merlin review and balance sheet review?

4.1. In the last update to RCC, a review over the Merlin incident and a Balance Sheet review over Debtors and Creditors were underway.

4.2. In response to the Merlin incident, the following investigation work has been performed;

- An investigation was carried out over the financial records held and internal controls in place, in order to identify the cause of the issue. A Deloitte Senior Manager was seconded to the POL Accounting and Governance team to perform this investigation.
- The investigation included review of the relevant debtor accounts, review of the cash transactions carried out by the cash centre manager, walkthrough of cash centre processes, review of cash transactions on the POLSAP outage dates, and review of BACS payments to customers.
- Formal interviews were held with the former employee to understand the causes of the unexplained balance.

4.3. The investigation performed has identified accounting entries which could relate to missing cash. However, the cause of this potential cash loss could not be confirmed to either be accounting errors following system outages, or the theft of cash. The balance is not supported by any physical cash or asset, and has been written off.

4.4. In response to the Merlin incident, the following controls have been implemented;

- An authorisation process over high value manual journals in POLSAP has been implemented and sample tested; refer to sections 3.4 and 3.5 of this paper.
- POLSAP user access has been reviewed and 54 roles have been removed in order to reduce risk; refer to section 3.6 of this paper.
- A control is being introduced to the framework for a bi-annual full cash count at all cash centres. A full cash count was performed of all cash centres in July, the results have been tied back to the relevant POLSAP GL accounts. Some cash in despatch was not counted at the time of the count, but alternative procedures

POL00423693

were performed to trace each of these items in Horizon to the subsequent acceptance by branches. No issues were noted.

4.5. The Balance Sheet review over Debtors and Creditors is now complete. Deloitte secondees were engaged to assist with the review, which focused on testing the material receivables and payables balances as at FY16/17 year end, with a focus on testing the clearing of balances (i.e. receipts or payments) after the year end, and reviewing support for any uncleared items.

4.6. The review identified a number of adjustments, netting to a debit to the P&L of £65k. With the exception of the Merlin cash centre balance, the adjustments mainly relate to aged balances which are no longer required or supported, which are individually immaterial.

4.7. The review also identified a need for balance sheet training in some areas, which we plan to carry out in October and November 2017.

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

5.1. 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.

5.2. We are also re-assessing controls over Network Cash. As per section 4.4 of this paper, a control is being added into the CSA tool for a full cash count to be performed on the FY17/18 year end date, and bi-annually going forwards from FY18/19. The FRC team are developing standard format procedures and documentation for the cash counts.

5.3. Masterdata was added to the scope of the FRC after year end; 3 Masterdata processes have been covered to date and 10 controls are now being self-assessed on a monthly basis. Some control gaps were identified from the initial 3 processes covered, most being due to reliance on manual processes with a lack of monitoring controls. None of the gaps indicate a risk of material misstatement. A new Masterdata controls analyst has now joined the FRC team, with initial priorities being over control gap remediation, Atos, and Payroll (including review of Success Factors).

5.4. 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

POL00423693

well as; the remaining Masterdata work to be performed, other Finance Service Centre controls, and Cash Management and Forecasting controls. A new controls analyst has now joined the FRC team and has started mapping risks and controls over the Finance Service Centre controls including the branch corrections process. Recruitment is underway for an additional controls analyst who will work on the other areas in scope.

POL00423693

Appendix 1 – July 2017 CSA results by process

Controls		Control Gaps				Control Owners		July 2017 CSA Results (submitted August 2017)				
Process	Total controls	Control gaps	H/M/L Impact of GAPS H	M	L	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
Bank & Cash Management	32	0	0	0	0	32	0	29	0	3	0	0
Bill To Cash	19	2	0	1	1	19	0	13	0	4	0	0
Control Environment	21	1	0	1	0	21	0	6	0	4	0	10
Fixed Assets	20	3	0	0	3	20	0	15	0	0	2	0
Payroll	47	1	0	1	0	47	0	42	0	2	2	0
Procure To Pay	28	0	0	0	0	28	0	14	1	12	1	0
Project Accounting	11	1	0	1	0	11	0	5	0	5	0	0
Record To Report	40	3	0	3	0	40	0	29	0	7	1	0
Settlement Process	14	0	0	0	0	14	0	9	0	5	0	0
Stock	7	2	0	2	0	7	0	2	0	3	0	0
Tax	19	0	0	0	0	19	0	12	0	7	0	0
Treasury	11	0	0	0	0	11	0	8	0	3	0	0
	269	**13**	**0**	**9**	**4**	**269**	**0**	**184**	**1**	**55**	**6**	**10**

Strictly Confidential

POL00423693

Appendix 2 – PwC independent assurance results (excluding Spreadsheets)

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.

Strictly Confidential

POL00423693

3.6 Business Continuity & Crisis Management update

Author: Tim Armit Sponsor: Jane MacLeod Meeting date: 13th Sept 2017

Executive Summary

Context

The level of awareness about continuity planning and crisis response continues to increase. In line with ISO Standards methodology Post Office has a strong Management System in place which meets our external requirements but gaps exist across all areas in terms of implementing this system. Priority has been given to customer facing operational areas, Chesterfield and Supply Chain with all other areas within scope but of lower priority currently.

Questions this paper addresses

- How resilient are Post Offices' current business processes, systems and applications?
- What are the next priority areas to be addressed?

Input Sought

The Committee is requested to note the report.

POL00423693

Conclusion

What is the status of business continuity?

1. The last RCC was presented with a high level road map of the status of business continuity and crisis response. This has now been broken down into more detail focussing on:

   - Locations
   - Business Functions
   - IT Systems

2. There are 21 identified key sites, mainly Supply Chain CVIT locations. Each of these is being visited and the site leaders worked with to agree crisis response and contingency options. A summary of the sites visited so far, high level findings and next steps is shown in the appendix below, this is ongoing work. Other keys sites such as Chesterfield have undergone a relocation exercise which proved the capability of teams to work in the recovery site successfully. On August 25th Finsbury Dials tested its capability to work at home with no issues raised and everyone able to work simultaneously remotely.

3. More detailed work on impacts and risks is required and this is ongoing. Until we understand the impact of each business area, location and system not being operational we cannot confirm if our recovery capabilities meet our needs. Additionally if we do not clearly understand the risks inherent within our operational environments we can't confirm we are planning to mitigate for them. Each site, system and business line will be analysed and reported on, this will be complete by June 2018. To get to this position each business area and location will be analysed for the impact it would suffer during an interruption to determine at what point this impact becomes intolerable. Each location will have the risks analysed and recovery strategies for all areas agreed. Priorities will be Supply Chain, Chesterfield, IT systems. Then Banking Framework, Bolton, Finsbury Dials. All other business areas will then follow.

4. IT Systems are being assessed for impact in conjunction with the IT Department. IT are to report back to RCC on the impact of the loss of key operational systems and business continuity are working with them to assess the impact of systems failures across POL. Detail on this will be in the IT report.

5. Given the dependency on IT systems which is currently being addressed, the review of each business function will be undertaken following the IT review. It is planned to have plans for all business functions in place by June 2018. Banking Framework and other key areas are being worked with but more focus on business areas will be taken in 2018 in the priority order shown above.

POL00423693

6. A spreadsheet listing all three key areas has been produced and every key point is assessed against the key elements of the ISO standard to measure progress, these are:

- Impact Analysis
- Risk Analysis
- Recovery Strategies
- Crisis Plans
- Business Continuity Plans
- Testing and Awareness

There are other components including supply chain analysis and plans for branches that will be included once the basic levels are all in place.

Industrial Action

7. There is a risk that Royal Mail may have industrial action later in 2017. Business Continuity have worked across Post Office to identify all the points of contact between Royal Mail and Post Office. Business Continuity have met with a large cross section of Royal Mail managers to discuss the risk of Industrial Action and what mitigation and contingencies are in place and can be put in place. This is ongoing with future meetings planned. It is thought unlikely that any industrial action will happen before the end of October and it cannot legally happen for at least 5 weeks.

POL00423693

Appendix 1
Status of progress

Action	*Update*	*Owner*	*Target Date*
Further training and education for the Business Protection Team including improvement of the procedure to invoke the Business Protection Team	Initial changes made to invocation in place. Workshop planned for September	Tim Armit	9/17
The IT DR capabilities and subsequent impact on the business need defining and plans considered.	Impact of system failure report first draft published for review	Mick Mitchell Tim Armit	9/17
The Industrial Action plans needs to be reviewed in light of current risks.	Internal POL meeting held and two Royal Mail meetings held to determine needs and plans. POL requirements will feed to the RM plans to ensure we know gaps and planned responses.	Mark Siviter / Tim Armit	10/17
Development and implementation of a recovery strategy for Bolton	Cost for Sungard solution agreed and budget, meeting with Bolton lead team to agree solution being planned for September.	Joe Conor / Tim Armit	10/17
Home working as a mitigator for a potential failure of Finsbury Dials needs to be tested and proved	Test run in August. Complete success with no issues. Plan to run this as an annual exercise going forward. Further work with IT on security and skype.	Tim Armit / Mick Mitchell	1/18
Stay Calm manual needs to be simplified and training provided as to its use	Training across Supply Chain depots underway. Agreement to restructure in place with key users within Supply Chain. Review of documentation complete. Draft new approach out for pilot now, once approach agreed new approach to be rolled out in October. Restructured document in place by year end.	Tim Armit / Marcia Bourne	12/17
Resilience levels across all key locations and facilities needs to be tested, improvements identified and implemented.	Chesterfield solution in place and approach to PC's being reviewed for improvement by IT. Finsbury Dial home working proven in a controlled manner and more realistic exercises will develop from this. Supply Chain solutions being reviewed. The levels of resilience will continue to be reviewed whilst plans and strategies are developed across all areas led by Tim Armit but owned by each business lead. This will take until June 2018	Paula Jenner / Tim Armit / Russell Hancock /	6/18

POL00423693

Action	*Update*	*Owner*	*Target Date*
Supply Chain Sites Visited: Aberdeen / Glasgow / Belfast / Norwich / Sheffield / Birmingham / Hemel Hempstead (at Norwich) / Swansea (at Birmingham)	Key initial findings include: • No confirmed or tested continuity locations for depots • No plans for large loss of vehicles • Clarification on crisis escalation and central crisis response needed These and other initial findings have been reported to Supply Chain leadership for them to resolve. Once all visits are complete timescales for resolution will be agreed with Supply Chain management and a method to track these implemented. The reviews are also uncovering some opportunities to review standard methods of operation. Once all issues identified are resolved the sites will show as green with respect their continuity capability. It is anticipated this will be complete by March 2018.	*Russell Hancock / Tim Armit*	*12/17*

POL00423693

POST OFFICE
RISK AND COMPLIANCE COMMITTEE

Annual Report and Accounts 2016/17

Executive Declaration, Top Risks and Risk Section for ARA

Author: Richard Williams/Deana Herley Sponsor: Jane MacLeod Meeting date: 13 September 2017

Executive Summary

Context

The purpose of this paper is to share the updates to the top risks and Executive Declaration results since the RCC in May, and to review the updated Executive Declaration and risk statements in the Annual Report and Accounts (ARA).

The Top Risks (where red means a rating greater than 3:4 / 4:3) is a summary based on feedback from all GE members and is a consolidated view across the POL business. In a number of cases, the scoring is based on factual incidents which have occurred.

The Executive Declaration process enables Group Executive (GE) members to consider (and attest twice yearly) as a part of year-end procedures, if any additional disclosures are required to the principal risks to be included in our ARA. The approach to disclosure as set out in appendices 2 and 3 was collectively agreed by RCC on 4 May 2017.

Our principal risks form a part of the Governance statement in the ARA (see Appendix 5). These are drafted based on the position of top risks agreed by Group Executive members and are supported by the Executive Declaration process.

Questions this paper addresses

1. What is the current profile of our top risks?
2. Why have we re-run the Executive Declaration?
3. What are the results of the re-run?
4. Are the Principal Risks as mapped in Appendix 5 the correct risks for inclusion in the ARA, with descriptions of those risks appropriate?

Conclusion

1. Since May 17, changes to the Top Risks (see Appendix 1) have included the following;
   - We have 13 'Top Risks' (up from 11 in May). Overall our red risk profile has remained stable due to the aggregated score parity in overall risk movement.
   - There are 4 new risks (defined as red rated risks having a score >12) which have been identified by Finance and Operations through the Placemat "top down" exercise, 3 being impacting ability to trade covering a) POLSAP replacement (5/3), b) Agents Pay IT (4/3) and c) Replacement of SAP HR (4/3) and a further risk covering cash risk (3/4).
   - 3 increasing risks relating to impacting ability to trade (5/4 from 4/4), retail proposition (4/4 from 4/3) and industrial action (4/4 from 4/3).

POL00423693

- 1 risk, government funding, is no longer deemed a top risk due to agreement with government to a Network Subsidy Payment to 2020/21 and continued investment over the period.
- 1 risk, IT delivery capability has reduced from a 4/4 to a 3/3 due to recent hires, including CTO and approved IT People Strategy. IT Demand Management will be insourced from Atos as of 4 September, enabling POL to better control the demand pipeline.
- The people capability and capacity risk has been considered and its rating deemed acceptable by management, following the challenge from May ARC, regarding impact of cost reductions with an outcome. We had c.90 reported vacancies as a result of OSOP and there are now 7 remaining, with steps being taken to reduce these gaps.
- All other risks have remained unchanged.

2. In May, we completed the Executive Declaration exercise to support GE members in considering (and attesting), if any additional disclosures were required in our Annual Report, as part of our year-end procedures (Appendices 2 and 3). This exercise has been rerun in August / September to consider changes, due to delays in ARA sign off. By doing this now, albeit slightly earlier than usual, we propose to use the results to replace the half year exercise in September / October, which would be the usual timeframe.

3. The results from May have been reviewed and updated with GE to give an updated position (Appendix 4). Since May, changes to the Executive Declaration are as follows:
   - 4 items have been removed due to no longer being of material significance:
     1. Card payment rules are evolving and the cost of processing is rising. Lower than forecasted impact due fewer card sales.
     2. £950m Working Capital Facility. Initiatives in place to ensure efficient use of our working capital.
     3. Net liabilities provision. Various reviews have been completed considering how we increase net asset provision.
     4. Uncertainty over future investment from HMG. Agreement with government to a Network Subsidy Payment to 2020/21 and continued investment over the period.
   - 5 new items (3, 7, 8, 9 and 15), 3 relating to fraud losses, 1 relating to IT Disaster Recovery and 1 relating to Teleco Amortisation.
   - 1 item (11) New Money Laundering Regulations have increased in potential materiality, with the outcome dependent on consultation with HMRC over agent scope.
   - 4 items (5, 10, 12 and 17) have decreased in materiality, due to actions taken to reduce exposure.
   - 7 items have (1, 2, 4, 6, 13, 14 and 16) have remained unchanged.
   - There are no items of material significance that require specific disclosure in the ARA. 11 items will be disclosed generically in the risk section of the ARA, as summarised in Appendix 5.

4. The draft principal risks set out in appendix 5 are those which will appear in the ARA and have been drafted based on the position of top risks (Appendix 1) and are supported by the Executive Declaration results (refer to Appendix 4).

POL00423693

Input Sought

The Committee is asked to review the information provided and:

a. Consider the proposed changes to our top risks;
b. Note the Executive Declaration results;
c. Agree draft principal risks as set out in Appendix 5, for inclusion in the ARA 2016/17; and
d. Consider whether there are any other matters that should be included and reported against.

POL00423693

Appendix 2 – Materiality

- The items listed in the table below are possible "material" issues or concerns which have been raised by Executive members for consideration for disclosure.
- Materiality has been defined for the purpose of this exercise as, *"qualitatively and/ or quantitatively, as a cut-off point above which something takes on a greater significance and may require a different course of action"*.
- In deciding how to recognise an item as material, Group Executive members are asked to assess whether it is something that is of a size or impact that would make a difference to the Post Office or our stakeholders, e.g. influence our decision making, cause us significant cost or reputational and/ or regulatory damage.
- Defined tipping points of materiality used to assess significance where defined, are listed below:

Items	Tipping Point
Risks	See Harm Table
Frauds, irregularities or losses	£50k or above, which could attract media attention, are systemic/ multiples or have a Network wide impact.
Material contracts	Contracts over £5m or cause significant impact/ harm to the business if they were to go wrong.
Events	Size or impact would make a difference to Post Office or stakeholders.

POST OFFICE

HARM TABLE - MEAUREMENT CRITERIA

Version: 18th Feb 2016, post RCC & ARC

Use EBITDAS target of £100m

Risk Scoring	Impact on*				Likelihood of*	
	Label	Financial** (EDITDAS)	Operational Continuity (Operations, IT, Colleagues)	Reputational (Stakeholder, Customer, Colleagues, Third Party, Media, Regulator)	Label	Probability
5	Critical	>20% of financial target or significant impact on all objectives	National service disruption/ significant location/s or business function/s for >3 days	- withdrawal of stakeholder/ customers/ colleagues/ 3rd party support, or - extensive national media coverage, or - formal regulatory intervention	Very Likely	>80%
4	Significant	>10-20% of financial target or significant impact on all objectives	National service disruption/ significant location/s or business function/s for <3 days	- significant challenge from stakeholder/ customers/ colleagues/ 3rd party support, or - some national media coverage, or - formal regulatory investigation	Likely	>50-80%
3	Major	>5-10% of financial target or significant impact on all objectives	Regional service disruption/ major location/s or major business function/s for <3 days	- major questioning from stakeholder/ customers/ colleagues/ 3rd party support, or - extensive local media coverage, or - informal regulatory enquiry	Possible	>25-50%
2	Moderate	>1-5% of financial target or significant impact on all objectives	Local service disruption at several locations or business functions for >3 days	- moderate concern from stakeholder/ customers/ colleagues/ 3rd party support, or - some local media coverage, or - informal regulatory conversations	Unlikely	>10-25%
1	Minor	0-1% of financial target or significant impact on all objectives	Local service disruption at several locations or business functions for <3 days	- neglible interest from stakeholder/ customers/ colleagues/ 3rd party support, or - no media coverage, or - no regulatory interest	Remote	0-10%

POL00423693

Appendix 3: Executive Declaration

EXECUTIVES' DECLARATION STATEMENT 2016/17
Twice annually for governance and reporting purposes each Executive is required to attest to the ARC the items listed below

Declaration:	
Based on my knowledge of the business, and particularly the areas that report to me, and following due enquiries, I declare that for the period **1 April to 31 March 2017**, I have disclosed any **known material items** (if not already disclosed at the half-year) and where I have not disclosed already, I have included details under the items below:	
1)	material **risks** to Post Office that are not captured in the Group Risk Profile
2)	material breakdowns of internal control, breaches or significant non-compliance with internal and external guidelines, including of the **General Control Framework** and **policies** that I am accountable for
3)	material **frauds**, **irregularities or losses** that have come to light, whether carried out by our staff, agents, contractors, suppliers or partners
4)	complex or subjective **accounting judgements**, **estimates and revenue transactions***
5)	changes to **accounting policy***
6)	**provisions or exceptional items** *
7)	**liabilities and contingencies**, including those associated with guarantees*
8)	**legal action** being taken by or against Post Office*
9)	any **legislative**, **regulatory** (including any **non-conformances with Money Laundering Regulations**) **or contractual compliance issues** that have come to light*

POL00423693

10) material **new contracts or extensions** entered into, **direct awards** and where I have not followed the **contract process**
11) **obligation breaches** on **contracts** that I am sponsor for*
12) direct or indirect **personal interest** in any transaction, arrangement or related agreements with parties entered into*
13) **gifts and hospitality** which have not been approved and registered in accordance with policy*
14) material events that could **crystallise** before the end of the reporting period above
15) any **other information** that could have a material impact on the period (indicated above).
**a requirement to disclose all not just material*

The information I have given above is true, complete and accurate to the best of my knowledge, information and belief.	
Name:	
Role:	
Signature:	
Date:	

POL00423693

Appendix 5: Draft Principal Risks (Mapped)

Draft Principal Risks	Top Risks	Executives Declaration
Competitiveness Post Office faces both opportunities for and threats to income from our competitive market place. These include: • Responding quickly to new entrants, and current competitors with new products and technologies, different strategies and business models, • Fulfilling customer expectations through digital channels new products and improved back office functions Successfully aligning strategy with partners and managing dependencies on third parties	[11/12] Market Developments / Competition (Retail, Financial Services and Telecoms) [15] Digital Competency	[16] Banking Framework
Retail Proposition We may not be able to retain, or attract sufficient retail partners to manage our new network of over 11,500.	[13] Retail Proposition	
Cyber threat Post Office is dependent on the continued availability of its information systems and associated infrastructure. These could be threatened, by - internal weaknesses, external events or cyber-attack.	[5] Cyber Threat / Information Protection	
IT impacting ability to trade The next phase of IT Transformation will have increased dependencies and interconnectivities as we replace legacy systems and implement a new integrated service. This could impact service delivery and continuity of IT services.	[1,2,3,6] IT Impacting Ability to Trade	[2] National Stock Centre Swindon [3] ITDR [4] Cyber Threat [5] Telecoms cyber attack
Industrial Action There are a number of commercial process dependencies supplied by and to Royal Mail Group (RMG). The risk of industrial action affecting such a key partner could lead to material disruption to Post Office through loss of service to customers, Postmasters, and business partners. It may also cause Post Office to fail to meet financial service regulatory requirements.	[14] Royal Mail Industrial Action	
Compliance Post Office operates under an extensive regulatory environment, covering areas such as financial and postal services, telecoms, procurement, competition law and data security. This environment continues to evolve, particularly in the financial services and telecoms areas, and we need to ensure that the changing requirements continue to be identified and met. Changes to regulation could also impact our ability to meet targets and goals.	[7] Conduct Risk [8] Increase in Regulation	[1] Non-compliance with PCR [10] AML regulatory duties for POL [11] Adherence to new AML regulations [12] Vetting [13] HMRC fine on registration of premises [14] Commercial risk from OFCOM intervention

* The following items are not reflected in the ARA Principal Risks for consideration;
Top Risks: [10] Cash Risk.
Exec Declaration: [6] Reconciliation issues between POL and MoneyGram, [7] P739 Fraud, [8] Parcelforce reversals, [9] Losses, [15] Telecoms Amortisation, [17] IT Controls Framework.

POL00423693

4.1. Executives' Declaration and Risk Section for ARA

APPENDIX 1

POL Top Risks as at 06/09/17

Principal Risks		GE Owner	Risk No	Top Risks Description & Comments	Score (I/L)		Rank		Change
					May-17	Sep-17	May-17	Sep-17	△
OPERATIONAL	Managing change	AC	1	**Replacement of POLSAP** We have to replace POLSAP or shore it up, creating existential risks. **Comments** The Back Office programme will migrate POL SAP to CFS. The scope covers a number of processes which drive our financials e.g. client settlements. A controls contractor is now embedded within the Programme to oversee migration. POL SAP balances, access profiles (baseline and process) and financial reporting controls will be formally signed off by the Financial Controller and the Financial Accounting and Governance Manager before migration. If POL SAP is not replaced it will be out of support. The existential risks could result in a misstatement of the numbers.		5 - 3		2	New
			2	**Agents Pay IT** We have to deliver agents pay via CFS. **Comments** The ART project will be live by Feb 2018. Pre-prod dual running Nov and Dec. Prod dual run in Jan. Full calculation in the new model only by Feb 2018.		4 - 3		J4	New
			3	**Replacement of SAP HR** We have to deliver payroll via SF, building on a fragile HRSC. **Comments** Success Factors Programme is replacing a number of services currently provided through HR POLSAP and the Back Office Transformation programme is working on the POLSAP Process Migration, with a current view that this will be live by June 2018. This will allow us to de-commission POLSAP by September 2018. Data archiving and residency of POLSAP is being investigated.		4 - 3		J4	New
TECH	Technology Ops	RH	4	**IT Delivery Capability** Unable to deliver in line with our Transformation cost, benefit and delivery plans due to lack of strength in POL technical leadership capability, lack of continuity of key people in key roles, and/ or IT Change Programmes designed and configured around high risk single event implementations. Resulting in change either not being delivered at all or taking longer, costing more, delivering less with eroded benefits. **Comments** Permanent CTO starts on 4th September. CEO & CFO approved IT People Strategy recruitment at QBR on 23rd August. This strategy will deliver permanent technical leadership, change and engineering capability to POL. IT Demand Management will be insourced from Atos as of 4th September, enabling POL to control the Demand Pipeline. Major new change programmes are being set up as Agile to reduce elapsed time from concept to production. Recommend Risk score adjusted to 3-3.	4 - 4	3 - 3	J2	n/a	▽
	IT Security	RH	5	**Cyber Threat / Information Protection** We have critical IT Security exposures highlighted by a third party (Deloitte) review across our security infrastructure. These relate to firewalls, pen testing and out of date infrastructure. We have mobilised a Security Transformation programme to mitigate this risk. Failure to adequately deploy and effectively manage data protection policies, standards and controls within the business and our partners/ suppliers, results in a breach of company data (colleague/ customer) **Comments** Security Operations Centre will be established in the over the next 6 to 9 months, providing oversight of all security controls from each provider, centralise and aggregate events and incidents to enable POL to react against security issues efficiently and effectively, thereby reducing our risk exposure.	4 - 3	4 - 3	J3	J4	◁▷
	Dependence on IT 3rd Parties	RH	6	**IT Impacting Ability to Trade** There are a number of our 3rd party suppliers which are supporting critical components in our IT Estate. The components have either reached the end of life or there is no back-up capability and could cause significant impact to the business if it fails. This risk is heightened against some of the Fujitsu infrastructure components due to the recent contract extension that only supports the restoration of service to some out of support components by "best endeavours". Work is underway to remediate where possible until platforms are modernised. **Comments** We have infrastructure programmes underway to mitigate this risk (HDCR, Back Office Transformation and Branch/Network rollout). In addition we are delivering the POL DR Framework, which will ensure service recovery schedules and recovery points that meet business need, that regular DR tests are carried out, and any actions arising are completed. Recommend status changes to 5-4.	4 - 4	5 - 4	J2	1	△
LEGAL & REGULATORY	Compliance with laws and regulations	JMaC	7	**Conduct risk** There is a risk of non-compliance including conduct requirements for mis-selling, non-compliant marketing, sales product or distribution.	4 - 3	4 - 3	J3	J4	◁▷
			8	**Increase in Regulation** There is a risk that the on-going increase in regulation, for example, AML (Enhanced Fit & Proper requirements for AML, SMR etc) ,FS, (Insurance Distribution Directive Requirements) and Telecoms businesses, increases the risk of non-compliance and/or making various business activities unprofitable.	4 - 3	4 - 3	J3	J4	◁▷
FINANCIAL	Sufficient cash / headroom	AC	9	**Government Funding and Headroom** Delays in agreeing the remainder of the requested funding results in deferral of investment plans and consequential delays in implementation of strategy.	5 - 3	n/a	1	n/a	▽
			10	**Cash risk** We are using too much cash, risking loss, funding costs and change funding **Comments** A project team is reviewing cash management in its entirety focusing on forecast completeness and inaccuracies. The 'cash declaration' element of the project is critical as without it being right the team will not know what should be in branch. Additional resource in post will look to improve the customer experience of getting cash out and will also be tackling excess cash to reduce fraud / losses. Separately the Forex experience is being reviewed. Projects are scheduled to complete by year end.		3 - 4		J4	New
STRATEGY	Competitiveness	ME/NK /KG	11	**Market Developments/ Competition (Retail: Mails & Govt Services)** Unable to respond quickly enough to new entrants with different strategies/ business models, current competitors with new products/ technologies, who take market share and/ or profitability. As a result our customer experience, propositions and channel strategy fail to deliver what customers want.	4 - 4	4 - 4	J2	J3	◁▷
			12	**Market Developments/ Competition (Financial Services & Telecoms)** The existing business model is sub optimal. We are unable to respond quickly enough to new entrants with different strategies/ business models, and/ or current competitors with new products/ technologies, who take market share and/ or profitability. We do not resolve business dependencies on third parties particularly with aligning our strategy with BoI. As a result our customer experience, propositions and channel strategy fail to deliver what customers want.	4 - 3	4 - 3	J3	J4	◁▷
	Market	AC/KG	13	**Retail Proposition** Unable to retain and or/find sufficient new retail partners because of the complexity and controls of the current proposition and value to the retailer, which leads to a decline in network numbers below 11,500 **Comments** Projects to mitigate include: simplification, extension of automation to agency branches, white space branches and new retain value proposition to multiple partners.	4 - 3	4 - 4	J3	J3	△
	Customer Relevance	KG	14	**Royal Mail Industrial Action** Because there are a number of Post Office commercial processes dependent on services supplied by and to RM there is a risk that a major crisis or industrial action affecting Royal Mail could disrupt or terminate those services resulting in loss of service to Post Office customers and Postmasters. **Comments** The risk of action is high and will remain high over the next 12 weeks as the whole process of negotiation is worked through. It is very unlikely that the CWU will withdraw from balloting their members and RMG have a poor track record of winning. So the likelihood is a successful ballot for action which provides a mandate for the CWU to get the best deal they can or strike. RM will use casual staff and managers to make collections from Post Offices.	4 - 3	4 - 4	J3	J3	△
		ME/NK /KG	15	**Digital Competency** Lack of digital competency to spot and implement quickly enough (e.g. new products, customer journey, back office).	3 - 4	3 - 4	J4	J4	◁▷

POL00423693

4.1. Executives' Declaration and Risk Section for ARA

APPENDIX 4

Executive Declaration as at 06/09/17

	Principal Risks	Statement	Item No	Item	Identified by GE Member	Change Δ
OPERATIONAL	Procure and contracts	Material new contracts or extensions entered into, direct awards and where I have not followed the contract process.	1	Non-compliance with PCR. Over the past year and prior to this, POL has entered into a number of contracts and/or contract extensions that have been direct awards and not compliant with PCR these incidents are generally low risk and with a commercial imperative. New controls have been introduced to record incidents or exceptions going forward. This will bring greater clarity over level of non-compliance with PCR.	Jane MacLeod / Mark Davies / Nicholas Kennett	◁▷
TECH	Business Interruption (ITDR)	Material risks to Post Office that are not captured in the Group Risk Profile.	2	National Stock Centre Swindon. We have one national stock centre in Swindon which is the only location from which we serve the branch network with stamps and other stock items. The IT is considerably aged and back up requires manual transportation of tapes to an off-site location. There is currently activity under the Back Office Transformation to scope an IT solution for Swindon however a significant failure in the meantime would require manual contingencies to be implemented; these are more labour intensive, increasing cost and potentially slowing service.	Alisdair Cameron	◁▷
			3	IT Disaster Recovery. POL IT have identified that a number of systems haven't fully completed DR tests for a period of time. We have reviewed the current DR position to understand gaps and mitigation plans; reviewed DR plans with business and process owners to ensure they are aligned with Business Continuity planning; and strengthened the governance around DR.	Rob Houghton	△ New
	IT Security		4	Cyber Threat. There are a number of Cyber Threat risks which are now managed by IT. We have several risks on the IT register that relate to firewalls, pen testing, applications not supported effectively (i.e. Firefox and Chrome) within the EUC. As the team develops the risks will be mitigated and managed to an acceptable level, one of the key actions for the team is to set up the Security Operations Centre which is expected to be live by the end of 2017.	Rob Houghton	◁▷
		Any legislative, regulatory or contractual compliance issues that have come to light.	5	Telecoms cyber-attack. Post Office Broadband business and c.108 thousand customers suffered a cyber-attack (DDOS or "BOT" attack) at the end of November 2016. This was part of a global attack. This led to customer either being denied service or having service speeds significantly reduced for a period of 3-6 days. A fix was quickly implemented but additional contact centre costs for extended hours were incurred (c £100,000). Minimal customer claims were made (338 for £1,500 in total). The attack was reported to the Post Office RCC & ARC.	Nicholas Kennett	▽
LEGAL & REGULATORY	Managing losses and Fraud	Material risks to Post Office that are not captured in the Group Risk Profile.	6	Reconciliation issues due to timeouts occurring between POL and MoneyGram. These could lead to write-offs as there will be differences between MoneyGram and POL figures. There are meetings scheduled in September to finalise the position, the worst case scenario is that POL will have to write off [IRRELEVANT]	Nicholas Kennett	◁▷
		Material frauds, irregularities or losses that have come to light, whether carried out by our staff, agents, contractors, suppliers or partners.	7	We believe 3 branches have been fraudulently claiming for P739s. This is likely to have been going on since 2012 (separation), but because the volume and values are low it has escaped detection. We know there is an issue because even our largest P739 branches do not often process more than 100 items a week (a very small number of the total 600 odd branches have this volume). Last week one of the offending branches posted volumes of 4000. Security are involved. The issue is that Horizon requires manual entry of the quantity and the limit is set at 99999. We are changing the limit on the field in Horizon to a much lower number and am speaking with RM about other longer term potential solutions. We are not sure yet of the fraud value as we are still looking into old data sets but the product volumes and values are relatively low although the frequency and duration still need to be confirmed. Last year we did volumes of 2.1m @ an income of [IRRELEVANT] per item [IRRELEVANT] into RM revenue associated with the product) and pay agents Mains [IRRELEVANT] and local [IRRELEVANT] per item.	Kevin Gilliland	△ New
			8	Parcelforce Reversals. We have identified branches (2 with significant instances and 3 with suspicious activity) potentially reversing more Parcelforce transactions, and at higher value, than they are transacting. This difference is essentially being funded through our settlement process by Parcelforce however, if we cannot recover it from the agent POL may be liable. The issue is owing to the reversal system not "talking" to the postal services sales system within Horizon. The reversal creates a separate, unconnected transaction and does not confirm with postal services that the postage has been cancelled. The product team will conduct ongoing monitoring of the reversals across the network to identify any branches which have a higher average or have a negative refund to sale ratio. In the longer term transaction simplification will close this risk down. The new system removes the existing sales process and will allow PFW labels to be printed via Horizon printers, removing the prepopulated labels from circulation. The new system will work like other postage services processed via Horizon and will force reversals via the spoiled label route instead. This will deliver in April 2018 at the earliest as it is tied into other transaction simplification processes, Royal Mail and Parcelforce agreement, and is dependant new printer kit to be rolled out to the network.		△ New
			9	Losses [IRRELEVANT] YTD, with [IRRELEVANT] in period 4.	Alisdair Cameron	△ New
	Financial Crime	Liabilities and contingencies, including those associated with guarantees.	10	AML regulatory duties. HMRC has informed Post Office, through the Post Office GC and MLRO that there are instances where we they consider that we may not have met our AML regulatory duties in the relevant period for Travel Money (and possibly Bill Payment depending on whether Bill payments are properly within HMRC's regulatory scope), foreign exchange and MoneyGram and gift cards. This may result in Post Office incurring penalties and remedial costs; details have not yet been determined by HMRC. A remediation action plan for Bureau de Change has been shared with HMRC, and which they have verbally approved in principle. An AML Steering Group has been established to oversee delivery of all remedial activity around policies, risk assessments, training, etc. All of these elements are now on track with suitable BAU controls in place. We have been advised by HMRC that they may levy a penalty in the region of £400k in relation to breaches of Regulation 19 (Record Keeping) and Regulation 20 (Policies & Procedures) for Bureau de Change.	Jane MacLeod / Nicholas Kennett	▽
		Material events that could crystallise before the end of the reporting period.	11	New Money Laundering Regulations. The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 came into force on 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 awaited from HMRC. 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 regime also extends to agents, however, HMRC do not yet have an agreed approach. 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.). Post Office have until the date of our next annual registration (1st June 2018) to comply with these new requirements.	Jane MacLeod / Nicholas Kennett	△
	Compliance with laws and regulations	Material risks to Post Office that are not captured in the Group Risk Profile.	12	Vetting. In April 2017, POL implemented a general vetting solution. A plan is being built across IT, Support Services and other areas to support the delivery of postmaster identification and vetting to support contractual obligations including the Banking Framework and regulatory obligations. Pre solution vetting and training procedures for employees, agents and/or agent employees may not have been consistently applied and/or applied in a way that fully complied with our obligations to other parties e.g. Banking Framework, POMS and BoI as regulated principals, Royal Mail, contract obligations and government clients. Current legislation does not require us to retrospectively vet existing staff. Specifically concerning the Banking Framework, Martin Kearsley has confirmed that the banking partners were aware on joining that POL would not be retrospectively vetting staff to the standards implemented in April 2017. There are a number of regulatory changes that may change this stand-point. We are awaiting a Consultation Paper regarding the implementation of the Senior Manager and Certification Regime for ARs, this could require a retrospective check for individuals holding Senior Manager and/or Certified functions to evidence a Fitness & Propriety level outlined in the paper. We are also in consultation with HMRC with regard to Fitness and Propriety standards within Money Service Businesses (Bureau, MoneyGram), we have not yet been advised as to whether this will require retrospective vetting to meet these standards or which populations will be affected.	Martin Kirke / Nicholas Kennett	▽
		Liabilities and contingencies, including those associated with guarantees.	13	HMRC fine on registration of premises. We received the penalty notice for [IRRELEVANT] in August 2017, in relation to the historic failure to file notifications of changes of premises at which regulated activities occurred, and this has now been paid. It is possible that Moneygram, could seek to recover the amount of any fines or penalties from Post Office, should they be levied against Moneygram by HMRC. We have not had any comment or approach by MoneyGram in relation to their premises registration, but we believe that the HMRC supervisor that was reviewing MoneyGram in 2016 has been on long term sick leave.	Alisdair Cameron / Jane MacLeod	◁▷
		Any legislative, regulatory or contractual compliance issues that have come to light.	14	Commercial risk from Ofcom intervention in standalone landline telephone service. Ofcom is consulting on a number of remedies to increase customer switching and reduce price paid by consumers in this market. The proposed remedies are only targeted at BT and are expected to be implemented early in 2018, but include a potential [IRRELEVANT] per month reduction in Line rental charges, which if Post Office choses to respond may impact the Post Office home phone only business. We looking to mitigate this risk by participating in the consultation process, and refining our customer propositions, however the potential impact in FY 16/17 could be a reduction of [IRRELEVANT] depending on the exact remedies and POL strategic response.	Nicholas Kennett	◁▷
FINANCIAL	Reporting results and providing data accurately	Complex and subjective accounting judgements, estimates and revenue transactions.	15	Telco Amortisation. As part of an internal Balance Sheet review it was identified that there was an under amortisation of prepaid Fujitsu costs [IRRELEVANT] under amortised). The same review highlighted an over amortisation of older Fujitsu costs [IRRELEVANT] over amortised). The net result for FY 2016/7 is an over-amortisation [IRRELEVANT] This process needs to be reviewed in FY 2017/18 to ensure that costs are not prepaid incorrectly and amortisation charge is correct and complete.	Nicholas Kennett	△ New
	Sufficient cash / headroom	Material risks to Post Office that are not captured in the Group Risk Profile.	16	The closure of banks, and access through our Banking Framework could see significant charge for the Supply Chain. We have seen bank closures impact branches in different ways; some relatively unaffected whilst others' cash positions move radically (e.g. from c [IRRELEVANT] deficit per week to c [IRRELEVANT] surplus). We don't currently have a reliable model for how business banking could impact on Supply Chain. The introduction of Lloyd's business banking could be significant in terms of the amount of coin delivered to branches. We are mitigating this through engagement with the Banking Team.	Alisdair Cameron	◁▷
	Control Activities		17	IT Controls Framework. To effectively manage our key operational IT risks, we have worked in partnership with KPMG to implement the industry best practice control framework COBIT5. This Post Office IT Controls Framework (ITCF) is progressing to the final stages. There are 11 key processes for which we have identified 193 controls: 108 are implemented, 64 are partially in place (so they do not fully mitigate the risk) and 21 are currently missing. The target to close all remaining gaps is March 2018. Compared to other IT control framework projects, this level of control gap is not unusually large for this stage in the transformation. Remediation has been carried out against 4 of the 11 key processes, and we will complete remediation activities by mid-September. Test scripts will be developed during September and implemented on the Self-Assessment tool (TrAction) in October. Training will be rolled out to control owners over a 3 month period.	Rob Houghton	▽

POL00423693

5.0 Placemat

Author: Richard Williams/Deana Herley Sponsor: Jane MacLeod Meeting date: 13 September 2017

Executive Summary

Context

At the end of 2016 it was agreed that Post Office would pilot a self-assessment methodology to understand management's view of the effectiveness of the internal risk and control framework. Following the Supply Chain pilot in May, the methodology (referred to as the 'Placemat') has been rolled out, initially, in Finance and Operations (F&O) and then in Legal, Risk and Governance (LRG) as part of a wider roll out across PO which is expected to complete by the end of the 2017-18 financial year.

The purpose of this paper is to update the RCC on the status of the Placemat roll out to date, the results from the F&O and LRG business areas, as well as future plans for the roll out.

Questions this paper addresses

1. How do you read the Placemat and what is it telling us?
2. How are we driving value from implementing the Placemat?
3. How have we engaged with the business?
4. What are the governance arrangements in "run state"?
5. What is the timing of the wider Placemat delivery?

Conclusion

1. The Placemat has been populated with the results from F&O business area (Appendix 1). The overall RAG scores have been informed by a "top down" view of the 34 risks (net) of high importance, mapped to Placemat principal risk types which now exist for this area (Appendices 1 and 2). As a 2nd line function, LRG mostly oversees and advises on the management of risks that are owned by 1st line. Without a holistic view of the wider portfolio, it is difficult to give a complete / scored "top down" position for LRG at this stage. LRG watchlist risks are set out in Appendix 3. In the interim, the Placemat for LRG will remain in a position of "too soon to rate".
2. The Placemat gives us a single point of reference on risk matters, and a more meaningful representation of our overall risk picture. The reporting is supported by both a "top down" and "bottom up" comprehensive identification and prioritisation of risk.
3. Following completion of the Supply Chain pilot in May, the Placemat approach was applied to the rest of F&O (15 teams). We have also completed it with LRG

POL00423693

(7 teams). We are joined up with the GDPR, Joiners Movers Leavers, and Legal and Regulatory Framework project teams.

4. The Placemat approach helps to establish clearer accountabilities for risk management across the 3 line of defence. As the roll out completes, operational management (1st line) will take the lead on reassessment, with Risk and Assurance (2nd line) moving from enabling, to check and challenge. Internal and External Audit (3rd line) will provide independent assurance over the results and will report as necessary.
5. During September, we expect to complete the rollout to Government and Payments Services, the first area within Retail. In parallel, we are engaging with Telecoms, which will also support their preparation for the ICO PECR audit planned for January 2018. A full roll out in Retail is proposed by the end of November. We aim to fully populate the Placemat by the end of the 2017-18 financial year to inform and support annual reporting.

Input Sought

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

The Report

How do you read the Placemat and what is it telling us?

7. Once fully completed, the Placemat will provide a view of how well the Post Office as a whole and by each business area is managing the principal risks to the business. The principal risks listed in the Placemat (Appendix 1) are the main types of risks that a business is likely to face. The risks in each business area are mapped to these principal risk types and the effectiveness of existing controls is assessed. The harm table, which together with a risk matrix (Appendix 4), underpin the Placemat's overall RAG scores. The completed Placemat for the F&O business area is shown in Appendix 1. A consolidated Placemat will be presented at future meetings, reporting risks by exception in each business area.
8. So far, for the completed business areas, the Placemat is telling us;

   F&O has identified 34 top down risks, converged into the 3 net risk RAG rating categories and based on the average impact / likelihood (I/L) from the harm-table scales,

RAG	No of Risks	% of total	Impact	Likelihood	Average Risk Score
Red	6	18	4.0	3.5	14.0
Amber	22	64	2.7	3.8	10.3
Green	6	18	3.5	2.3	8.1
Weighted Average	**34**	**100**	**3.1**	**3.5**	**10.5**

POL00423693

Influencing Factors

Red: 4 (67% of the net red risks), relate to 'Managing Change' as a result of the Back Office programme replacing a fragile PO SAP and HR SAP with CFS and Success Factors. There are a number of Finance / HRSC processes in scope which directly drive our numbers.

Amber: 11 (50% of the net amber risks) are assessed at I/L 2:5, with the concentration of these in Network Operations and an alignment to a corresponding project either planned or underway. All risks have amber rating parity in their respective Placemat risk categories.

Green: 3 (50% of the net green risks) are assessed at I/L 5:1 and whilst a green at PO level, at a local level, have been reflected in the Placemat as Amber.

Refer to Appendix 2 for further detail.

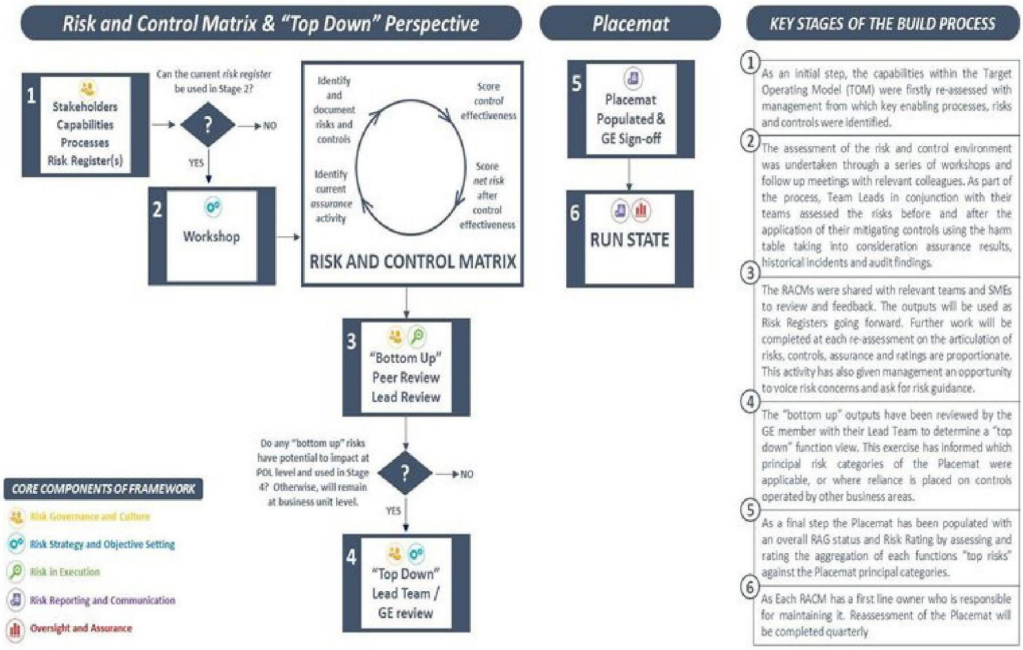
9. LRG has identified a "bottom up" view of risks and controls at a team level. The risks identified would not exceed the materiality threshold at a PO wide level. An effort has been made to build a "top down" view, in order to populate the Placemat. As a 2nd line function, LRG mostly oversees and advises on the management of risks that are owned by 1st line. Without a holistic view of the wider portfolio, it is difficult to give a complete / scored "top down" position at this stage of the roll out. A watchlist of risks is set out in Appendix 3, including:
    - Maturity of the culture in PO with regards legal, regulatory and contractual compliance.
    - Regulatory risk arising from increased visibility of PO and POMs to regulators.
    - Ensuring that the compliance framework imposed on us contractually is viable and deliverable.
    - Potential impact of Postmaster litigation on framework of our contractual relationships with agents.
    - Business engagement on GDPR.
    - Poor contract management impacting PO financially and reputationally.
    - Cyber Threat.
10. In the interim, the Placemat for LRG will remain in a position of "too soon to rate", however this will be reconsidered at each roll out and reassessment.
11. This is not a one-off exercise. The Placemat results will be reassessed by each business area quarterly, which will involve the identification of any new risks and review of current ones. It will also involve closing off risks that are no longer relevant. This process will be fully scoped and piloted for F&O and LRG during October, and presented back to the RCC and ARC in November.
12. At each meeting the paper will set out the movement of principal risks, commentary on key controls, as well as any mitigating factors, informed by either a roll out to a new business area or reassessment of an existing business area.
13. The Placemat process will also inform disclosures in our Annual Report for 2017/18 including: description of principal risks and uncertainties we face; any concerns regarding going concern based on relevant accounting issues or

POL00423693

material uncertainties; and commentary on our review of risk management and systems of internal control.

How are we driving value from implementing the Placemat?

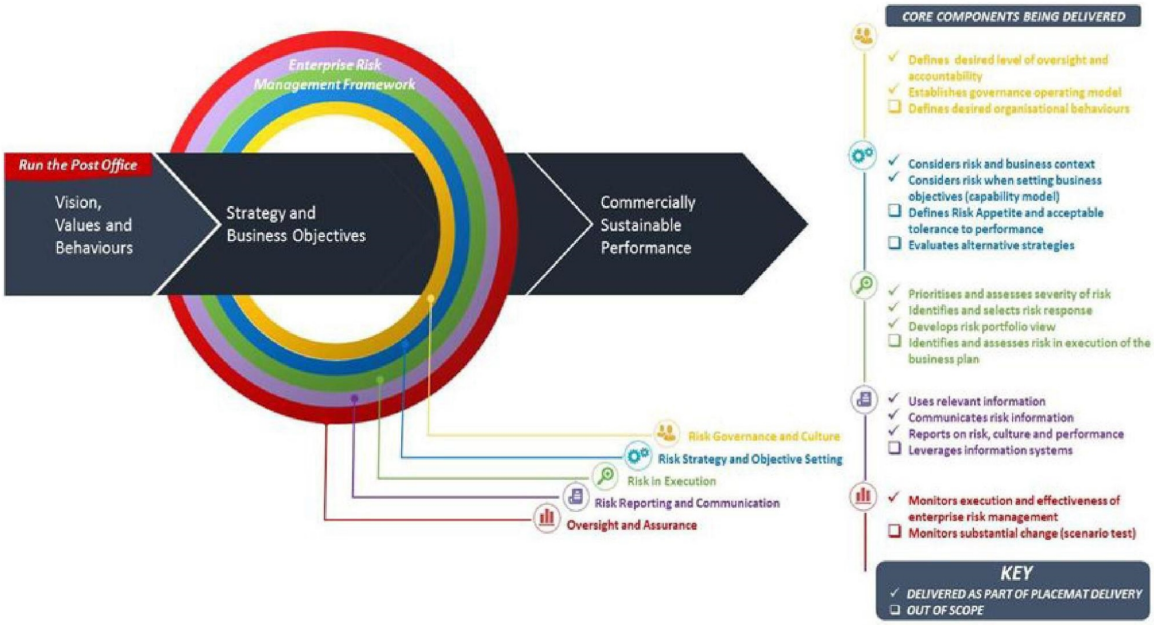
14. An effective risk framework helps drive a culture where the implications of decisions can be discussed explicitly and openly, and employees at all levels understand how much risk they can take in pursuit of objectives. Whilst some aspects of the risk framework have been developed, overall it is currently underdeveloped, delivered on a siloed basis and not enterprise wide in design or scope.
15. The diagram below highlights, through a series of steps, how the Placemat deliverables will strengthen our risk framework components. This also illustrates how the Placemat will standardise and unify what already exists (including group risk profile, top down risks, risk registers, executive declaration, incident and assurance reporting) to deliver more value out of it. The focus of activity to date has been on identifying, prioritising and assessing the severity of risk.



16. The key outputs delivered through the Placemat process are:
    - Risk and Control Matrix (RACM) by team providing bottom up view of the risk and control environment;
    - Top down view by business area; and
    - Placemat populated with overall results by business area.
17. The Placemat outputs are already being used by Internal Audit to inform planning.

POL00423693

18. The diagram below illustrates how the Placemat will strengthen the risk framework. This will support the business to gain a clearer view of its overall level of risk, respond in a considered way and ultimately, a more commercially sustainable way. The components delivered will start to inform a portfolio view of risk which will then allow for the value of "out of scope" components to be considered for development.



19. Examples of how the core deliverables of the Placemat are embedding the principles of sound risk management include:

Risk Governance and Culture	• It is designed to provide the Board and ARC with greater confidence when discharging accountability of risk taking. • Clearer accountabilities and responsibilities for each of the lines of defence. • Will help risk community to be aware of/understand what is strategically important to the business, and what to watch out for. • Pathway to upskilling 1st line of defence in proactively managing risks.
Risk Strategy and Objective Setting	• Will help risk community to be aware/understand what is strategically important to the business, and what to watch out for. • Standardised tools and techniques have been developed to populate risk registers which have improved the quality of outputs.
Risk in Execution	• A comprehensive identification and prioritisation of top down risks. • Helps to recognise how a lack of, or gaps in controls could be driving incidents or near misses.
Risk Reporting and Communication	• Gives a single point of reference. The insights will help to answer the question, how broad are the risks we are considering? • Gives a way of aggregating proactively similar lower level risks, which occur on multiple risk registers, e.g. conduct, BCP etc. at a consolidated group level.

POL00423693

	• The reporting will help the business "join the dots" on risk matters. The format has been created with the view that it will convey insights on risks that truly shape our performance, by connecting management with the rest of the organisation on risk matters.
Oversight and Assurance	• The grouping of key risks under the relevant principal risks will give a meaningful representation of the risk picture. • Allows for more targeted stress testing and focused assurance activity.

How have we engaged with the business?

20. Following completion of the Supply Chain pilot, the Placemat approach was applied to the rest of F&O. In parallel, we have also applied the Placemat approach to LRG. This work has involved approximately 50 workshops and follow up meetings across 22 teams. We have engaged with GE and Senior Management to identify "top down" risks and outcomes ensuring that process and outcomes are aligned. Introductory sessions have also been given to other parts of the business to get wider feedback and support in preparation for future roll outs.
21. We are engaging with a number of project teams to remove duplication and leverage outputs with GDPR, Joiners Movers Leavers and Legal and Regulatory Framework.

What are the governance arrangements in "run state"?

22. Accountabilities in the "run state" will be split between the 3 lines of defence. In the "run state" 1st line will take the lead, with 2nd line moving from enabling to check and challenge. The 3rd line will provide independent assurance on the results.

What is the timing of the wider Placemat delivery?

23. During September, we will complete the Placemat rollout with Government and Payments Services, with a full delivery of Retail proposed by the end of November. In parallel, we will complete with Telecoms, prioritised to support the business's preparedness for ICO PECR audit planned for January 2018. We aim to fully populate the Placemat by the end of the 2017-18 financial year with PO-wide reporting brought to the May RCC and ARC.

POL00423693

APPENDIX 1

Self-Assessment of the Internal Risk and Control Framework - Post Office Limited

As at 06092017

Ref		Principal Risks	GE Owner	LRG			Finance & Operations		
				Q2 17	Q3 17	Q4 18	Q2 17	Q3 17	Q4 18
1	OPERATIONAL	Manage process and deliver services	TBC	Too soon to rate			2		
2		Product risk	NK / KG						
3		Make payments	AC				2		
4		Records management	TBC						
5		Procure and contracts	AC				2		
6		Managing change	AC				1		
7		Keep our people, customers and third parties safe	AC				2		
8		Physically secure	AC				3		
9		BCP	JMaC				2		
10	TECH	Technology Ops	RH						
11		Business Interruption (ITDR)					2		
12		IT Security							
13		Dependence on IT 3rd Parties							
14	LEGAL & REGULATORY	Managing losses and Fraud	AC				2		
15		Financial Crime	JMaC						
16		Information Protection	JMaC				2		
17		Brand	Mark Davies						
18		Record and pay taxes	AC				2		
19		Compliance with laws and regulations	JMaC				2		
21	FINANCIAL	Reporting results and providing data accurately	AC				2		
22		Sufficient cash / headroom					2		
23		Ensuring sustainable profit					2		
24		Control activities					2		
25	STRATEGY	Competitiveness	ME/NK/KG						
26		Strategic Risk							
27		Market							
28		Customer Relevance							
29	PEOPLE	Communicate, inspire and align	MK				2		

Key	See Risk Rating User Guide

POL00423693

APPENDIX 2

	Finance & Operations Risks	Principal Risk	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Comments
High Risks								
1	Retail proposition is not attractive, churn is rising, risking 11,500	Manage process and deliver services	Mark Ellis	Tom Moran	4	4	16	Projects to mitigate include: simplification, extension of automation to agency branches, white space and new retain value proposition to multiple partners.
2	High levels of change will cause fragile systems to fail	Managing change	Ben Cooke	Tim White	4	4	16	There are a significant number of business and IT programs impacting applications and processes. All of these programs must follow the IT change process when making technical changes, and each are supported by enterprise architecture, checking designs to ensure overall coherence.
3	We have to replace POLSAP or shore it up, creating existential risks	Managing change	Amanda Radford	Danielle Goddard / Ben Cooke	5	3	15	The Back Office programme will migrate POL SAP to CFS. The scope covers a number of processes which drive our financials e.g. client settlements. A controls contractor is now embedded within the Programme to oversee migration. POL SAP balances, access profiles (baseline and process) and financial reporting controls will be formally signed off by the Financial Controller and the Financial Accounting and Governance Manager before migration. If POL SAP is not replaced it will be out of support. The existential risks could result in a misstatement of the numbers.
4	We have to deliver agents pay via CFS	Managing change	Amanda Radford	Joe Connor / Ben Cooke	4	3	12	The agent remuneration project will be live by Feb 2018. Pre-prod dual running Nov and Dec. Prod dual run in Jan. Full calculation in the new model only by Feb 2018.
5	We have to deliver payroll via SF, building on a fragile HRSC	Managing change	Angela Van-Den-Bogerd	Joe Connor / Martyn Lewis	4	3	12	Success Factors Programme is replacing a number of services currently provided through HR POLSAP and the Back Office Transformation programme is working on the POLSAP Process Migration, with a current view that this will be live by June 2018. This will allow us to de-commission POLSAP by September 2018. Data archiving and residency of POLSAP is being investigated.
6	We are using too much cash, risking loss, funding costs and change funding	Sufficient cash / headroom	Russell Hancock	Doug Brown	3	4	12	A project team is reviewing cash management in its entirety focusing on forecast completeness and inaccuracies. The 'cash declaration' element of the project is critical as without it being right the team will not know what should be in branch. Additional resource in post will look to improve the customer experience of getting cash out and will also be tackling excess cash to reduce fraud / losses. Separately the Forex experience is being reviewed. Projects are scheduled to complete by year end.
Medium Risks								
7	Financial Reporting is inaccurate creating reputational damage	Reporting results and providing data accurately	Amanda Radford	Danielle Goddard	5	2	10	The Financial Controls Framework (FCF) has been extended to cover FCS processes, branch corrections, agent debt and POMs processes. This work has now started. FCF controls are self-assessed by owners monthly.
8	Safety outcomes are not world class and where they are not in line with required legal and regulatory standards, may lead to serious injury	Keep our people, customers and third parties safe	Angela Van-Den-Bogerd	Martin Hopcroft	5	2	10	Additional Person in Control training has been provided to DMB managers and colleagues and Supply Chain Managers. Over the next 3 months additional training will be provided to all Support teams. Work is ongoing to ensure contractors are clear on roles and responsibilities. The scope of agent activities and opportunity for Post Office to provide guidance is also under review. Additionally, to reduce overall Health & Safety risk, a deep dive review of Health & Safety has been undertaken by the GE Safety Committee and action agreed to reduce each area of risk, reporting to the Committee on a monthly basis at the Operations Board with subsequent 6 monthly 'deep dive' reviews planned. To assess the robustness of the Safety Management System and to identify improvement opportunities to meet World Class level, an independent 3rd party audit is also being planned for Q3.

POL00423693

9	Our MI is limited leading to poor decisions	Reporting results and providing data accurately	Amanda Radford	Somita Yogi	2	5	10	The Head of Management Information is working with Amanda Radford (Financial Control) and Ben Cooke (IT) to move forward with a business case which considers, what our current constraints are and how we should we move forward (implementing proper structure and tooling to rectify). There are also plans to do a proof of concept for rolling out self-service tool.
10	We appoint unsuitable applicants leading to performance issues and re-work due to increased terminations through losses.	Manage process and deliver services	Mark Ellis	John Breedon	2	5	10	A review of applications process has been complete and plan for implementing recommendations is now being developed.
11	Agents or other third parties steal from us and lose our money	Managing losses and fraud	Mark Ellis	Mark Raymond / Kim Abbott	2	5	10	Paramount is the need to ensure the recruitment process and vetting attract lower risk individuals and that contracts are enforced robustly. The Fraud Analysis team aim to identify losses early so early intervention via telephone or scheduling audits can take place. In addition a system for early intervention is to be introduced where activity will include tasking Security Operations to make visits to identified branches. External company review – EXL are engaged on a piece of work to look to streamline and make more effective the Fraud Analysis Team's reports and analysis. A new debt recovery and investigation process is going to be introduced to recover losses in a far more timely manner including partnership approach reviewing live cases with Security Operations, legal team, contracts and agent debt teams to establish clear action plans to recover loss. Branch Communications including notifications of convictions are to be publicised as a deterrent. Moving forward test cases to prosecute will be identified with a view to returning to a full Prosecution Policy where Proceeds of Crime Act can be utilised, making POL an unattractive business to steal from.
12	Limited monitoring of and communication with agents, reducing conformance	Managing losses and fraud	Mark Ellis	Kim Abbotts	2	5	10	An annual call plan has been developed. Monthly calls to branch are made on a prioritised basis. The Branch Standards team are unable to currently fulfil level of demand which has been raised with GE. The benefits of re introducing post appointment visits are being considered.
13	Branch opening hours are wrong, affecting customers	Manage process and deliver services	Mark Ellis	Tom Moran	2	5	10	The Opening Hours Project is under way, with the first batch of work focusing on cleansing data. Q4 'business as usual' activity is planned with the Branch Standards team.
14	Debt recovery is slow and ineffective creating loss	Managing losses and fraud	Stuart Nesbit	Michelle Stevens	2	5	10	A new faster debt path was designed at a recent workshop. Recovery letters are been redrafted with Legal and then issued, which initially will be a manual process to monitor their effectiveness. We are currently looking to develop a more sophisticated debt management system, which will enable the better integregation of management information.
15	Informal controls and compliance over Operations	Control activities	Various	Danielle Goddard	2	5	10	Refer to risk 7 comments.
16	We can't communicate effectively with all of our people	Communicate, inspire and align	Russell Hancock Mark Ellis	n/a	2	5	10	
17	Our change is delivered late, risking costs and benefits or has unintended consequences	Managing change	Angela Van-Den-Bogerd	Jenny Ellwood	2	5	10	Work is underway to assess the do-ability of the integrated plan. Looking at this from an IT, Network, Network Operations, HRSC and FSC perspective. The Gating process is also under review and plans underway to re-educate and reinforce minimum standards with our change governance and controls. The results of this will be presented to ECG in September. Additionally, Stuart Nesbit (FSC) is leading on a review of the forecast and phasing of spend and benefits with the FD's. Once the accuracy of this is validated, variances will be tracked and the reason for those variances tracked for trends and concerns.

POL00423693

18	Manual processes mean we can't demonstrate compliance on agent vetting and training	Manage process and deliver services	Angela Van-Den-Bogerd / Mark Ellis	John Breedon	2	5	10	The Enhanced User Management Programme is looking to control access to Horizon which will be subject to successful vetting and training. New starters will not be able to obtain Horizon access until vetting and training is successfully completed, making it easier to control. Existing staff will have access to Horizon removed if they do not pass the required compliance training (access could be to a product set or to the full system, depending upon which training they do not sit and pass). However, this Programme is under pressure and has only an approved plan to deploy to '500' branches, which if all goes as planned will commence with 50 branches on 11 September and be complete before the December change freeze.
19	A lack of training and support for newer agents creates loss and churn	Manage process and deliver services	Mark Ellis	Pam Heap	2	5	10	A structural review of the field teams (Network Ops) is under way. A full review of agent training material is to be completed with the Learning Team.
20	We report net liabilities reducing confidence in Board and third parties	Procure and contracts	Amanda Radford	Danielle Goddard	3	3	9	Various reviews have been completed considering how we increase net asset provision.
21	Limited DR/BCP plans, largely untested increase the impact of systems and site loss	BCP	Various	Tim Armit / Mick Mitchell	3	3	9	Ongoing enhancement of plans and strategies is being completed across Supply Chain, Chesterfield and Bolton. Chesterfield has a tested recovery solution with SunGard. Supply Chain depots are all being taken through training and the Stay Calm manual rewritten. A recovery solution for Bolton has been proposed and is being considered. Finsbury Dials work at home exercise is planned in August 2017. Risks, impacts and strategies will be developed across all areas in 2017/18.
22	Loss of Swindon operation causes widespread product loss	BCP	Russell Hancock	Rhys Davies	3	3	9	With the closure of Merlin House the contingency for Swindon (albeit on a limited line basis) there is currently, no alternative physical space to put it. A like for like alternative is being scoped at Swansea CViT – albeit with the same constraints.
23	We do not have sufficient funds to create a sustainable business	Sufficient cash / headroom	Amanda Radford	Danielle Goddard	4	2	8	A number of initiatives are in place to ensure efficient use of our working capital (particularly our cash inventory - see 6 above) to ensure we create as much headroom under our facilities as possible. In addition, we are formulating a negotiation strategy with Santander to reduce the constraint on headroom driven by their security arrangements and are in talks with banks to arrange up to [redacted] of standby facilities. Both these initiatives will create additional headroom capacity under existing facilities.

POL00423693

24	Limited cash data and forecasting leads to a facility breach	Sufficient cash / headroom	Amanda Radford	Mark Dixon	4	2	8	We primarily manage this risk by ensuring we have accurate cash forecasting processes in place. This is a focus for us and there are a number of initiatives in place to improve cash flow forecasting, including the Cash Management project. We approach cash flow forecasting from 2 perspectives: (i) cash in / cash out for the short term view (Treasury); (ii) projections of balance sheets for the medium / long-term view (FP&A). The short-term approach becomes less accurate the further out that you go and hence the need to have two approaches and to align them. We have a daily 8-day rolling forecast in place making use of our TMS to consolidate cash flows. The use of the TMS rather than a reliance on spreadsheets enhances controls. We have put in place weekly and monthly reporting and variance analysis which we distribute to senior management as well as daily reporting and variance analysis which is distributed to the Head of Treasury. The Teams focus is on improving our forecasting using this variance analysis. As a result we have built a new model to forecast Note Circulation Scheme balances, an area in which we clearly need to improve. As a result of OSOP changes in the Wholesale Cash Team, and hence reduced resource levels, there are delays in implementing the new model. We now need to focus on improvements around process and modelling of the medium term and will be addressing this within the cash management project.
25	We cannot report, forecast or optimise branch cash	Ensuring sustainable profit	Russell Hancock	Doug Brown	2	4	8	A new system is being implemented through Back Office (scheduled for March). The Supply Chain element of POL SAP will move to CWC. This will enable us to forecast more accurately, for example the dates forecasted on will be system driven. This will give us the functionality to create, change events and cleanse data to better reflect normal trading. Branches will also be able to order cash online which will improve the overall experience.
Watch List								
26	We are not compliant on tax attracting fines and censure	Record and pay taxes	Amanda Radford	Mark Dixon	3	2	6	Although Tax will consist of one individual going forward, there are a number of trained accountants involved with tax preparation at POL. Where specialist input is required additional information is requested from external providers, which by nature of experts and regulated in their chosen field. It is anticipated that the going forward, people other than the new tax manager will be involved in the preparation, with the manager performing review. This will ensure adequate segregation of duties, and also that a 'four-eyes' review has been adopted. This process will take a number of months to be embedded.
27	We procure badly, destroying value	Procure and contracts	Barbara Brannon	William Porter	3	2	6	Sourcing Council will be embedded into change management cycles by the end of year. Category Managers will lead on providing clear content requirements. Business leads will be required to attend meetings, with GE or SLT sponsor signing off the process agreed. Our ability to track spend against supplier will be improved in the short term through a monthly spend report generated showing contract value and forecast by October. Work is nearing completion to review suppliers, where spend is over £5k and allocate owners. The longer term solution will be a contract management system. A business case for this is currently being reviewed. Our ability to manage procurement documentation will be improved through the digital 365 project to SharePoint. A document standard for physical / electronic storage will also be drafted. Bravo will be used by Category Managers to currently plug gaps. The longer term fix for this will be the implementation of a Contract Manager system.

POL00423693

28	We procure illegally, attracting fines and censure	Compliance with laws and regulations	Barbara Brannon	William Porter / Jacqueline Scott	2	3	6	Over the next couple of months the Procurement Policy will be refreshed, articulating how to buy and communicated to colleagues / suppliers. This will include a no pay policy. Procurement are also proposing the following: 1. SAP requisition workflow will be also adjusted to move Procurement to the start of the process to help embed. 2. A minimum requirement for all project works to have procurement provisional budget to be introduced. Pipeline accuracy to be Procurement and Category Manager KPI by October. Pipeline will be published to key stakeholders to support business prioritisation. Non-compliance continues to be logged, tracked and escalated to GE and RCC.
29	We do not keep cash physically secure	Physically secure	Russell Hancock	Mark Raymond / John Flood	5	1	5	IRRELEVANT is either on the processing floor trays, cages or sealed covered by CCTV. IRRELEVANT is held in the operational vault. IRRELEVANT is held in the bonded vault.
30	Risk of kidnap in SC etc.	Physically secure	Russell Hancock	Mark Raymond	5	1	5	Tiger kidnap training is delivered annually to all staff in Supply Chain. Winter safety awareness training also covers route changes etc.
31	Risk of political/social violence in Northern Ireland	Keep our people, customers and third parties safe	Russell Hancock	Mark Raymond	5	1	5	In terms of public order in Northern Ireland, to date, 2017 has been widely described as the most peaceful for some years although there remain numerous social and political issues in many communities across the province with some being subject to violent criminal activity. Dissident Republican Terrorist activity has increased significantly with the Police Service of Northern Ireland (PSNI) being the primary target. POL Security is updated by the PSNI on a regular basis of all risks and potential risks to the business. The general risk to POL NI remains at Moderate.
32	Financial forecasting is limited	Ensuring sustainable profit	Amanda Radford	Ian Lakin	1	5	5	A new interim head of FP&A has been appointed who will review the current reporting and forecasting processes which will look to address the risk.
33	Purchase to pay process is complex leading to errors and delays	Make payments	Stuart Nesbit	Barbara Brannon	1	5	5	Procurement and FSC are working closely to improve vendor and business conformance to ensure payments are made within 30 days as per the Performance and Reporting requirements due to come into effect in 2018/19.
34	We do not settle accurately and quickly with clients	Make payments	Stuart Nesbit	Kay Wilson	4	1	4	Due to the low probability no specific additional plans. In the event of system outage manual workarounds are required which through human error could result in clients being paid incorrectly, despite additional checking. The Back Office programme is looking to remove the manual nature.

POL00423693

APPENDIX 3

	Legal, Risk & Governance Risks	Principal Risk	SLT Accountability	SME Accountability	Impact	Likelihood	Risk Score	Comments
Watch List								
1	Reputational damage and financial loss arising from poor contract management	Procure and let contracts						
2	Immature culture within POL as regards legal, regulatory and contractual compliance (network)	Compliance with laws and regulations						
3	Cyber risk - Failure to identify and Control the Insider threat and include security controls in contracts with suppliers.	IT Security						
4	Regulatory risk arising from increased visiblity of POL & POMS to regulators eg. ICO re GDPR, HMRC re AML/CTF, FCA re POMS expansion, FCA via Banking Framework	Compliance with laws and regulations						
5	Whether Post Master litigation could result in material challenge to the framework of our contractual relationships with agents.	Compliance with laws and regulations						
6	Whether once properly understood, the compliance framework imposed on us contractually is actually viable and deliverable across the network as now structured.	Compliance with laws and regulations						
7	GDPR - lack of engagement by the business (eg around identifying data architecture) has the ability to cause material delay to the programme	Compliance with laws and regulations						

POL00423693

APPENDIX 4

Risk Rating User Guide

The overall Risk Rating is calculated using a weighted average of risk that is considered appropriate, recognising that the applied rating is subjective, and is based on the following:

Impact - if risk exists, based on the harm table, what impact could this have on the business?
Likelihood - while risk by nature is inevitable, based on the harm table, what is the likelihood of this particular risk appearing in practice?
Combined score - takes the Impact Risk x Likelihood to calculate a combined score
Controls - weighting of controls to mitigate the perceived risk
Overall RAG - Residual Risk is the combined score divided by the mitigating controls

NB: Residual risk is the threat that remains after identified risks have not been eliminated by compensating controls. For each risk recorded, the Committee should determine and agree whether to make plans to reduce it, avoid it, accept or transfer it.

Harm Table and RAG Rating Segmentation

Impact	Impact Rating (A)	RAG
Low	1	G
Medium	2	A
Medium	3	A
Medium	4	R
High	5	R

Likelihood	Likelihood Rating (B)	RAG
Low	1	G
Medium	2	A
Medium	3	A
Medium	4	R
High	5	R

POST OFFICE

HARM TABLE - MEAUREMENT CRITERIA

Version: 18th Feb 2016, post RCC & ARC

Use EBITDAS target of £100m

Risk Scoring	Impact on* Label	Financial** (EBITDAS)	Operational Continuity (Operations, IT, Colleagues)	Reputational (Stakeholder, Customer, Colleagues, Third Party, Media, Regulator)	Likelihood of* Label	Probability
5	Critical	>20% of financial target or significant impact on all objectives	National service disruption/ significant location/s or business function/s for >5 days	- withdrawal of stakeholder/ customers/ colleagues/ 3rd party support, or - extensive national media coverage, or - formal regulatory intervention	Very Likely	>80%
4	Significant	>10-20% of financial target or significant impact on all objectives	National service disruption/ significant location/s or business function/s for <5 days	- significant challenge from stakeholder/ customers/ colleagues/ 3rd party support, or - some national media coverage, or - formal regulatory investigation	Likely	>50-80%
3	Major	>5-10% of financial target or significant impact on all objectives	Regional service disruption/ major location/s or major business function/s for <3 days	- major questioning from stakeholder/ customers/ colleagues/ 3rd party support, or - extensive local media coverage, or - informal regulatory enquiry	Possible	>25-50%
2	Moderate	>1-5% of financial target or significant impact on all objectives	Local service disruption at several locations or business functions for >1 days	- moderate concern from stakeholder/ customers/ colleagues/ 3rd party support, or - some local media coverage, or - informal regulatory conversations	Unlikely	>10-25%
1	Minor	0-1% of financial target or significant impact on all objectives	Local service disruption at several locations or business functions for <1 days	- negligible interest from stakeholder/ customers/ colleagues/ 3rd party support, or - no media coverage, or - no regulatory interest	Remote	0-10%

Gross (Inherent) Risk

Combined Score (C) = (A) x (B)

Latest Combined Score is a calculated values = Impact x Likelihood

1	G
2	G
3	G
4	G
5	G
6	A
7	A
8	A
9	A
10	A
11	R
12	R
13	R
14	R
15	R
16	R
17	R
18	R
19	R
20	R
21	R
22	R
23	R
24	R
>=25	R

Control Effectiveness

Controls (D)

Controls put in place to mitigate the risk	Low	1	R
	Medium	2	A
	High	3	G

Net (Residual) Risk

Overall RAG (C) / (D)

Low	1	G
Medium	6	A
High	11	R
Risk not applicable		

Minimum Score

POL00423693

Post Office Legal and Regulatory Framework

Author: Ben Foat Sponsor: Jane MacLeod Meeting date: 13 September 2017

Executive Summary

Context

Post Office Limited (Post Office) is a multiline business operating across numerous sectors including Financial Services, Telecoms, Retail, Government Services, and Mails with a significantly unionised work force and, as a result of its public ownership, is also subject to additional public sector legal obligations such as public procurement rules. The Post Office is also directly or indirectly subject to numerous regulators including HMRC, FCA, CMA, ICO, and OFCOM. As a distributor of a vast array of products and services, it manages over 1,700 commercial contracts, thousands of employment contracts, property licences and instruments, and hundreds of disputes and complaints, all of which are generally underpinned by legislation and regulation. Consequently, the legal risk across the POL group is broad and complex.

The ARC is to receive training prior to the next ARC meeting on Post Office's legislative and regulatory framework.

This report sets out, in draft, the legal and regulatory framework under which Post Office operates and suggests who, within the business, is responsible for managing compliance with those pieces of legislation and regulation. It solely focuses on the material and most frequently encountered laws and is by no means exhaustive. This work will be incorporated into broader discussions around accountability within the business.

Questions addressed in this report

1. What are the material and most frequently encountered laws?
2. Who is responsible for ensuring compliance with legislation and regulation?
3. How are new legal trends and developments applicable to Post Office managed?
4. What do we need to do next to progress?

Conclusion

1. Appendix 1 is an overview matrix which sets out the top 48 material and most frequently encountered pieces of legislation and suggests which GE member is

POL00423693

accountable or responsible, from a first line of defence perspective, for ensuring compliance with those laws.

2. Appendix 2 provides a more comprehensive outline of those laws which are rated 'red' or 'amber' in terms of materiality (see paragraph 6 below), as well as the known controls and the evidence of such controls.
3. The Legal Team identifies new legal trends and developments through its Regulatory Developments Tracker (Horizon Scanning). Any new or proposed material changes to laws and regulation is communicated to the relevant parts of the business as well as being communicated through the cross functional Law and Trends Forum. Working groups are then set up to further assess the impact of the new or material changes and implement those changes within the business.
4. Further refinements to Appendix 1 and 2 will be made incorporating the feedback from the RCC specifically any clarifications over which parts of the business are responsible or accountable from a first line of defence perspective.

Input Sought

1. The Committee is asked to discuss the responsibilities allocated to GE or GE-1 and to make recommendations as to further refinement.

Input Received

2. This report has incorporated the Finance & Operations compliance matrix together with the comments from Retail, IT, FS and HR.

POL00423693

The Report

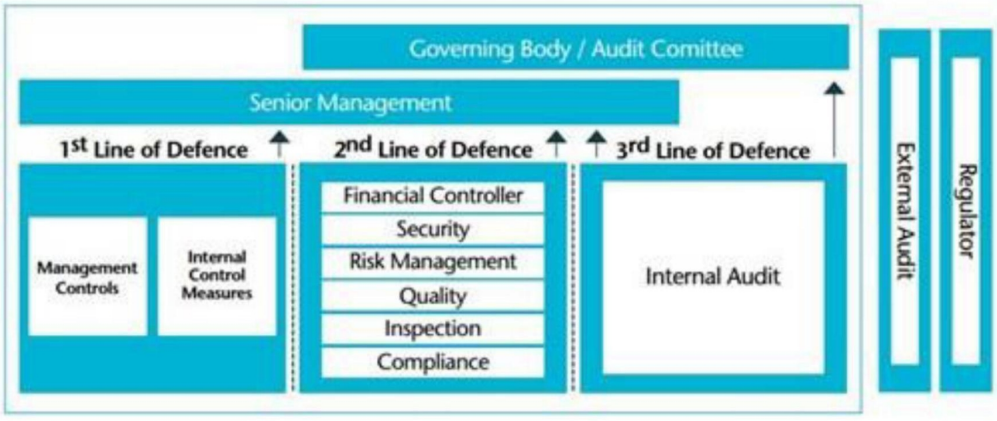
What are the material and most frequently encountered laws?

5. There are hundreds of pieces of legislation and regulation that apply to Post Office. Appendix 1 and 2 sets out the most material and most frequently encountered laws at Post Office.
6. A RAG status has been adopted to differentiate materiality on the following basis:
   - Red – where there is potential individual criminal sanctions and or personal liability for Board / GE;
   - Amber – where there is significant sanctions including corporate criminal offence or significant penalty (without individual sanctions);
   - Green – where there is typical sanctions (e.g fines)

Who is responsible for ensuring compliance with legislation and regulation?

7. As set out in the Appendices, we have allocated 'Accountability' for each piece of legislation to key GE sponsors, and indicated who else is 'responsible' for compliance at an operating level.
8. As Post Office's risk management framework matures, we will be able to address this more fully through the 3 lines of defence risk management model. In summary:

   - first line – functions that own and manage risk
   - second line – functions that oversee or specialise in risk management, compliance (ie Legal, Compliance, Risk, etc)
   - third line – functions that provide independent assurance e.g internal audit.



9. Post Office' second line capability is still relatively immature and the distinction between first and second line responsibilities needs further articulation.

POL00423693

Nevertheless as the 'placemat' control effectiveness self-assessment work is rolled out across Post Office, this will facilitate a greater awareness of first line responsibilities, as well as enable the development of more mature 2nd line oversight capability.

10. Accordingly, Appendix 1 provides an overview matrix which seeks to delineate accountability (ownership of risk) and responsibility (those who need to comply with requirements or follow direction from the accountable owner within their area of responsibility). For example, it is proposed that Jane MacLeod (Group Legal, Risk & Governance Director) is accountable for the Bribery & Corruption Act (as the Financial Crime team specify the controls to be operated to best prevent bribery). However, all areas of the business are responsible for ensuring its compliance through enforcing internal controls such as the Gifts & Entertainment Policy in respect of their areas within the business).
11. It is also proposed that, by way of example, Al Cameron (Chief Finance & Operations Officer) is accountable for public procurement but all areas of the business are responsible for ensuring that they comply with the internal controls set out by him through the Procurement Director, Barbara Brannon. In the overview matrix, R denotes responsibility and A denotes accountability.
12. Appendix 2 provides more detailed descriptions of those pieces of legislation rated as 'red' or 'amber'. Details of green rated legislation have also been prepared, and are available from the legal team on request.

How are new legal trends and developments relevant to Post Office managed?

13. The Legal Team is responsible for identifying new and emerging areas of legal risk. On a monthly basis it identifies new legal trends and developments through its Regulatory Developments Tracker (Horizon Scanning). Some areas of the business also maintain horizon scanning specific to their area. Any new or proposed material changes to laws and regulation is communicated to the relevant parts of the business as well as being communicated through the Law and Trends Forum which has representatives across the business. The Law and Trends Forum enables alignment across the business. Working groups are then established in relation to material new pieces of legislation, consisting of relevant stakeholder, to further assess the impact and provide recommendations in respect of any changes to existing internal or management controls.

What do we need to do next to progress?

14. Following the feedback from the RCC, Appendix 1 and 2 will be updated and be sent to the Strategy Team who are working on the broader issues of accountabilities within the organisation. These documents may also serve as a useful tool for those involved in SMCR project.

POL00423693

Appendix

1. Material Legislations/Regulations - Overview Matrix
2. Material Legislations/Regulations - Detailed Framework

POL00423693

1. Overview Matrix – Proposed Responsibility and Accountability

Material Legislation / Regulation	Business Area	CEO (Paula Vennells)	FS & Telco (Nick Kennett)	Retail (Kevin Gilliland)	Strategy (Martin Edwards)	HR (Martin Kirke)	IT (Rob Houghton)	LRG/CoSec (Jane MacLeod)	Ops (Al Cameron)	Comms, Brand & Corporate Affairs (Mark Davies)	Board Impact
Bribery Act 2010	All	R	R	R	R	R	R	A	R	R	
Business Rates	Ops								A		
Communications Act 2003	Telco, Retail		A	R							
Companies Act 2006	CEO, LRG, Ops	A						A	A		
Consumer Insurance (Disclosure and Representations) Act 2012	FS, Retail		A	R							
Corporate Manslaughter and Corporate Homicide Act 2007	Ops								A		
Criminal Finances Act 2017	All		R	R	R	R	R	R	A	R	
Data Protection Act 1998 & GDPR	All		R	R	R	R	R	A	R	R	
Digital Economy Act 2017	Retail, Ops, FS, Brand		A	R					R	R	
Employment Rights Act 1996	All		R	R	R	A	R	R	R	R	
Energy Acts Directives and Regulations (various)	Ops								A		
Enterprise Act 2016 (competition)	All		A	RA	R	R	R	R	R	R	
Enterprise Act 2016 (pay cap)	All		R	R	R	A	R	R	R	R	
Environmental Legislation and Regulations	Ops								A		
Environmental Protection Act 1990	Ops								A		
Equality Act 2010	All		R	R	R	A	R	R	R	R	
FCA Conduct of Business Sourcebook (COBS/ICOBS)	FS, Retail		A	R							
Financial Services and Markets Act 2000/FCA Handbook	FS, Retail		A	R							
Freedom of Information Act 2000	LRG							A			
Gross Negligence Manslaughter	Ops, Retail			R					A		
Health & Safety at Work Act 1974	Ops, HR, Retail			R		A			A		
Insurance Act 2015	FS, Retail		A	R							
IMD & Insurance Distribution Directive	FS, Retail		A	R							
Intellectual Property Laws (various)	Brand									A	

POL00423693

Material Legislation / Regulation	Business Area	CEO (Paula Vennells)	FS & Telco (Nick Kennett)	Retail (Kevin Gilliland)	Strategy (Martin Edwards)	HR (Martin Kirke)	IT (Rob Houghton)	LRG/CoSec (Jane MacLeod)	Ops (Al Cameron)	Comms, Brand & Corporate Affairs (Mark Davies)	Board Impact
Landlord and Tenant Acts	Ops								A		
Law of Property Acts; Land Registration Act 2002; 2003 Rules	Ops								A		
Modern Slavery Act 2015	HR, Ops, Retail			R		A			R		
MLR 2017	FS, Retail		A	R				A			
Ofcom's Conditions of Entitlement	FS, Retail, Brand		A	R						R	
Payment Services Regulations 2017	FS, Retail		R	A							
Postal Services Act 2011	Retail, FS, Strategy		R	A	R						
Privacy and Electronic Communications Regulations 2003/Network and ISD	LRG, FS		A					A			
Public Contracts Regulations 2015	All		R	R	R	R	R	R	A	R	
Public Interest Disclosure Act 1998 (whistleblowing)	All		R	R	R	A	R	R	R	R	
Reforming the Intermediaries Legislation (IR35)	HR					A					
Re-use of Public Sector Information Regulations	LRG							A			
s.3 Small Business, Enterprise and Employment Act 2015	Ops, Brand								A	R	
Senior Managers & Certification Regime	HR, FS		A			A					
The Consumer Rights Act 2015	Retail, FS		R	A							
The Payment Card Industry Data Security Standard	FS, Retail		R	A							
The Welsh Language (Wales) Measure 2011 and associated Regulations	Retail, FS, Brand		R	A						R	
Town and Country Planning Act 1990 and various others	Ops								A		
Trade Unions and Labour Relations (Consolidation) Act 1992 (TULRCA)	HR					A					
Transfer of Undertakings (Protection of Employment) Regulations 2006	All		R	R	R	A	R	R	R	R	
Treaty on the Functioning of the European Union; Competition Act 1998	All		A	A	R	R	R	R	R	R	

POL00423693

Material Legislation / Regulation	Business Area	CEO (Paula Vennells)	FS & Telco (Nick Kennett)	Retail (Kevin Gilliland)	Strategy (Martin Edwards)	HR (Martin Kirke)	IT (Rob Houghton)	LRG/CoSec (Jane MacLeod)	Ops (Al Cameron)	Comms, Brand & Corporate Affairs (Mark Davies)	Board Impact
Treaty on the Functioning of the European Union - State Aid	Retail, Strategy, Ops			R	A				A		
Universal Postal Union Convention/CAA	Retail			A							
Value Added Tax Act 1994	Ops								A		

2. Detailed Framework

Legislation / Regulation	Description	Obligations	Business Area	Responsibility	Accountability	Controls / Policies	Evidence	Board Impact
Bribery Act 2010	This Act deals with an offence of offering, promising or giving a financial or other advantage for the purpose of bringing an improper performance of a function or activity. Requires active measures to prevent bribery.	POL and POMS must comply with six principles of adequate procedures to prevent bribery: - Proportionate procedures – the procedures adopted should be proportionate to the risk faced. - Top-level commitment – POL/POMS should adopt a culture of zero tolerance through a commitment by senior management. - Risk assessment – POL/POMS should identify its bribery risks and prioritise its actions in high risk areas. - Due diligence – POL/POMS should take appropriate care when entering into relationships or markets with a risk of bribery. - Communication – POL/POMS policy should be clearly communicated to all	All	Paula Vennells Al Cameron Kevin Gilliland Nick Kennett Rob Houghton Martin Kirke Martin Edwards Mark Davies	Jane MacLeod	ABC policy Annual risk assessments and review of residual risks and controls Training to POL branches and employees Gifts and Hospitality register Guidelines and processes about giving/receiving gifts Risk and Compliance Team including Financial Crime and Compliance Teams	Policies and procedures on Intranet and updated annually. Completed risk assessments retained in restricted access drive. Risk assessment progress reported to AML Steering Group and R&CC. HR maintain training records for directly employed staff. Quarterly G&H records provided to each GE for their area. Annual reporting re. G&H to R&CC and ARC. Gifts and Hospitality register	[redacted]

POL00423693

		relevant parties, supported by appropriate training and "speak up" procedures. - Monitoring and review – the procedures put in place should be reviewed and updated as the company's risks change over time.				Whistleblowing Policy Code of Conduct Agreement clauses Financial Crime Policy		
Communications Act 2003	This is the primary source of telecoms and broadcasting regulation in the UK and sets out the authorisation regime, competition rules, access and interconnection, numbering and universal service obligations. Ofcom is the regulator.	Under this Act POL, as an Electronic Communications Services ("ECS") provider, is generally authorised to operate its Telecoms business provided that it complies with applicable conditions of Ofcom's General Conditions of Entitlement. POL has to act in accordance with consumer law in its telecoms and postal business activities.	FS & Telecoms Retail	Kevin Gilliland	Nick Kennett	Regulatory Team (Jono Hill) Fujitsu assists POL on compliance to technical service requirements as part of their managed service provision under the Telecoms MSA. Compliance programmes Vulnerable customer approach and Dunning 'bad debt relief' approach.	Regular external audits on billings. Other MI and Info submitted to Ofcom for published league tables etc.	[redacted]
Companies Act 2006	Contains statutory statement of directors' duties with seven key general duties. Directors' duties are owed to the	Directors: Duty to act within powers; Duty to promote the success of the company; Duty to exercise independent judgment; Duty to exercise reasonable skill, care and diligence; Duty to avoid	CEO LRG Operations		Paula Vennells Jane MacLeod Al Cameron	Company Secretary	Regulatory Tracker and monitoring of legislative developments.	[redacted]

POL00423693

	company, but directors must also consider the interests of the company's employees and creditors. Also governs consolidated financial statements/company accounts and auditing.	conflicts of interest; Duty not to accept benefits from third parties; and Duty to declare interest in proposed transaction or arrangement. Directors are responsible for the preparation, approval and filing of company accounts.						[redacted]
Corporate Manslaughter and Corporate Homicide Act 2007	Creates the offence of corporate manslaughter by organisations. No new duties obligations under the act, though it is specifically linked to Health & Safety requirements. Breaches can result in unlimited fines. Individuals within organisations can also face prosecution for Gross Negligence Manslaughter.	Provided POL takes their obligations under Health & Safety law seriously, they are not likely to be in breach of this act. POL should keep their Health & Safety management systems under review in particular the way in which their activities are managed or organised by senior management. POL needs to take into account appropriate health and safety guidance and ensure there are no attitudes, policies, systems or accepted practices within POL likely to encourage serious management failure or produce a tolerance of it.	Operations		Al Cameron	See entry "Health and Safety at Work Act 1974".	See entry "Health and Safety at Work Act 1974".	

POL00423693

Criminal Finances Act 2017	In force from September 2017. Creates a new corporate criminal offence for failure to prevent criminal facilitation of criminal tax evasion. Unlimited fine for failure to prevent (and no defence proven). Amends POCA 2002 to change the current SARs regime, provide enhanced powers (including disclosure powers) re proceeds of crime/money laundering and new Unexplained Wealth Orders regime (granted by High Court).	Focusing on point 1.): A 'failure to prevent' corporate criminal offence is placed on a 'relevant body' (e.g. POL) where it fails to prevent an 'associated person' (i.e. employees, contractors, sub-contractors, agents, consultants or any other persons providing a service for or on behalf of POL), from criminally facilitating criminal tax evasion (UK or equivalent offence under foreign law). The only defence is to have 'reasonable procedures' put in place to prevent facilitation by it 'associated persons' (or that it was not reasonable to have these).	All	Jane MacLeod Kevin Gilliland Nick Kennett Rob Houghton Martin Kirke Martin Edwards Mark Davies	Al Cameron	Financial Crime Policy	Working Group: Reasonable procedures (defence) Meeting agendas and minutes recorded - saved in Legal team shared drive	[redacted]
Data Protection Act 1998 & GDPR	Act requires data controller to process personal data in accordance with 8 principles. Stricter regime and penalties under GDPR (including fine up to 4% of global	When POL is determining the manner and purpose of the personal data it need to ensure the personal data is: 1. processed fairly and lawfully (cl 2 and 3) 2. only used for the specified and lawful purpose 3. adequate, relevant and not excessive	All	Al Cameron Kevin Gilliland Nick Kennett Rob Houghton	Jane MacLeod	Information Protection & Assurance Team DPA clauses in contracts Data Protection and Information Security Policies	GDPR Programme and appointment of Programme Manager (Clare D'Netto) / Steering Group - including review of POL material contracts and P-Suite. Data maps.	[redacted]

POL00423693

	turnover or EUR£20m, whichever greater). UK Data Protection Bill in progress - tbc.	4. accurate and kept up to data 5. not kept for longer than necessary 6. processed in accordance with the data subject's rights 7. processed with adequate technical and organisational measures Not transferred to a country that is outside the EEA unless ensures adequate level of protection. DSARs		Martin Kirke Martin Edwards Mark Davies		Training to business areas		[redacted]
Digital Economy Act 2017	The Act reflects the Government's modernisation of communications services. Changes are made to the law governing installation and maintenance of telecoms infrastructure, public sector data sharing, direct marketing activities, IP (copyright infringement) and provides powers for Ofcom to specific requirements regarding end-users switching communications providers and compensation for	Marketing – comply with ICO's code on Direct Marketing (breach of which is not an offence but is admissible as evidence in any proceedings). Property – to comply with reform of the ICO's Electronic Communication Code regarding telecom operators and landlords; amends the Landlord and Tenant Act 1954. Public sector personal data sharing – question of whether POL is a 'public authority' (definition is the same as under Equality Act 2010 and Immigration Act 2016 – which POL does not consider itself to constitute a 'public function'), also not listed as a 'Specified Person' under the Act.	Retail Operations FS & Telco Brand	Kevin Gilliland Al Cameron Mark Davies	Nick Kennett	GDPR Programme (re ICO's code on direct marketing)	Regulatory Tracker	[redacted]

POL00423693

	failure to meet performance standards.							
Enterprise Act 2016 (competition law)	Introduces a criminal offence for taking part in cartel activity. However, also introduces other important changes in relation to merger control, disqualification of directors for breaches of competition law, super-complaints to the CMA by certain consumer bodies.	POMS and POL must ensure that none of its directors is in breach of competition law. POL and POMS must also ensure that it deals with any questions or complaints from the CMA. FS (POMS): must ensure that it has mechanisms and controls in place to allow swift payout on insurance claims.	All	Martin Edwards Martin Kirke Rob Houghton Jane MacLeod Al Cameron Mark Davies Kevin Gilliland	Nick Kennett Kevin Gilliland	Regulatory Governance Manual HR team leading on apprenticeships Working Group for payment cap set up and includes representatives from HR, legal and public affairs Training provided to Directors		[redacted]
Environmental Legislation and Regulations	There are numerous other Environmental Regulations arising from the above Acts for example governing the following areas: - Permits required for the discharge of waste - Pollution prevention - Energy efficiency - Contamination of land waterways etc.	POL has obligations under most of these regulations. Example - The management of any discharge of heating oil, vehicle fuel at Supply Chain depots. Energy efficiency relates to gas electricity fuel usage etc. The waste concerned is produced owing to the supply by POL of equipment or other items to its administrative offices etc. DMBs for use or sale.	Operations		Al Cameron	Persons In Charge H&S Managers Property Managers CBRE/Servest	Environmental Tactical Group has been set up. Land - waste collection for non IT areas is managed via Servest contract and the service is monitored through a formal service review monthly. Our land waste compliance is high. Rubbish collection breaches on timings are also monitored with Servest to ensure any Local Authority penalties are addressed. Air - the risk is low. CRC is a CBRE service line and monitored through formal monthly service line reviews and our carbon is	[redacted]

POL00423693

	There are further regulations made under the European Communities Act 1972 Section 2(2): - Management of electrical and electronic equipment (WEEE) waste. - Management of waste batteries and accumulators. - Packaging requirements.						reported yearly. Our data accuracy (based on meter reads) is very high. Water - this is a low risk for property. CBRE monitor our physical controls (through interceptors) and we have checked these.	[redacted]
Environmental Protection Act 1990	The Act applies to England, Wales and Scotland. Its application is wide ranging. Breaches of Environmental Law are often criminal offences. They can result in: - Fixed Penalty Fines - Prosecution of a company or individuals for breach of health and safety - If convicted companies can face large fines, potentially unlimited if death has occurred.	It imposes upon POL general duties for waste management and releasing emissions into the environment. It sets out a regime for the regulation and licensing of the disposal of controlled waste on land, imposes a duty to remediate contaminated land and introduces the statutory nuisance regime. Impact on POL can be serious. Brand damage can occur as a result of the incident. Even more serious Fixed Penalty Notices may have to be revealed when POL is tendering for business.	Operations		Al Cameron	Compliance with all relevant obligations under this Act are managed by the Property Team (Property Compliance Manager) and the particular business areas. Health Safety Environment and Wellbeing team, external Specialists e.g. Servest who manage the collection, transport and disposal of our waste and the Legal Team.	The tactical group has set targets for environmental waste and has a plan to reduce our waste. Our record of progress against landfill targets and CRC is good and incidents are very low.	[redacted]

POL00423693

Equality Act 2010	The Equality Act 2010 protects people from discrimination in the workplace and in wider society. It replaced previous anti-discrimination laws with a single Act, making the law easier to understand and strengthening protections. It sets out the different ways in which it's unlawful to treat someone.	POL required to comply with provisions as an employer. POL is also a "service provider" ("concerned with the provision of a service to the public or a section of the public") in its DMB (directly managed branch) network and must therefore make reasonable adjustments to accommodate the needs of customers from various "protected groups" e.g. elderly and disabled.	All	Nick Kennett Kevin Gilliland Martin Edwards Rob Houghton Jane MacLeod Al Cameron Mark Davies	Martin Kirke	Legal team to manage risks. HR policies and processes to mitigate risk of unlawful behaviour. Network Team have defined process to assess new branch premises (both DMBs and agency) for suitability and accessibility. Legal team engaged with Network and HR teams.	Equality Act and Accessibility Policy available on intranet and also provided to agents.	[redacted]
Financial Services and Markets Act 2000 (FSMA) / FCA Handbook	POL: It is a framework for regulation of financial services within the UK. POL as an appointed representative for the BOI and POMS. POL must comply with applicable rules and obligations within FSMA. POL meets with the PRA as part of BOI relationship. Due to BOI relationship, POL is also subject to	POL: POL is under contractual obligations to comply with the regulations in relation to financial services it provides. As such, POL must observe and comply with rules and regulations applying to the financial services sector (otherwise it may be in breach of the appointed representative agreements). Banking Framework: SYSC 8 requirements. POMS: FSMA requires POMS to have appropriate protections for customers	FS Retail	Kevin Gilliland	Nick Kennett	POL: contractual arrangements with POMS and BOI, Appointed Representative Agreements with both principals. Sales Oversight Compliance Forum, Customer and Conduct Risk Committee for BOI. Joint Conduct and Customer Risk Committee.	Minutes of meetings, T&C reports, Monitoring reports e.g. VMS. Incident and breach reporting. Reporting to RCC and ARC.	[redacted]

POL00423693

	Funeral Planning Authority requirements. POMS: FSMA will apply to POMS as it is the regulated insurance intermediary and POL's principal. FCA Handbook: Imposes principles and rules on how customers can be approached, marketing and suitability of products and customers. Note: Consumer Credit Act 1974 (as amended) governs credit cards, loans and overdraft products. POL is an appointed representative of BOI in this respect and is covered under the AR Agreement.	within the insurance policies. FCA Handbook: POMS must ensure that marketing of the insurance policies is done within the guidelines of the Handbook. Principles 6 and 7 also apply: "pay due regard to the interests of its customers and treat them fairly" and "pay due regard to the information needs of its clients and communicate information to them in a way which is clear, fair and not misleading".				POMS: contractual relationship with POL; Regulatory Governance Manual; Compliance review; Vulnerable Customers Policy; Training & Competence Policy; Financial Promotions Policy; Complaints Handling & Review (BOI undertakes); Quality Monitoring; Conduct compliance manual; Quality of Sales MI; Staff Vetting Policy - Martin Kirke; Success Factors and PO Money Academy.		[redacted]
Freedom of Information Act 2000 / Environmental	Provides public access to information held by public authorities by	As a public authority, POL is directly affected by this legislation and must publish or disclose certain information about its	LRG		Jane MacLeod	Information Rights Manager Case-by-case evaluation of	FOIA Procedures Guidance 2012 (needs updating) for Freedom of Information and Environmental	[redacted]

POL00423693

Information Regulations	obliging them to publish certain information about their activities and entitles the public to make requests for information from public authorities. ICO is the relevant regulator and will investigate complaints made against public authorities and produce decision notices - (can be appealed) failure to comply is contempt of court, punishable by fine.	activities and performance. POMS is affected by the virtue of being POL (100% owned) subsidiary and contractual relationships with POL. When receiving written requests for information from member of public, POL would have to consider the application, tell the applicant whether the information is held and provide it unless an exemption applies. A breach is committed where: failure to respond adequately to requests for information; failure to adopt model public scheme or do not publish correct information and deliberately destroying, hiding or altering requested information to prevent its release.				requests received, collation of information and preparation of replies and review of data collated, redaction where required. Management of cases needs to take into account DPA 1998 and ROPSI.	Information Regulations is held on the FOIA restricted drive. Includes Guidance for the Information Rights Team and Information Law Panel, for business areas and for public-facing staff. Numerous templates to assist the management of the processes, spreadsheets to monitor and manage workloads and evidence compliance.	[redacted]
Gross Negligence Manslaughter	An individual may be prosecuted for this crime where a death results from their unreasonable significant gross negligence. An individual's actions would have to be more than simply careless or negligent. There actions would need to be so unreasonable as	Provided the individual takes their obligations including those to be exercised on behalf of POL under Health & Safety law seriously they are not likely to be prosecuted for Gross Negligence Manslaughter.	Operations Retail	Kevin Gilliland	Al Cameron	See entry "Health and Safety at Work Act 1974".	See entry "Health and Safety at Work Act 1974".	[redacted]

POL00423693

	to be grossly negligent and criminal.							[redacted]
Health & Safety at Work Act 1974 and various related Regulations	Section 37 H&SW Act - where an offence has been committed by a company attributable to the consent, connivance or neglect of any director, manager or other similar officer of the company that person shall be guilty of an offence and liable to criminal prosecution and punishment. - Management of Health and Safety at Work Regulations 1999 – imposes a duty to carry out suitable and sufficient risk assessments which are the cornerstone of health and safety management - Construction (Design and Management) Regulations 2015 – imposes obligations on all parties involved in construction	General duty to 'ensure so far as is reasonably practicable the health, safety and welfare at work of all their employees'. Breaches often criminal offences and large fines. Provide and maintain safety equipment and safe systems of work; ensure materials used are properly stored, handled, used and transported; provide information, training, instruction and supervision - ensure staff are aware of instructions provided by manufacturers and suppliers of equipment; provide a safe place of employment; provide a safe working environment; provide a written safety policy/risk assessment look after the health and safety of others, for example the public; talk to safety representatives. The Act also imposes duties on POL in relation to those entering upon premises that it controls, e.g. contractors and visitors and in a more limited way: POL's wider undertaking.	Operations HR Retail	Kevin Gilliland	Al Cameron Martin Kirke	H&S Committee / Legal and external law firms / CBRE / Servest Property Compliance Managers, Equipment Managers and Persons In Charge, Health, Safety & Environment team Health & Safety Policy Risk assessments, safe systems at work, training and compliance checks undertaken and evidence capture Various audits (Asbestos): Draft Asbestos Management Plan	Advice, guidance and policies on H&S sharepoint/intranet. H&S Business Partners and Head of Property Compliance hold documentary evidence of compliance. Collation of Certificates of Compliance, issue and monitoring of H&S Activity Calendars. Monthly Operations Safety Board and Supply Chain Risk Meeting, Quarterly National and Regional H&S Consultation Meetings, Road Risk Forum and 6 monthly Group Executive H&S Committee 'deep dive' meetings. Training to GE, Lead teams and across business teams as required. Trade Union H&S Reps Inspection reports. Property statutory compliance surveys.	[redacted]

POL00423693

	works and projects. Other regulations not arising out of the Health and Safety Act 1974: Regulatory Reform (Fire Safety) Order 2005 imposes obligations in relation to fire risk assessments, management of Fire Safety and enforcement sanctions (including prosecution) for breach of the Order and The Control of Asbestos Regulations 2012 (CAR 2012).							
Insurance Mediation Directive (IMD) & Insurance Distribution Directive (IDD)	IMD: Removes the barriers to a single market for insurance and reinsurance intermediation. Authorised firms must allocate responsibility of the firm's insurance mediation activity to a director or senior manager. IDD:	IMD: If POMS carried out an insurance mediation activity it must: - must be authorised by a relevant competent authority; - are subject to certain obligations relating to systems and controls, regulatory capital, client assets and approved persons; and - are regulated with respect to the way that they communicate with clients, issue financial promotions (including	FS Retail	Kevin Gilliland	Nick Kennett	Registration with the FCA Regulatory Governance Manual POMS Compliance team	Project Athena currently managed by Christelle Losa (including weekly updates) is in relation to the revised guidance by the FCA on compliance with IDD. Project team has been established and we are on-track with adherence to the timescales required by the FCA. All policies are signed off and reviewed by Steering Committees within group and are stored on Sharepoint.	[redacted]

POL00423693

	Enhances consumer protection, promotes competition and establishes pan-European level playing field by harmonisation. IDD will be enacted via FSMA and FCA rules in the UK. Enters into force in February 2018.	content), handle claims and advise on, sell and cancel products.						[redacted]
Intellectual Property Laws (various)	Key legal rights for PO: trade marks, domain names and goodwill. Key legislation: Trade Marks Act 1994 and Copyright, Designs and Patents Act 1988.	Protection of PO's IP rights and brand - maintaining, enforcing and defending.	Brand		Mark Davies	Standard agreements: e.g. PO Trade Mark and Copyright Licence Agreements	PO Brand Guidelines Draft Brand Terms of Reference Template agreements/schedules on Legal team shared drive	[redacted]
Modern Slavery Act 2015	This Act creates an obligation on a business to publish a statement about the steps it has taken to ensure that slavery and human trafficking are not taking place in any part of the business or any part of the supply chain.	POL obligations: Undertake due diligence of supply chains. Prepare and publish an annual statement of compliance within 6 months of year end.	HR Operations Retail	Al Cameron Kevin Gilliland	Martin Kirke	Working Group set up and led by HR representative from Procurement, Legal, HR and Retail.	Modern Slavery Statement due to be signed off by the Board in October 2017 - to publish on POL intranet. Whistleblowing Policy updated to include MS; Code of Business Standards will do the same. Assessed Post Office procurement process to ensure aligns with MSA and reviewed standard form	[redacted]

POL00423693

	Introduction of three criminal offences - slavery, servitude and forced or compulsory labour; human trafficking; and committing any offence with the intent to commit human trafficking. Failure to prevent modern slavery can lead to criminal and civil prosecution.						procurement contracts. PQQ process amended to take account of MSA. Suppliers must now confirm that they comply with the MSA and provide a copy of their statement. Reviewed Postmaster contracts and issued Guidelines for Postmasters to assist them in complying with MSA.	[redacted]
Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017)	Regulations that govern Money Service Businesses, such as POL, due to the fact that it provides currency exchange and money transmitting services. A board member or senior management member must be appointed as officer responsible for compliance with MLR 2017. A nominated officer must also be appointed.	POL must maintain up to date premises register with HMRC of all premises where regulated activity is undertaken. Fit & Proper tests must be undertaken. POL must have adequate mechanisms for receipt, review, investigation and disclosure to the NCA of SARs. POL must undertake risk assessments and carry out 'customer due diligence' measures to check that your customers are who they say they are and that there is no evidence of ML or TF. It must also put in place internal controls and transactions monitoring systems. The nature of these controls will depend	FS Retail LRG	Kevin Gilliland	Nick Kennett Jane MacLeod	Anti-money laundering provisions in contracts ABC, AML/CTF, Financial Crime Policies AML Steering Group and Financial Crime Governance Forum Risk assessments for all new/changed products and services Annual training, awareness and comms plan	Policies on Intranet and updated annually. Completed risk assessments retained in restricted access drive, progress reported to AML Steering Group and R&CC. HR maintain training records for directly employed staff. Branch Standards Team maintain records for Network training. SAR reports are monitored monthly by Head of Financial Crime all records filed in restricted access drive.	[redacted]

POL00423693

	Extensive provision for the investigation of breaches and civil enforcement action/criminal prosecution where breach found. The FCA prosecutes criminal offences under MLR. Note: the government has also proposed a new offence making the company criminally liable for failure to prevent economic crime, including money laundering. This is likely to be a strict liability offence, with the defence being adequate procedures put in place - likely to come into force in late 2017.	on the size and complexity of POL, including the number of customers it has and the number and type of products and services it provides. Also contractual commitments for MLRs with MoneyGram, Partner Banks, Gift Cards etc.				including training to the business via Success Factors Training to the branches Advice provided by external firms		[redacted]
Payment Services Regulations 2017	It is the key payment-related legislation setting out the framework for standardisation of the payment institutions, minimum	PO must ensure it is compliant with the following areas: - Cash deposits and withdrawals - Payment card transactions - e.g. travel money and e-money requirements	FS Retail	Nick Kennett	Kevin Gilliland	PSD2 mapping of products	Complaints data (regime was complaints based supervision until July 2017).	[redacted]

POL00423693

	standards in the payments area and increased transparency and protection for customers. The FCA, using regulatory powers, deals with enforcement of PSR which may impose public sanctions (penalties/censures) and can instigate criminal prosecutions on firms authorised under PSR for breaches. Also able to order firms to provide restitution to customers and cancel authorisations.	- Money remittance - Payments sent through the intermediary of a telecom, IT system or network operator						
Privacy and Electronic Communications Regulations 2003 (PECR) / Network and Information Security Directive (NIS Directive)	This Act gives individuals specific privacy rights in relation to electronic communication.	The Act complements the Data Protection Act and contains rules on marketing calls, emails, texts and faxes, cookies (and similar technologies), keeping communications services secure and customer privacy regarding traffic and location data, itemised billing, line identification and directory listings.	LRG FS& Telecoms		Jane MacLeod Nick Kennett	Information Protection & Assurance Team (led by Jules Harris) and Telecoms team (led by Meredith Sharples). PECR clauses in relevant contracts (e.g. IT Towers agreements).	ISO27001 ISMS Certification supports objectives of PECR. ISO compliant policies regarding Information Security/management of information. Policies located at the IPA Intranet page e.g.: Acceptable Use Policy, Information Assurance Policy, Cyber Information Security Policy, PCI Compliance Standard, Information Classification	

POL00423693

						DPO role within IPA provides subject matter expertise to the business regarding compliance with PECR.	Standard, Access Control Standard. PCIDSS Certification - customer card payment transactions. Telecoms will be subject of a PECR Audit in Q1 2018 conducted by the ICO - management and control of the contract between POL and Fujitsu will be assessed.	[redacted]
Public Interest Disclosure Act 1998 / FCA SYSC 18.4 (whistleblowing)	To protect whistleblowers from detrimental treatment or victimisation from employers after making a qualifying disclosure. FCA SYSC - (POMS) protection of whistleblowers from being victimised from disclosing 'reportable concerns' (including protected disclosure, breach of firm's policies and procedures and behaviour that harms or likely to harm reputation or financial well	Qualifying disclosures are disclosures of information where the worker reasonably believes (and it is in the public interest) that one or more of the following matters is either happening, has taken place, or is likely to happen in the future: A criminal offence; breach of a legal obligation; a miscarriage of justice; a danger to the health and safety of any individual; damage to the environment; deliberate attempt to conceal any of the above. New FCA rules in 2016 on whistleblowing means firms must have a whistleblowers' champion in place - this should be a non-executive director or senior manager who will need to report to the board	All	Nick Kennett Kevin Gilliland Martin Edwards Martin Kirke Rob Houghton Jane MacLeod Al Cameron Mark Davies	Martin Kirke	Whistleblowing Policy	Whistleblowing Policy on POL intranet, comms issued to employees and Postmasters.	[redacted]

POL00423693

	being of the firm).	on whistleblowing stats, at least on an annual basis.						
s.3 Small Business, Enterprise and Employment Act 2015 / The Reporting on Payment Practices and Performance Regulations 2017	Duty to report on payments practices and performances. Rules require large companies (meeting certain thresholds) to publish information about their payment practices and performance regarding supplier invoices, twice a year on a government web service.	Currently, POL and FRES must report from September 2018. Possibly POMS. Failure to comply will be a criminal offence by the company and every director of the company will be liable, punishable on summary conviction by a fine not exceeding level 5 on the standard scale. If a company fails to publish a report by the required deadline, a director will not be liable if the director has taken all reasonable steps to ensure compliance.	Operations Brand	Mark Davies	Al Cameron	POL is piloting the obligations in advance of September 2018. Finance is currently working with Accenture for system developments that allow the reporting to be delivered. Working with internal community to ensure procedures are understood and followed to ensure prompt payment. Updating vendor T&Cs to ensure these are followed to ensure prompt payment.	Internal report produced/circulated on the impact of the duty to all Post Office entities. Information held by the AP team in FSC on current performance and future reporting. Working Group chaired by Ben Foat - action points recorded.	[redacted]
Senior Managers & Certification Regime	Introduction of senior managers' statutory duty of responsibility - to take reasonable steps to prevent regulatory breaches in their area of responsibility (no	POMS likely to be an 'enhanced' SM&CR firm. Example of some core/enhanced regime requirements: - ensure clear allocation of various designated senior management responsibilities.	HR FS		Martin Kirke Nick Kennett	Conduct Risk Policy Regulatory Governance Manual	Project Atlas has been commissioned and POMS has established its internal team and governance structure and has contracted with Thistle Initiatives to provide external support and industry guidance.	[redacted]

POL00423693

	longer a presumption of responsibility). The Regime applies to staff in roles that can cause 'significant harm' to either the firm or its customers. The regime has been extended to all FSMA authorised/FCA regulated firms includes POMS (solo regulated), to take effect in 2018 (most likely end of 2018). The Conduct Rules (replaces 'Approved Persons' regime) has been extended to apply to all directors, including NEDs. The FCA is able to enforce these directly against directors, such as where a NED fails to act with honesty and integrity. If the firm takes action against the individual for breach of the Rules, it must be	- develop "Statements of Responsibilities" to record the allocation of responsibility to individual Senior Managers. - "Responsibilities Map" to be a single document describing the POMS' management and governance arrangements in order to demonstrate that there are no gaps in accountability. - Regulatory references Possible extension to appointed representatives and Head of Legal (awaiting further FCA consultations) - tbc.					Project manager, Ben Spencer White, is in place and the project has commenced. Final consultation only just issued by FCA in August 2017 with view to implementation during mid to late 2018.	[redacted]

POL00423693

	reported to the FCA. Burden of proof to show senior manager failed to meet expected standards in an enforcement action lies with the FCA.							
Trade Unions and Labour Relations (Consolidation) Act 1992 (TULRCA)	TULRCA is a complex piece of legislation that consolidates the law relating to trade unions. It also covers industrial action.	Key aspects of TULRCA include: Trade Union obligations: Rights of trade union members (including in relation to union membership and activities) Collective bargaining rules Redundancy and the duty to consult collectively Obligations for trade union immunity for loss caused by industrial action	HR		Martin Kirke	IRSG GEIRSG (where legal is represented) All communications with the unions are sent to legal for sign off	Collective Agreements are located on Legal Shared drive and copies are also with external panel Firm Bond Dickinson.	[redacted]
Treaty on the Functioning of the European Union (TFEU) articles 101 and 102	The Act provides updated framework for identifying and dealing with restrictive business practices and abuse of	Ensure ongoing compliance with European and competition UK law. Examples of relevance: Network / restrictions Public procurement	All	Martin Edwards Jane MacLeod Martin Kirke	Kevin Gilliland Nick Kennett	Assess compliance on a continuous basis taking into account changes in legislation and Brexit	Monitoring of legislative developments and Regulatory Tracker	[redacted]

POL00423693

Competition Act 1998	dominant market position. European and UK competition law requirements.			Rob Houghton Al Cameron Mark Davies		Consider competition law implications in existing and new agreements Training employees/stakeholders Include competition law requirements in code of conduct Restrictions Policy Dawn Raid Policy (draft)		[redacted]
Value Added Tax Act 1994	The legislation for the payment of VAT.	POL is obliged to comply with HMRC's requirements regarding the payment and accounting for VAT.	Operations		Al Cameron	Monitoring of any adjustments in VAT regime. Accurate calculation of VAT, filing of VAT returns, payment of VAT.	Qualified tax professionals undertake the indirect tax work on a day by day basis. The firm undertakes wider development to ensure that the professionals are up to date with latest legislative changes and have access to the latest tax legislation and working papers (e.g. Tolleys library). POL also have access to KPMG LLP,	

POL00423693

							to discuss any complex indirect tax areas / seek reassurance where appropriate. VAT payment dates have remained consistent for a number of years and in line with the expectations of trained tax professionals. Direct debits are set up for VAT payments to reduce the risk of omissions.	

POL00423693

6.2 Procurement Compliance Reporting

Author: Barbara Brannon Sponsor: Al Cameron Meeting Date: 13 September 2017

Executive Summary

Context

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

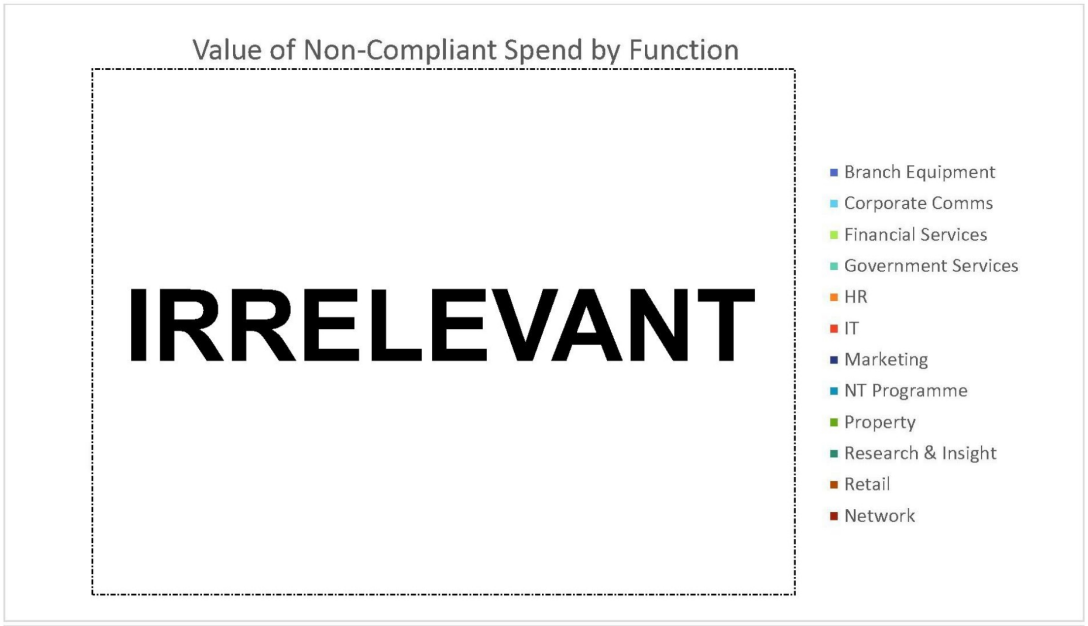
Failure to abide by the legislation or "slicing and dicing" contracts exposes POL to risk, both as far the commercial outcomes of the contracts as well as the reputational damage, legal remedies, censure & fines that can follow the discovery of a breach. Our compliance to PCR can be requested under a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

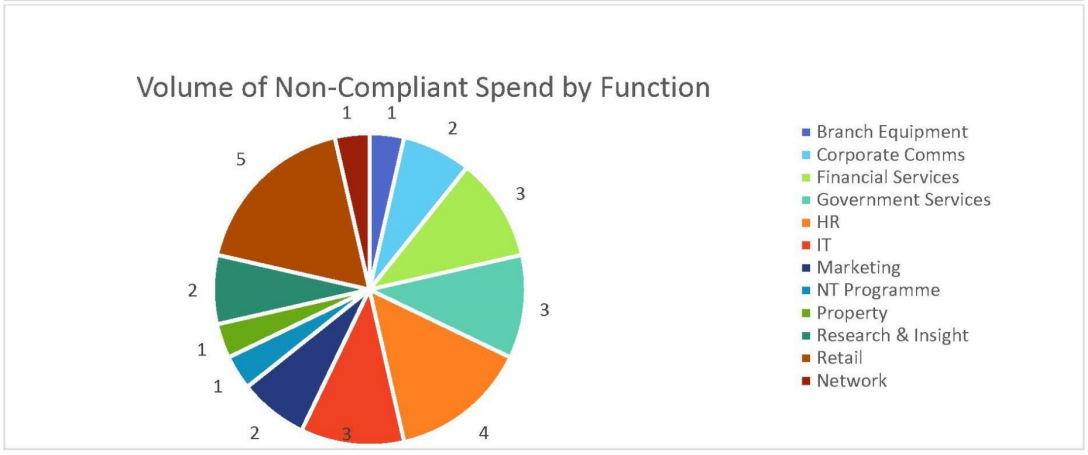
The PCR Compliance Register allows for the tracking of breaches to PCR regulations at the Post Office and internal governance processes. One aim of collating this information is to drive improvement in awareness and compliance behaviour across the organisation. The second and primary aim is to work with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

Questions addressed in this paper

1. *How many and what types of procurement non-compliance have occurred in the past quarter?*
   Since January 2017 there have been a total of 28 non-compliant incidents, 23 of which are direct awards in breach of PCR regulations documented by the Procurement Team. The remaining 5 are in breach of internal governance but not of PCR regulations. Minor breaches are often captured after an external commitment is made when invoices are presented for payment but in the main, these tend to be of low value and risk and are reducing in frequency.

POL00423693





Function	Sum of Value
Branch Equipment	
Corporate Communications	
Financial Services	
Government Services	
HR	
IT	
Marketing	
NT Programme	
Property	
Research & Insight	
Retail	
Network	
Grand Total	

IRRELEVANT

POL00423693

One non-compliant incident in particular skews these numbers, IRRELEVANT [revenue] against a 12 month extension of the Global Payments contract.

Global Payments has become non-compliant on a technicality of PCR, in that the value of the contract now exceeds that which was advertised during a fully compliant process. A legal review has deemed the remaining 24 month contract extension period to be low risk and Procurement and Retail are actively working on the strategy for re-Procurement in due course. IRRELEVANT represents the expected revenue for the next period and a further IRRELEVANT is forecast for the final period of the contract as we go through the award process for the new contract.

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

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

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

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

POL00423693

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

Conclusion

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

The YTD non-compliance value is potentially very high at IRRELEVANT due to the Bank of Ireland and the Global Payments extensions. A more realistic figure illustrating a typical run rate however is IRRELEVANT. Individually, all large value non-compliant contracts have been reviewed by appropriate Post Office governance forums with agreement on next steps and actions towards remediation allocated where appropriate.

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

Input Sought

Review and note content only. Please advise of any suggested improvements or additional information required for the next quarter and whether this forum is an appropriate one to receive a forward "look ahead" of 3rd party contracts with pending PCR issues.

POL00423693

The Report

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

A full explanation of the individual compliance breaches is attached in Appendix 1. Each entry details the nature of, and the value of the breach.

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

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

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

Nine contracts were entered into during this period without compliance to internal governance processes on contract and commercial review. All were for awards of between £0 and £50,000.

3. *Why were the approvals given?*

The rationale for approval is relevant to the individual service and is detailed within Appendix 1.

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

There were no unapproved, material breaches during this period.

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

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

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

POL00423693

on a tactical basis to extend contractual services while public tender processes are executed.

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

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

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

POL00423693

Appendix 1 Extract from Procurement Compliance Report

Incident Ref No	Date	Function	GE Member	Value	Supplier Name	Breach Type 1 - PCR Threshold	Breach Type 2 - Internal Governance	Event (what happened) ONLY FOR £25K>	Cause (why did it happen) ONLY FOR £25K>
2017/0008	20 March 2017	Government Services	Kevin Gilliland	IRRELEVANT		PCR - >£164.5k	No CAF	Initial contract awarded following a non-compliant tender process (RFI with selected Bidders v full OJEU). 2 years "build/dev" work undertaken at risk by Digi (pending formal award to POL under the Government FWA (Cabinet Office) for Identity Assurance) which was not to become effective until sign off of the Call Off Contract [27/03/15] for 21 months to 26/12/17 with 3 x 12 months options to extend. Challenge period for original award is now time barred but any extension option called off will initiate a new time limit for challenge. In re-drafting the a second Agreement to flow down additional terms from Cabinet Office the Term appears to be back dated to 21/09/13 for 21 months taking the 3 x 12 month extension options to 20/06/18.	Initial Contract awarded following an RFI process and not full PCR.
2017/0009	21 March 2017	Research & Insight	Paula Vennells			PCR - >£164.5k	Expired Contract	Voice of Customer tracking is used as a performance measure for the business. It used to be a measure for the whole business but is now a measure for the individual Post office's performance	It was developed as a performace tracker with a framework supplier. The supplier then split the business and this work was then novated to the new entity - due to it being a performance measure POL could not stop and start an OJEU procedure as we would loose the data and would not be able to legitimise and new trakcer without running in parrallel tracker, TThe cost and internal resource requiremetns for which would have been prohibitive at teh current time.
2017/0010	22 March 2017	Retail	Kevin Gilliland			PCR - >£164.5k	Compliant	The original Vow Agreements 1) DMBs and 2) Wholesale & Online were compliant awards following a public PCR procedure, covering for a period of 5 years to 31/07/16.	Re-procurement was planned in a timely manner but Project Paddington delayed it's launch, so that the re-procurement was unlikely to be completed prior to Contracts expiry, 31/07/17.
2017/0011	22 March 2017	Retail	Kevin Gilliland			PCR - >£164.5k	Out of Scope of Contract	The Original Global Pay Agreement was compliantly awarded under a public PCR procedure, covering a period of 5 years to 08/05/17. With TWO x 12 month options to extend. NB The spend includes for 90% onward payment by GP to Visa & Mastercard	POL is looking to exercise its option to undertake the first 12 month option to extend to 08/05/17, however the original value was advertised between IRRELEVANT. Spend forecast to 08/05/417 is estimated IRRELEVANT in, which will exceed the forecast range, with TWO further 12 month options to extend.
2017/0012	22 March 2017	Government Services	Kevin Gilliland			PCR - >£164.5k	Expired Contract	The original BOI/POL ATM Agreement was not let via a Public Procurement. In addition there was a period of implementation so ATMs start falling out of individual contract terms between May 17 - March 21.	The Original Agreement (as well as being awarded outside of a public procurement) has not been structured in a way that brings the ATMs co-terminus with the final contract end date (Mar 21)
2017/0013	23 March 2017	HR	Martin Kirke			PCR - >£164.5k	Expired Contract	Requirements and HR personnel changed. OLD PSL fell into disuse.	Re-org meant an immediate requirement for a lot of concentrated recruitment
2017/0016	12th April 2017	Marketing	Nick Kennett			PCR - >£164.5k	Expired Contract	Latest requisition is sub-OJEU threshold but there are several per month that support mainly Credit Cards, Loans and Mortgage products.	Originally appointed compliantly following an OJEU process in 2012. All compliant extensions now exhausted.
2017/0019	01 June 2017	HR	Martin Kirke			PCR - >£164.5k	No CAF		There is a contract with Towers Watson although it has been in place for IRRELEVANT and the spend will have exceeded IRRELEVANT That said Towers know about the pension arrangements and going forward the spend is likely to be below [redacted] per annum
2017/0028	01 May 2017	Financial Services	Nick Kennett			PCR - >£164.5k	Compliant	Continuation of POL CRM system. 1 year award. Awaiting strategy.	Continuation of RMG system, no desire / plan to move away from provider. Awaiting CRM strategy.

POL00423693

Appendix 1 Extract from Procurement Compliance Report

Incident Ref No	Actions Taken ONLY FOR £25K>	Further Planned Actions ONLY FOR £25K>	Action Owner ONLY FOR £25K>	Due Date/ completed ONLY FOR £25K>
2017/0008	Circular references in the Government FWA, Call Off Contracts, Order Forms, lack of documents, and signed documents stored in a central location (and the same in the Digidentity Agreements) has made ascertaining the start and end dates of the Agreements very complex. This was further compounded by additional terms being put on POL by CO which needed to be flowed down to Digidentity and in the drafting the second Digidentity Agreement terms have been inadvertently shortened and appears to have been back dated to 21/09/13 for 21 months taking the 3 x 12 month extension options to 20/06/18.	Pending direction from Cabinet Office as to what their intention is for extension of POLs current Call Off Contract which runs to 13/04/17 (for NEW identities and 13/07/18 to maintain those users processed to 13/04/17). The Gvt FWA runs to 23/03/18, with the ability to extend for a further ONE year period to 23/03/19. In theory CO could therefore place a new Call Off Contract on POL for a period of 3 years (2 years NEW, 1 year maintenance) ON NOTICE potentially to 23/03/22. POL working with external legal (Bond Dickinson) to assess the risk of extension v re-procurement once we have latest indication from CO on extension of the current Call Off. It is planned for a Supplemental Agreement to correct the dates and to show a continuous Agreement from award to cover for the extension option yet to be agreed (dependant on risk).	Jonathan P Evans	20/04/2017
2017/0009	Due to the tracker still being an important measure for the individual post offices the suppleris contracgt will be extended.	Once POL understands how it wants to measure performance a review of current CCS framework that may be applicable or an full OJUE for the trakcingf requirement will be conducted.	Ruth Moyer	
2017/0010	To secure supplies beyond 31/07/16, whilst undertaking a re-procurement exercise, contract extensions were placed for a period of 9 months to 30/04/17. As outside of the originally advertised OJEU notice these are non-compliant awards. Judged to be low risk during a procurement exercise for a short term extension. The initial extension also covered an option to further extend by a second period of 9 months and this is now being undert aken to further extend (non-compliantly) to 31/01/18. This is required as the re-procurement exercised was cancelled given the material changes being undertaken to POLs DMB strategy.	POL is reviewing its DMB strategy and contracting options for its retail space to optimise revenue for the reducing branch network. A GE paper is planned for 10/04/17 (outside formal monthly GE, 20/04/17)	Keith Maples	10/04/2017
2017/0011	The reason for the overspend has been an underforecast of (counter) transactions by POL together with an increase in on-line transactions, but in addition regulated changes to the interchange rates have increased cost to POL (outside of POLs control).	Legal advice is being sought on the procurement risk to be presented to GE, 20/04/17. POL will be retending this and will start the re-procurement planning to allow for the public re-procurement together with a 12 month implementation time to award a new contract 09/05/18.	Nick Spicer	20/04/2017
2017/0012	[redacted]	Strategy paper being developed as to POLs approach. There are additional complexities, as this will be affected by interchange rates which is currently under review by LINK members, the changing DMB strategy, Government funding under SGEIs, the DWP Poca Agreement and the relationship with BOI.	Andrew Goddard	30/04/2017
2017/0013	As a temporary measure, a short term agreement with standardise commercial terms and fees has been implemented with approximately 50 suppliers. The agreement effective from 1st July 2017 is in place until 31st March 2018 with an option to extend if necessary.	Waiting for the release of the new CCS (Crown Commercial Services) framework due in March 2018. As a full procurement process to implement a PSL would take over 12 months to complete, we have been advised to wait until details of the CCS framework are available before we agree next steps. Update meeting with Procurement and Legal arranged for January 2018.	Stacie Drury	12-Apr-17
2017/0016	Seeking proposal from Carat (Media Agency) for consolidation within their compliantly let contract.	If proposal is acceptable from Carat then consolidate with them enabling an integrated approach to our full media investment.	Louise Fowler	Jul-17
2017/0019	It was agreed to close the RMPP (DB Pension scheme) in 2016, closure required actuarial advice from a provider that knew the history and complexity of the RMPP. It was necessary to keep Towers Watson for their expertise.	In line with the Board strategy to de-risk the RMPP as far as possible, PO has requested that the Trustee of RMPP look to buy-out the liabilities of the RMPP as soon as possible whilst not requiring further money from PO. The earliest this can happen is 1 April 2018. It is anticipated that the majority of RMPP liabilities will be bought out by 1 April 2019 at the latest. Actuarial advice will be required during this phase. Anticipated spend to 2019 will be IRRELEVANT If buy-out occurs in 2018 spend will IRRELEVANT		
2017/0028	Non-compliant extension in place	CRM Platform to be re-tendered as it has previously been purchased non-compliantly. Awaiting strategy and confirmation of requirements from IT before Procurement approach can be agreed. Renewal due in April 2018.	Jaco Vermeleun	31/12/2017

POL00423693

6.3 Criminal Finances Act Update

Author: Ben Foat Sponsor: Jane MacLeod Meeting date: 13 September 2017

Executive Summary

Context

The Criminal Finances Act 2017 (Act) comes into force on 30 September 2017 and introduces a new corporate offence of failing to prevent the facilitation of UK and foreign criminal tax evasion. The penalty for non-compliance is a criminal corporate offence and potentially unlimited fine.

Post Office Limited (Post Office) applies a zero tolerance policy to criminal tax evasion and the criminal facilitation of criminal tax evasion as set out in its Financial Crime Policy. It is committed to preventing such facilitation within all parts of the business.

This Act was identified by the Legal Team via the Regulatory Developments Tracker and communicated to the business through the Law & Trends Forum. A cross functional working group was consequently set up to manage the new obligations imposed by the Act.

Questions addressed in this report

1. What does the Act stipulate and what are the consequences of non-compliance?
2. How does it apply to Post Office?
3. What have we done?
4. Who is accountable?
5. What do we need to do next to progress?

Conclusion

1. The Act provides that it is a criminal offence where a relevant body, such as Post Office, fails to prevent an associated person from criminally facilitating criminal tax evasion of another. Consequently, Post Office must implement reasonable and proportionate procedures to prevent its associated persons from criminally facilitating criminal tax evasion of another person. The penalty of non-compliance is a criminal corporate offence as well as a potentially unlimited fine.
2. It has a broad application to Post Office as the Act applies to all associated persons including employees, postmasters/agents, suppliers, contractors and consultants.

POL00423693

3. A working group has been set up to advise the business of the enhancements needed to existing systems and implementations necessary (to prevent criminal tax evasion and its facilitation) to ensure that Post Office can avail itself of the "reasonable procedures" defence. For example, Post Office has introduced new obligations on our postmaster agents, contractors and suppliers to ensure that they (and their associated persons) comply with the requirements of the Act.
4. The relevant business areas are responsible for implementing the recommended reasonable precautions (from a first line of defence). Legal and Financial Crime together with the working group are responsible for second line of defence risk management.
5. The working group will continue to progress its implementation plan including assessing due diligence processes, support with communication as well as providing recommendations regarding ongoing monitoring and review to ensure Post Office complies with the Act.

Input Sought

1. The Committee is asked to note the paper.

Input Received

2. Criminal Finances Act working group has provided input into this paper.

POL00423693

The Report

What does the Act require?

Post Office applies a zero tolerance policy to criminal tax evasion and the criminal facilitation of criminal tax evasion as set out in its Financial Crime Policy. It is committed to preventing such facilitation within all parts of the business.

Purpose of the Act

The Act is intended to tackle money laundering and corruption, recover the proceeds of crime and counter terrorist financing. The Act introduces two new corporate offences of failure to prevent facilitation of tax evasion (criminal UK tax evasion and foreign tax evasion) and amends the Proceeds of Crime Act 2002 and anti-terrorism legislation. This Report focuses on the new "failure to prevent" offence.

Offence

In summary, a relevant body (Post Office) may be prosecuted for the "failure to prevent" offence if an associated person (employees, postmasters/agents, suppliers, contractors or any other person acting for or on behalf of Post Office) criminally facilitates either a UK or foreign criminal tax evasion committed by another person. The aim of these offences is to hold relevant bodies (companies and partnerships) to account for its associated persons where criminal facilitation is committed in respect of criminal tax evasion offence by another.

There must be both criminal tax evasion by a third party and criminal facilitation by the associated person. If the associated person only accidentally, ignorantly or negligently facilitated tax evasion, or tax evasion had only arisen accidentally, ignorantly, negligently or there is no criminal tax evasion but instead tax avoidance, then the "failure to prevent" offence is not committed by the relevant body.

Reasonable Procedures Defence

It will be a defence for Post Office to show that it had reasonable procedures in place to prevent such facilitation, or that it was not reasonable to expect it to have such procedures. The HMRC Draft Guidance of October 2016 notes that the Act does not hold relevant bodies to account for their customers' tax crimes or require the relevant body to prevent customers from committing tax evasion. Its purpose is to encourage businesses not to turn a blind eye to instances where their associated persons have deliberately assisted another person to evade tax.

The question of reasonableness is to be determined by the context or surrounding circumstances. The draft HMRC Guidance also recognises that the "reasonable procedures" defence is both risk-based and proportionate and so the regime cannot be a zero failure regime. It suggests that businesses follow a similar approach under the Bribery Act:

1. Risk assessment

POL00423693

2. Proportionality of risk-based prevention procedures
3. Top-level commitment
4. Due Diligence
5. Communication (including training)
6. Monitoring and Review

Whilst there is no previous case law on this new offence, the tone of the Guidance and the experience to date of prosecution and deferred prosecutions under the Bribery Act underline that its aim is to target those who deliberately turn a blind eye to wrongdoings and ignore what is happening within their businesses.

How does it apply to Post Office?

The working group identified 3 areas which present the highest risk to Post Office:

1. Agent/postmaster network
2. Contractors
3. Suppliers

Example -
If a postmaster deliberately and dishonestly facilitated (e.g. aided and abetted by being actively involved) in deliberate and dishonest tax evasion of a UK tax by a UK tax payer (e.g. postmaster assistants, staff, customer) and both are proven beyond reasonable doubt where Post Office cannot show that it had put in place reasonable procedures (or that these would not have been reasonable to have) to prevent such facilitation by its agents/postmasters then Post Office will be liable and subject to a criminal corporate offence with a financial penalty.

Employees, such as those in procurement, may also present a risk because of the nature of their job and the pressures that will undoubtedly often arise on timing and cost of procuring services.

What have we done?

A cross functional working group consisting of Legal, Financial Crime, HR, Finance & Ops, Procurement and Retail is working through how Post Office can avoid failure to prevent criminal facilitation of criminal tax evasion by ensuring that it implements proportionate and reasonable procedures as follows:

Key Areas of Risk	Reasonable Procedures
Agent/Postmaster Network	1. Existing postmasters will receive Guidance (imposing contractual terms) into their contracts to ensure that they comply with requirements of the Act and Post Office's obligations regarding the prevention and detection of tax evasion and preventing the facilitation of tax evasion (including an

POL00423693

	obligation to report any suspicion of criminal facilitation or criminal tax evasion). 2. Standard postmaster contracts used for new postmasters to be updated to reflect new obligations. 3. Payments Policy for all postmasters has been revised to ensure ongoing checks of bank accounts matching postmaster's bank details in the contract. 4. Review of postmaster on-boarding process is planned. 5. Any failure to comply with the new contractual terms and/or the Criminal Finances Act could result in immediate termination of the contract.
Contractors	1. Deed of Variation to the contract with Sopra Steria (Post Office's supplier of contractors) has been drafted to ensure that they (and their individual contractors) comply with the requirements of the Act and Post Office's obligations regarding the prevention and detection of tax evasion (including an obligation to report any suspicion of criminal facilitation or tax evasion to Post Office).
Suppliers	1. Standard supplier contracts will be amended to introduce the new obligations (as set out above) for new suppliers. 2. Existing suppliers will receive Guidance (imposing contractual terms) into their contracts (as set out above). 3. Ongoing overhaul/review of supplier on-boarding process by Procurement.
Employees	1. Communication to all employees is planned. Targeted communication to Finance, HR and Procurement is also planned. 2. Official Post Office's statement of zero tolerance to the criminal facilitation of criminal tax evasion inserted in the Financial Crime Policy.

POL00423693

Who is accountable?

All business areas are accountable for ensuring compliance with the Act in respect of their own activities:

- Retail is responsible for ensuring compliance with the Act in respect of the agent network.
- Finance & Ops is responsible for ensuring compliance with the Act in respect of suppliers.
- HR is responsible for ensuring compliance with the Act in respect of employee.

The Legal and Financial Crime Team together with the working group provide 2nd line of defence risk management.

What do we need to do next?

The working group continues to progress the implementation plan, working with different parts of the business to implement the recommended enhancements to ensure Post Office can avail itself of the reasonable procedures defence.

This work will include:

1. further examination of the due diligence conducted within the organisation (including the on-boarding of those that could be categorised as associated persons);
2. implementation of reasonable procedures;
3. roll out of communication across the organisation (including the agency network) and to targeted groups of Post Office's zero tolerance approach to criminal tax evasion and criminal facilitation; and
4. recommendations on how Post Office will conduct ongoing monitoring and review of existing procedures and their effectiveness (so that it can avail itself of the reasonable procedures defence).

A further report will be provided to the RCC at the next meeting in November.

POL00423693

7.1 Internal Audit Report

Author: Johann Appel Sponsor: Jane MacLeod Meeting date: 13 September 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 Risk and Compliance Committee (RCC) in July and progress on the 2017/18 Internal Audit Plan.

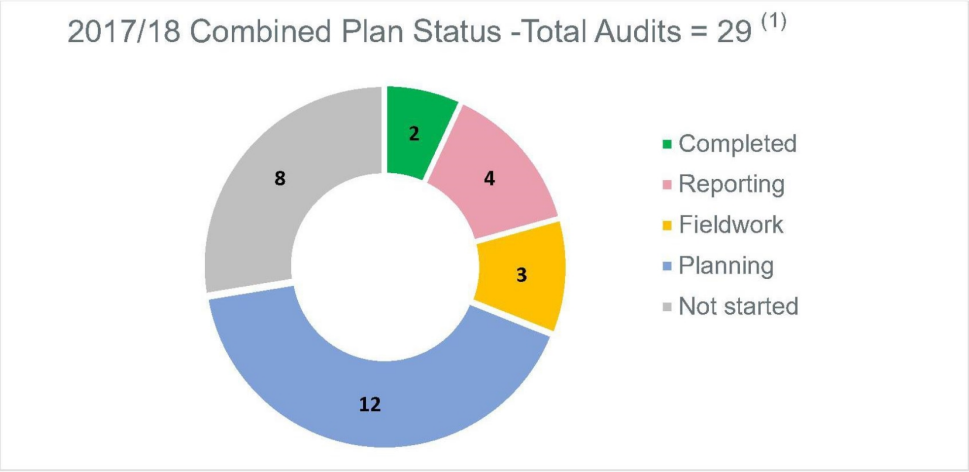
Questions this paper addresses

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

Conclusion

1. Progress against plan:

Delivery of the 2017/18 audit plan is well underway. We have finalised two reviews, with a further four currently in draft report stage and three audits in fieldwork. Particular emphasis is placed on timely audit planning and as a consequence 12 reviews are currently being scoped for delivery between September and January. Early engagement with the business in the planning phase is proving to result in a more effective audit process. Current progress against plan is as follows:



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

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

POL00423693

2. Open and Overdue Audit Actions (as at 31 August 2017):

Audit Action Status:	
Open (not yet due)	41
Overdue (<30 days)	4
Overdue (>30 days)	3
Total	48

More detailed information is provided in paragraph 9 - 10, including commentary on progress made with remediation of adverse audit reports.

3. Significant Issues:
There are no significant issues we believe the committee should be made aware of.

Input Sought

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

POL00423693

The Report

4. Changes to Plan since July RCC meeting

We have made one change to the audit schedule. We have agreed with management that it would be premature to review the Cyber Security controls given that the Security Transformation project is still ongoing and there are still actions outstanding from the 2016 Information Security review. The Cyber Security (Phase 1) review planned for August was therefore replaced with a follow-up of the 2016 Information Security review. An audit of Cyber Security will be considered in Q4.

The remainder of the 2017/18 plan will be refreshed during October to ensure that it is aligned with Post Office's changing risk profile and that the remaining audits on the plan are still relevant. Information obtained from the ongoing work on the risk 'placemat' will be a key consideration during the refresh of the audit plan.

5. Internal Audit Reviews Completed

Since the May ARC meeting we have completed an audit of the VAT Process as well as an advisory review of the IT Controls Framework. Our findings and observations are summarised below:

<table>
<tr><th>Audit</th><th>Key Messages</th></tr>
<tr><td>VAT Process & Controls
(Ref. 2017/18-02)

Needs Improvement

Audit actions:
<table>
<tr><td>P1</td><td>0</td></tr>
<tr><td>P2</td><td>3</td></tr>
<tr><td>P3</td><td>4</td></tr>
<tr><td>Total</td><td>7</td></tr>
</table>
</td><td>(Reported at July RCC, but still to be reported to ARC.)

This audit has found that generally POL manages its VAT affairs 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 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 taken place.
• 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.</td></tr>
</table>

POL00423693

IT Controls Framework (Advisory) (Ref. 2016/17-15) Advisory – Highlight Report	As agreed with the ARC and with management, Internal Audit participated in the ITCF project in an advisory role, contributing expertise of IT risk, IT controls and COBIT 5 knowledge to ensure the outcome of the programme is fit for purpose. Overall IA observed that for the 11 processes in scope, progress has been made in benchmarking the processes against COBIT and identifying controls and process steps which need to be in place to ensure operational risks stay within the risk appetite. However, there is some risk to the project and further work to be done before the ITCF will be ready to be implemented and rolled out for self-assessment: • Based on the current status of the programme we believe the original timeline will not be met. Phase 3 (remediation) is still ongoing, having slipped from its June deadline. Management need to revisit the overall project timeline. • Further improvements have been suggested to ensure control descriptions and remediation plans are clear and mitigate identified risks.

6. Reviews In Reporting

	Review	Status / Remarks
1	SAP SF Payroll Migration (Change)	Final Draft Report with GE Sponsor for sign-off.
2	Financial Spreadsheet Controls	Draft Report issued for management comment.
3	Mails Process	PwC branded report issued for internal use by management. PO IA Draft Report being reviewed by management.
4	Integrated Change Plan and Dependencies (Change advisory)	Report being drafted by Deloitte.

7. Reviews In Progress

	Review	Status / Remarks
1	IT Security Transformation (Advisory)	Ongoing – providing challenge and input to the project.
2	Lottery Pay-out Verification	Management request to review design effectiveness of new validation controls over the Lottery Pay-out process. Fieldwork nearing completion.
3	Compliance with Banking Framework agreement	Fieldwork nearing completion.

8. Reviews In Planning

We request management's continued cooperation in agreeing the scope and timing of the following reviews that are being planned for delivery in Q2 to Q4:

POL00423693

	Review	Timing (start of fieldwork)
1	Customer Complaints	November
2	Branch Cash Forecasting & Management	September
3	MoneyGram: AML Compliance	September
4	FRES	October
5	Information Security (2016) Follow-up	September
6	Business Continuity	January
7	Pension Scheme(s)	November
8	Branch Technology - EUC Transition	September
9	IT Networks	October
10	EUM	September
11	Chameleon (Thin Client Solution)	September
12	Point to Point Encryption Implementation ("Pin Pad")	January

9. Updates on Internal Audit Overdue Actions

Audit Action Status:	BAU	Change	Total
Open (not yet due)	27	14	**41**
Overdue (<30 days)	4	0	**4**
Overdue (>30 days)	3	0	**3**
Total	34	14	**48**

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	Priority & date	Revised Date & Comment
Branch Network Sales Training & Competence Review		
Introduce a competency matrix for the T&D Framework, and subsequently develop a new framework/scheme for colleagues not currently captured by the existing scheme and framework.	P2 31/08/17	31 October Completion delayed because of Project Finch. The Training and Competence team has planned to include this element in the scheme by the end of September/beginning of October.
Update section A14 (sales process) to display appropriate information under the correct headings and focus on achieving fair customer outcomes.	P2 31/08/17	30 November The update of the document is in progress. Area Managers are reviewing changes to the 'What good looks like' statements. Expected to finalise it in the next couple of months. (Jayshree, August 2017)
Update the T&D Framework to include a section on the training and oversight for Senior Support Managers.	P2 31/08/17	30 November The update of the framework is in progress. Completion delayed because of Project Finch.

POL00423693

Financial Services – Branch Network Sales Quality Assurance		
Review training materials and provide updated training for Specialists.	P2 31/07/17	30 September Action complete, pending evidence to close action.
Formalise the approach to levelling VMS gradings and minute all levelling meetings going forward.	P2 31/07/17	30 September Process is being documented and will be completed in the next month.
VAT Process		
Implement a tax strategy, tax risk and governance policy. Review existing tax risk management and controls framework to identify gaps in the documentation of controls and formalising the process documentation for VAT and other taxes.	P2 31/08/17	30 November This is still in progress and will be submitted for approval at the November ARC.
Reconfigure the tax code allocation in CFS.	P2 31/07/17	30 September The request has not been actioned due to certain individuals being on annual leave. We expect this to be updated and reviewed by end of September.

10. Progress with remediation of adverse audit reports

Following is a summary of progress with remediation of adverse audit reports issued in the last 12 months (reports rated 'Unacceptable' or 'Needs Significant Improvement'):

Audit title	Rating	Number of audit actions			
		Total	Closed	Open (Not due)	Open (Overdue)
Identify and Access Management (IAM) [1] (Apr17)	Needs Significant Improvement	14	4	10	0
Information Security [2] (Sept 2016)	Needs Significant Improvement	17	9	8	0
IT Disaster Recovery & Resilience (Dec 2016)	Needs Significant Improvement	8	8	0	0

[1] We are involved in assisting management to define remedial actions following our review of the IAM process. As more actions are agreed, these will be added to the database and tracked to completion.

[2] We have begun a full review of the progress with the remediation plan for Information Security. Our review will consider whether the actions previously agreed are still appropriate, will evaluate evidence of closed actions and ensure related risks were mitigated, and will agree revised completion dates for the remaining actions.

END OF REPORT

POL00423693

Appendix 1

2017/18 Internal Audit Plan - Status as at 6 September 2017					
No.	**Title/Subject**	**Sponsor**	**Original / Addition**	**Timing**	**Status / Rating**
Internal Control Reviews					
1	VAT Process	A. Cameron	**Addition**	May	**Needs Improvement**
2	Lottery Payout Verification (Design Effectiveness)	K. Gilliland	**Addition**	August	Fieldwork
3	Financial Spreadsheet Controls	A. Cameron	**Addition**	August	Draft Report
4	IT Control Framework (Advisory)	R. Hougton	Original	March - Aug	**Highlight Report**
5	IT Security Transformation (Advisory)	R. Hougton	Original	March - Dec	Fieldwork
6	Customer Complaints	A. Cameron	Original	November	Planning
7	Branch Cash Forecasting & Management	A. Cameron	Original	September	Planning
8	Compliance with Banking Framework agreement	N. Kennett	Original	August	Fieldwork
9	MoneyGram: AML Compliance	J. MacLeod	Original	September	Planning
10	FRES	N. Kennett	Original	October	Planning
11	Mails Process	K. Gilliland	Original	July	Draft Report
12	Financial Control Framework	A. Cameron	Original	Q4	Not started
13	Telecoms control framework	N. Kennett	Original	October	Not started
14	Business Continuity	J. MacLeod	Original	January	Planning
15a	Cyber Security (Ph 1 - Follow-up of 2016 audit)	R. Hougton	Original	September	Planning
15b	Cyber Security (Ph 2)	R. Hougton	Original	Q4	Not started
16	IT Governance and IT Risk management (Operations)	R. Hougton	Original	Q3/4	Not started
17	Data Protection (follow up)	J. MacLeod	Original	Q4	Not started
18	Client Settlements Process	A. Cameron	Original	Q4	Not started
19	Pension Scheme(s)	A. Cameron	Original	November	Planning
Change Assurance					
20	Branch Technology - EUC Transition	K. Gilliland	Original	September	Planning
21	IT Networks	R. Houghton	Original	October	Planning
22	Back Office Transformation	A. Cameron	Original	Oct/Nov	Not started
23	SAP Success Factors - Payroll	A. Cameron	Original	June	Final Draft with GE
24	EUM	N. Kennett	Original	September	Planning
25	Agile Methodology and Governance	J. MacLeod	Original	Q4	Not started
26	Chameleon (Thin Client Solution)	K. Gilliland	Original	September	Planning
27	Integrated Change Plan and Dependencies (Advisory)	A. vd Bogerd	Original	July	Draft Report
28	Gating Process - Effectiveness	A. vd Bogerd	Original	Q4	Not started
29	Point to Point Encryption Implementation ("Pin Pad")	J. MacLeod	Original	January	Planning
30	Network Development PIR	K. Gilliland	Original	Q4	Not started
31	Placeholder (contingency)		Original		Not started
32	Placeholder (contingency)		Original		Not started
Note: Target audit delivery per original approved plan is for 29 audits (16 internal control reviews and 13 change assurance reviews).					

POL00423693

7.2 Camelot Audit Lessons Learned

Author: Keith Maple Sponsor: Kevin Gilliland Meeting date: 13 September 17

Overview

This describes the background to an issue identified with the reporting of the Lottery prize audit, summarises lessons learnt and the actions taken to prevent reoccurrence.

Questions

1. What is the background?
2. What was the issue?
3. What lessons have we learnt?
4. What actions have been taken to prevent a repeat?

Conclusions

1. Background

As part of the Post Office/ Camelot National Lottery Retailer Agreement prize monies are paid out by branches for winning tickets. POL hold a unique position in that outside of Camelot they are the only entity that can pay out lottery winning prizes of up to £50,000.

The Gambling Commission have increased pressure on Camelot over the past 12 months to improve compliance with the rules governing the payment of lottery prizes. Camelot have in turn trialled a series of KPIs/Service measures focused on the accuracy of the payment process, monitored via an audit process and with a view to eventually making them contractual obligations. These audits were trialled over a 6 month period from the final quarter of 2016.

Camelot randomly select 100 winning tickets a quarter for POL to check, ostensibly by desk audit, that each element of the required payment process has been completed. The audit covers various elements of the payment process including obtaining the name and address of the winner, reconciliation of the payment to Horizon and whether the ticket had been voided in line with Camelot requirements. Audit results are then given to Camelot.

2. What was the issue?

After a change in the management of the Retail team and a review of the audit operation, it was discovered that POL had been mis-declaring the 'true' results of the audits to Camelot. This was immediately brought to the attention of the RCC.

POL00423693

It must be emphasised that there was no contractual obligation to undertake these audits or to report their results to Camelot.

The audit of the winning tickets reviews whether the prize values are recorded accurately, that the claimant's name and address are recorded in full and match the Horizon receipt and that a signature has been obtained. There should also be evidence of confirmation that the receiver was over 16, and that each winning ticket was effectively voided, as paid, in the designated area.

The audit of February 2017 indicated that only 23% of the winning tickets met all of the audit's requirements. If the results of the audit excluded tickets that had only failed by not being voided correctly, the success rate increased to 81%.

Members of the previous Retail team (who are no longer with the business) chose to declare audit results that excluded tickets where the only criteria they failed on was a failure to void. Camelot were never made aware of this omission and as such the success rate of the audit was falsified.

3. What lessons have been learnt?

The audit of the winning tickets was carried out in the manner agreed by POL and Camelot. The audit results were manipulated to inflate the level of success and an express direction given to send them to Camelot. This occurred because of a possible integrity issue rather than a failure of the controls that are in place. There was no need for sign off at a higher level within POL before they were sent to Camelot. A programme in branch to re-emphasise the process of winning ticket payments has been introduced with visual aids, communications and a pending change to the Horizon screen to promote the requirement to void winning tickets.

4. What action has been taken to prevent a repeat?

Two courses of action were immediately initiated. The current Retail team identified the root cause/control failures and at same time the Internal Audit team were engaged.

It was considered by the latter that the Retail team appeared to have established the facts of the matter and identified the root cause / control failures. It was their belief that Internal Audit would not add any more value by reviewing the facts pertinent to this issue but will assess the design effectiveness of the remedial controls implemented. The internal audit is currently in progress and results will be reported at the November RCC and ARC meetings. Other actions:

1. The results of future quarterly audits will be signed off by the relevant Product Manager and the Head of Retail propositions. An additional 'independent' sign off will be undertaken by Finance or Internal Audit
2. Camelot also reserve the right to undertake their own audits of the POL audit process/results and these will be reviewed on a quarterly basis.

POL00423693

8.1 Anti-Money Laundering and Counter Terrorist Financing Policy

Author: Sally Smith | Sponsor: Jane MacLeod | Meeting Date: 13th Sept 2017

Executive Summary

Context

This paper sets out the updates and revisions to the Anti-Money Laundering and Counter Terrorist Financing 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 Anti-Money Laundering and Counter Terrorist Financing 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 Anti-Money Laundering and Counter Terrorist Financing Policy.

POL00423693

The Report

Why do we need to review this policy?

1. 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?

2. 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, and has been updated to reflect the new money laundering regulations.
3. Key changes include:
    - We have 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.
    - In line with regulatory requirements we have placed the completion and maintenance of financial crime risk assessments at the heart of the policy.
    - A new section has been included setting out the key offences under the regulations and their potential consequences to both the group and members of staff.
    - The General Counsel is now responsible for oversight of the MLRO and the group's compliance with regulatory obligations.
    - We have highlighted the regulatory requirements in relation to data retention.
4. Risk Assessment methodology and Product Information Packs that have been developed over the last 12 months are now referenced for the first time.
5. A new section has been included clearly mapping minimum control standards, responsibilities and timescales.

How did we develop these recommendations?

6. 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 and the Criminal Finances Act 2017.
7. Policy queries and issues that have arisen over the previous 12 months have been reviewed to ensure that these concerns are addressed, including risk assessment work undertaken since July 2016 and the HMRC supervisory audit undertaken since February 2016.

POL00423693

What are the implications of these changes?

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

8. 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.
9. Over the past few months the following communications have been issued to the network provide further support and guidance on the following issues: Gift Card Fraud (June), Completion of SARs (June), AML/CTF Training (July), recording ID numbers correctly for bureau transactions (August). We are scheduled to issue further guidance on the completion and submission of SARs in September. If any instances of non-conformance are identified additional training or communications will be issued on a risk sensitive basis.
10. Via EUM, the Financial Crime Team will be able to ensure that only those agents and staff who have completed their initial or annual renewal training will be allowed access to Horizon systems. Any customer facing or back office staff or agents who fail to complete their training within the first 30 days of joining or at annual renewal will be reported to relevant management for their review and escalation as required. The Financial Crime Team will undertake periodic compliance testing and report on conformance to the R&CC.
11. As part of the wider Product Manager training (being provided by Cranfield School of Management), a series of workshops for product managers in Financial Services & 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 Tool.
12. 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, but will be offered if required.
13. 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.
14. As part of our annual training obligations, AML/CTF training will be updated to reflect the new policy and regulatory requirements.

What will the impact be on our wider business?

15. While 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, the identification through documented risk assessment of potential or inherent and residual Financial Crime risks is not yet mature across the business and more needs to be done culturally to embed the methodology. The introduction of the Product Manager workshops will enhance compliance with this area.

POL00423693

16. As part of the roll out of the 'placemat' control self-assessment methodology, all business units will be required to ensure that they consider financial crime risks in their area when developing their own Risk and Controls Matrix. It is expected that the roll out of the 'placemat' methodology will be complete by end 2017/18.

What would the impact be of delaying approval?

17. 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.
18. 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.
19. 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.

POL00423693

GROUP POLICIES

Anti-Money Laundering and Counter Terrorist Financing Policy

Version – V3.1

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 that wherever possible use of Post Office systems and products for money laundering or terrorist financing is prevented, and the highest standards of financial crime prevention, detection and management are maintained.

POL00423693



1. Overview 3
1.1. Introduction by the Policy Owner 3
1.2. Purpose 3
1.3. Core Principles 3
1.4. Application 4
1.5. The Risk of Money Laundering and Terrorist Financing 4
1.6. Legislation 4
1.7. Offences 5
2. Risk Appetite and Minimum Control Standards 6
2.1. Risk Appetite 6
2.2. Risk Assessment 6
2.3. Policy Framework 7
2.4. Who must comply? 7
2.5. Minimum Control Standards 7
2.6. Product and Service Risk Tools 16
3. Where to go for help 17
3.1. Additional Policies 17
3.2. How to raise a concern 17
3.3. Who to contact for more information 17
4. Governance 18
4.1. Governance Responsibilities 18
5. Control 19
5.1. Policy Version 19
5.2. Policy Approval 19
Company Details 19

POL00423693

1. Overview

1.1. Introduction by the Policy Owner

The General Counsel has overall accountability to the Board of Directors for the design and monitoring of controls to prevent or deter Financial Crime which includes Anti Money Laundering (AML) and Counter Terrorist Financing (CTF). 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 Money Laundering and Terrorist Financing 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

Money Laundering and Terrorist Financing are criminal offences and everyone working in the business has a personal obligation to prevent them taking place. The governance arrangements described in this Policy are based upon the following core principles:

- 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;
- The Group ensures that its policies reflect the principles of the AML and CTF regulations and legislation;
- The Group's overall and ongoing risk management process includes a risk based assessment of the financial crime risks to which the Group and its business are exposed, and the quality of its AML and CTF controls and monitoring;
- The Group undertakes a training and awareness program to ensure employees are aware of the risks of money laundering and terrorist financing, what they should do if they are suspicious, and the consequences should they fail to comply with the law;
- The Group promotes ethical and professional standards to prevent it from being used, intentionally or unintentionally by criminals;
- Decisions taken by management are consistent with the Board's approved strategic objectives and Risk Appetite;
- Every member of staff is responsible for understanding and managing the risks they take on behalf of the Group;

---

[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.

POL00423693

- Clear accountabilities are delegated by management to staff 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.

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 Post Office being used to facilitate Money Laundering or Terrorist Financing activities, and therefore takes a risk based approach.

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 Money Laundering and Terrorist Financing is reviewed by the Board as part of its wider commitment to Financial Crime on a regular basis.

1.5. The Risk of Money Laundering and Terrorist Financing

Money Laundering
Money laundering is the process criminals use to hide, disguise and dispose of cash and assets obtained from criminal activity. Criminals want to disguise the source of their money and remove any link to the original crime. This allows them to avoid prosecution and confiscation of funds.

Terrorist Financing
Terrorist financing involves dealing with money or property that may be used to fund terrorism. The funds and property may be from legitimate sources (e.g. personal funds, charities, sponsored trips, etc.) or criminal sources.

Failure to manage the these risks can result in financial loss, customer impact, terrorism, regulatory breaches, fines, prosecution, prevention from selling a particular product, loss of existing or future contracts/relationships and damage to reputation.

1.6. Legislation

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

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (known as Money Laundering Regulations 2017)
- The Proceeds of Crime Act 2002
- The Criminal Finances Act 2017
- Policing and Crime Act 2017
- The Terrorism Act 2000
- Counter-Terrorism Act 2008

POL00423693

The Group monitors and takes into consideration guidance and other assistance offered by regulatory, industry and other specialist bodies, for example the Joint Money Laundering Steering Group (JMLSG), UK Finance (which incorporates BBA, UK Payments and Financial Fraud Action UL), Link, etc. publish trends and analysis on current threats and issues.

Oversight of compliance with the Money Laundering Regulations by the Group is undertaken by HMRC in the case of Post Office Limited and the Financial Conduct Authority (FCA) is the case of Post Office Management Services Limited (POMS).

Post Office Limited is an Appointed Representative of the Bank of Ireland and 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 risks.

1.7. Offences

The Money Laundering regulations set out five offences for which the Group or a member of its staff can be prosecuted under:

1. **Concealing** - where an employee conceals, disguises, converts or transfers criminal proceeds, or removes them from the UK
2. **Arrangement -** where an employee allows the Group to enter into or become involved in an arrangement where an employee knows or suspects that it involves the proceeds of crime.
3. **Acquisition, use or possession** - where an employee acquires, uses or takes possession of criminal proceeds.

   If found guilty of these offences an individual can be given an unlimited fine or up to 14 years in prison or both. The only defence is that an employee had completed and submitted a Suspicious Activity Report to the Money Laundering Reporting Officer (MLRO), apart from 'acquisition' where the Group or a relevant individual would need to evidence that the proceeds had been acquired at fair market price and that they were not aware that they were criminal proceeds.
4. **Failure to disclose -** where an employee fails to report to the MLRO their suspicions or knowledge that someone is involved in Financial Crime.

   If found guilty of this offence an individual can be given an unlimited fine or up to five years in prison or both. There are two defences to this offence; training did not cover how to complete a SAR or "a reasonable excuse" such as that an employee was rushed to hospital just prior to completing the report. The reasonableness of the excuse will be tested in court.
5. **Tipping Off –** an offence will be committed if information which prejudices an investigation into Financial Crime is shared by an employee - for examples if an employee informs a suspect that they are under investigation.

   If found guilty of this offence an individual can be given an unlimited fine or up to two years in prison or both. The only defence is if an employee did not know or suspect that what was said would prejudice the investigation

POL00423693

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 is 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 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. Risk Assessment

The Money Laundering regulations require that Post Office completes Group wide risk assessments with a clear rationale to prevent and detect money laundering and terrorist financing.

Risk assessment must include:

- Identifying the inherent money laundering risks that are relevant to the Group, product and/or service
- Assessing customer type, customer behaviour, normal product/service activity, delivery channels, etc.
- Assessing controls to manage and reduce the impact of inherent risks
- Assessing how the Group will monitor controls and improve their efficiency
- Keeping records of key decisions

The Group requires risk assessments to be completed for individual products and services to ensure that sufficient controls are in place to detect and prevent money laundering or terrorist financing, and for these risk assessments to be refreshed annually.

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

POL00423693

2.3. 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.

The Anti-Money Laundering and Counter Terrorist Financing 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.

2.4. 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 or to have their own equivalent Policy.

Where non-compliance is identified the matter must be referred to the MLRO (currently the Head of Financial Crime). Any investigations will be carried out in accordance with the Investigations Policy. Where an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary offence.

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 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

POL00423693

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Oversight	Group does not comply with its AML/CTF regulatory responsibilities.	Directive Control: The General Counsel is appointed as the officer responsible for overseeing compliance with regulations.	General Counsel	Ongoing
		Preventative Control: The Group appoints an appropriate individual within the Risk & Compliance area as MLRO. With the assistance of the Financial Crime Team, the MLRO's main responsibilities include: • To receive reports of suspected money laundering or terrorist financing and to disclose to the NCA where required • Keep the Group up to date in relation to Financial Crime legislation • Putting in place and then monitoring compliance with the AML/CTF regime • Reporting to the ARC and R&CC all instances of non-compliance and any regulatory concerns or issues • Reporting to the regulators instances of non-compliance, where required	MLRO	Ongoing
		• Annual MLRO reports for the Board (for Post Office Management Services Limited and for Post Office Limited) covering: the governance framework; operation and effectiveness of the control framework (including documentation of policies and risk assessments); external threats/ landscape; summary of business issues and recommendations.	MLRO	Annual
		Corrective Control: Risk assessments must be undertaken where an issue is highlighted, an incident occurs or the regulations change.	MLRO	Issue, incident or change

POL00423693

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 money laundering or terrorist financing has not been considered in the design, which may result in facilitation of laundering or terrorist financing leading to reputational damage and/or regulatory sanctions.	Preventative Control: As part of the design of a new product or service: • A Product Information Pack (see 2.6 below) must be completed. • Product or service risks must be considered and documented using the Risk Assessment Tool (see 2.6 below). Prior to launch the Product Information Pack and the Product and Service Risk Assessment must be reviewed and approved by the Financial Crime Team.	Product Manager Financial Crime Team	During design phase Prior to Launch
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 money laundering or terrorist financing 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. 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. 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 Product Manager Product Manager	Annually, or at any time there is a change Any time there is a change Any time there is a change

POL00423693

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Existing products and services (continued)		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
Financial settlement and reconciliation	Inadequate controls and audit trails relating to financial settlement and reconciliation may result in facilitation of laundering or terrorist financing leading to 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 money laundering or terrorist financing. Detective Control: Audit trails must be maintained so that system access can be monitored. To ensure that the Group's controls remain effective, the Group undertakes internal audits to test and assess their effectiveness.	Chief Financial Officer Chief Information Officer Internal Audit	Ongoing Ongoing Ongoing
Monitoring	The Group fails to undertake adequate transaction monitoring and fails to prevent and detect money laundering and terrorist financing.	Preventative Control: Where the Group is directly regulated for products or services, sufficient transaction monitoring must be undertaken to ensure that suspicious activity, non-conformance and breaches can be identified, and provide assurance that customer data capture and due diligence thresholds have been set at a level commensurate with the risk exposure and to ensure compliance with money laundering regulations.	Product Manager/MLRO	Ongoing

POL00423693

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Due Diligence	Group fails to undertake appropriate due diligence of a customer and fails to identify criminal activity.	Preventative Control: The Group takes a risk based approach and considers: • The product or service • Its intended customer market base and normal transaction activity • Any other risks relating to the product Detective Control: The extent to which the Group will gather due diligence information varies depending upon the risk that the product or service poses however must be considered when: • a business relationship is established with a customer • money laundering or terrorist financing is suspected • there are doubts about a customer's identification information obtained previously	Financial Crime Team/Product Manager Financial Crime Team/Product Manager	Annually, or at any time there is a change As required
Politically Exposed Persons (PEP)[4]	Post Office fails to appropriately manage the risks associated with doing business with PEPs.	Preventative Control: All products and services are required to have in place identification procedures, commensurate with the underlying risk to ensure that it can identify where the product and service is being used by a PEP. Determine the level of identification and assess if PEP checks are required.	Product Manager Product Manager	Ongoing Ongoing

[4] PEPs are those who have or are seen to have access to public influence and/or public money and as such are seen as being at higher risk of corruption. A PEP is someone who is: An individual who has or has been in a prominent public role in the UK or abroad such as Heads of State, MPs, Heads of Armed Forces, etc. An immediate family member or a known close associate of such as person.

POL00423693

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Politically Exposed Persons (PEP) (continued)		Detective Control: Ensure sufficient information is captured to undertake PEPs screening where deemed appropriate. Enhanced Due Diligence is required on any PEP relationship. Corrective Control: Where PEPs screening identifies PEPs, ensure that sufficient due diligence is undertaken to manage the risks.	Product Manager Product Manager Product Manager	Ongoing Ongoing Ongoing
Sanctions[5]	The Group transacts with a customer who is sanctioned, resulting in the Group breaching international sanctions, reputational damage and/or regulatory sanctions.	Preventative Control: All products and services are required to have in place sufficient identification procedures, commensurate with the underlying risk to ensure that the product and service is not used by a customer who is sanctioned. Detective Control: Ensure sufficient information is captured to undertake Sanctions screening where deemed appropriate prior to a transaction occurring.	Product Manager Product Manager	Ongoing Ongoing

[5] Sanctions are restrictions put in place by a government or a multilateral organisation (such as the United Nations) that limit a person, company or countries access to financial services or financial markets, funds or economic resources in order to achieve a specific foreign policy or national security objective.

POL00423693

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Sanctions (continued)		Corrective Control: Where screening identifies Sanctions, ensure that transactions are declined and the transaction is reported via SAR. In the event that an employee become aware or suspects that a Sanctioned party is conducting business within the Group this must be reported immediately to the MLRO.	Product Manager/MLRO All employees	Ongoing Ongoing
Premises Registration	The Group fails to maintain up to date premises registration leading to penalties and sanctions. (The Group must maintain an up to date register of premises addresses that undertake directly regulated activity with HMRC – any changes must be registered and the relevant fees paid within 30 days)	Directive Control: Business rules must be agreed with HMRC in respect of the premises types that must be registered (e.g. Mobile Vans). Preventative Control: Premises registration business rules are reviewed annually and any potential changes to premises type are discussed and agreed with HMRC. Branch premises data is reviewed fortnightly and changes submitted to HMRC.	MLRO Financial Crime Team Network Design & Analysis Team and Financial Crime Team	Ongoing Ongoing Fortnightly
Training	Through inadequate training, staff allow money laundering or terrorist financing to take place, resulting in reputation damage and regulatory fines.	Preventative Control: Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training tailored to business risk areas. Outsource providers, clients & suppliers must maintain records to evidence that staff have received adequate and regular training.	Financial Crime Team/HR Product Manager/MLRO	Annual Ongoing

POL00423693

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Training (continued)		New branch staff are required to complete AML/CTF training before they transact on Horizon, and back office staff and contractors within 30 days of joining. Detective Controls: Pass rate and number of test attempts is monitored to identify risk areas and any additional training or guidance required.	HR Financial Crime Team	Ongoing Ongoing
Fit and Proper	Due to inadequate screening, there is a risk that key individuals are unfit to undertake a role.	Preventative Control: All Board members, GE and the MLRO must pass the HMRC Fit & Proper test to ensure that the Group has employed individuals who are suitable to perform their roles. A register of completed and up to date Fit & Proper tests is maintained. Post Office completes pre-employment screening to ensure that an individual is fit and proper for their role. For further information please see the employee vetting policy. Detective Control: The Group completes ongoing screening to ensure that an individual continues to remain fit and proper for their role.	Financial Crime Team Director of Human Resources Director of Human Resources	Within 30 days of appointment Pre-employment Ongoing where required

POL00423693

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Record Keeping	Customer and transactional data is not retained resulting in the Group being unable to identify suspicious or out of character transactions, leading to the Group being used to launder money.	Preventative Control: For products and services where the Group is directly regulated, records must be kept of all transaction data and data obtained for the purpose of identification for a minimum of 5 years from the date of creation/transaction. The MLRO also ensures that documents relating to money laundering topics (e.g. files on suspicious activity reports and investigations) are maintained for a minimum of 5 years.	Product Managers MLRO	Ongoing Ongoing
Suspicious Activity Reports ("SAR") and Reporting	Failure to report suspicions to the National Crime Agency[6] results in the Group being used to fund terrorism.	Preventative Control: The Group provides training to all employees and postmasters and provides easily accessible methods to report a suspicion to the MLRO and the Financial Crime Team. Where there are suspicions or concerns, the MLRO can apply to the NCA for permission to continue a transaction – seeking a defence.[7] Corrective Control: Where issues are identified additional training and guidance is provided to increase employee understanding of the SAR regime.	All employees and postmasters MLRO Financial Crime Team	Ongoing As required Ongoing

[6] The NCA receives all SARs reported in the UK and their role is to investigate in conjunction with other intelligence. Where appropriate the NCA may provide copies of SARs to other intelligence bodies and investigation services (Law Enforcement, HMRC, etc.).

[7] Where defence is requested, this can take up to seven working days for the NCA to review and during this time customers must not be advised that defence is being applied for as this would constitute 'tipping off'.

POL00423693

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Suspicious Activity Reports ("SAR") and Reporting (continued)		Appropriate mechanisms are in place to protect Post Office and de-risk where concerns are identified relating to a specific individual or Group undertaking transactions in the Post Office network. Detective Control: Where a SAR is not disclosed to NCA, it is reviewed and assessed by a senior manager, and the subject matter of the report is monitored for a minimum of three months to ensure that the appropriate decision was taken. Audit trails are maintained so that reports made can be monitored.	Financial Crime Team Financial Crime Team	Ongoing Ongoing

2.6. 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.

POL00423693

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 that Post Offices products, services or processes have been used to facilitate money laundering, terrorist financing, or dishonest or fraudulent activity has a duty to:

- Discuss the matter fully with their Line Manager; or,
- Report their suspicions by telephoning Grapevine on GRO or,
- Report the matter directly to the Money Laundering Reporting Officer (MLRO)
- Staff can contact the Post Office's General Counsel, who can be contacted by email at: whistleblowing GRO or by telephone on: GRO
- Alternatively staff can use the Speak Up service available on GRO
- or via a secure on-line web portal: http://www.intouchfeedback.com/postoffice

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

POL00423693

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.

POL00423693

5. Control

5.1. Policy Version

Date	Version	Updated by	Change Details
November 2016	3	Georgina Blair	Final Version approved by ARC
August 2017	3.1	Thomas Richmond	Version updated to reflect legislation changes

5.2. Policy Approval

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

Committee	Date Approved
POL R&CC	
POMS R&CC	
POL ARC	
POMS ARC	

Policy Sponsor: General Counsel/Group Director of Legal, Risk & Governance

Policy Owner: Head of Financial Crime

Policy Author: Head of Financial Crime

Next review: August 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.

POL00423693

8.2 Whistleblowing Policy

Author: Sally Smith Sponsor: Jane MacLeod Meeting Date: 13th September 2017

Executive Summary

Context

This paper sets out the updates and revisions to the Whistleblowing 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 Whistleblowing Policy has been amended to clarify the 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

Input Sought

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

POL00423693

The Report

Why do we need to review this Policy?

1. 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?

2. We have redesigned the Policy template and format but the substance and obligations have not changed. 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.
3. Key changes include:
   - Updating contact details and help line numbers
   - Ensuring that all teams across the business that may receive whistleblowing reports ensure that these are passed onto the Whistleblowing Officer and handled confidentially
   - A new section has been included clearly mapping minimum control standards, responsibilities and timescales.

How did we develop these recommendations?

4. 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?

5. No material changes are required to comply with this updated Policy.
6. 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.

What will the impact be on our wider business?

7. Transparency of Post Office's adherence and commitment to the Employment Rights Act 1996 and the Public Interest Disclosure Act 1998

What would the impact be of delaying approval?

8. Risk that the group breaches the Employment Rights Act 1996 and the Public Interest Disclosure Act 1998 by not having up to date policies and procedures to provide protections to whistleblowers.
9. 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.
10. 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.

POL00423693

GROUP POLICIES

Whistleblowing Policy

Version – V1.5

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 that colleagues know how to report concerns regarding wrongdoing or dangerous practices and that they can do so without fear of recrimination.

POL00423693



1. Overview 3
1.1. Introduction by the Policy Owner 3
1.2. Purpose 3
1.3. Core Principles 3
1.4. Application 3
1.5. Legislation 4
1.6. What is Whistleblowing 4
1.7. Protecting the whistleblower 4
1.8. Whistleblowing Officer and 'Speak Up' 5
1.9. External Disclosures 5
2. Risk Appetite and Minimum Control Standards 7
2.1. Risk Appetite 7
2.2. Policy Framework 7
2.3. Who Must Comply? 7
2.4. Minimum Control Standards 8
3. Definitions 12
3.1. Definitions 12
4. Where to go for help 13
4.1. Additional Policies 13
4.2. How to raise a concern 13
4.3. Who to contact for more information 13
5. Governance 14
5.1. Governance Responsibilities 14
6. Control 15
6.1. Policy Version 15
6.2. Policy Approval 15
Company Details 15

POL00423693

1. Overview

1.1. Introduction by the Policy Owner

The General Counsel has overall accountability to the Board of Directors for the implementation of controls ensuring Post Office meets it Whistleblowing obligations. Whistleblowing is an agenda item for the Audit and Risk Committee and the Post Office board is updated as required.

1.2. Purpose

This Policy has been established to set the minimum operating standards relating to the management of Whistleblowing 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

Whistleblowing is the reporting of suspected wrongdoing and/or dangerous practices within Post Office. This would include serious accidents, fraud, regulatory breaches, financial impropriety and/or reputational damage.

In order to encourage Whistleblowing and provide appropriate protections to whistleblowers, the governance arrangements described in this Policy are based upon the following core principles:

- To encourage the reporting of any concerns as soon as possible in the knowledge that all concerns will be taken seriously and investigated, and that confidentiality will be respected;
- To provide guidance as to how to raise those concerns;
- To provide whistleblowers reassurance that all concerns are raised without fear of reprisals, even if they turn out to be mistaken;
- Post Office is committed to and oversees the implementation of a Policy in line with the Group's risk appetite. The Policy and associated procedures (set out or referred to in this document) are proportionate to the risks and complexity of the Group;
- Post Office undertakes a training and awareness program to ensure employees are aware of the Whistleblowing policy and procedure.

1.4. Application

This Policy is applicable to all employees within the Group and outlines the protections provided for whistleblowers by law. In order to encourage reporting of wrongdoing, Post Office will, where appropriate, extend equivalent protection to Postmasters, Agent Assistants, and members of the public.

[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.

POL00423693

1.5. Legislation

The Group seeks to comply with all relevant UK legal and regulatory requirements including (but not limited to) the following legislation as amended or supplemented from time to time:

- Employment Rights Act 1996
- Public Interest Disclosure Act 1998

1.6. What is Whistleblowing

"Whistleblowing" refers to the act of exposing potential or actual wrongdoing and/or dangerous practices by reporting it either internally within an organisation, or to an external party. A whistleblower is a person who raises a genuine concern in relation to any wrongdoing, this includes criminal activity, miscarriages of justice, dangers to health and safety and the deliberate attempt to conceal it.

Individuals[3] should raise a concern if they are aware of, or suspect, wrongdoing which affects others (e.g. customers, members of the public, colleagues or the Post Office). The following lists some examples (this is a non-exhaustive list) of situations where an individual may raise a concern:

- Financial Crime including Fraud, Money Laundering and financing of terrorism,
- Giving, offering or taking of bribes,
- Financial mismanagement,
- Misreporting,
- Practices that could put individuals or the environment at risk,
- Breach of Post Office internal policies and procedures (including the Code of Business Standards),
- Concerns about slavery or human trafficking, and
- Any conduct likely to damage Post Office's reputation

Grievances and matters such as bullying and harassment are addressed under Post Office's HR policies and concerns in relation to such matters should be raised in accordance with the procedures set out in the appropriate HR policy.

If an individual is uncertain about whether something is within the scope of this Policy they should seek advice from the Whistleblowing Officer, whose contact details are set out in this Policy.

1.7. Protecting the whistleblower

Post Office has a statutory obligation to protect whistleblowers and will support any individual who raises genuine concerns under this Policy, even if they turn out to be mistaken. Post Office are committed to respecting the confidentiality of all whistleblowers, and including those who wish to remain anonymous.

Post Office will make every effort to protect the whistleblower's identity, however, it may be necessary in the course of an investigation to share this information with a relevant stakeholder (e.g. an investigator). There is no requirement for a whistleblower to provide personal contact information. However, not providing this information may reduce Post Office's ability to undertake a thorough investigation into the concerns raised.

[3] In this Policy "individuals" means Postmasters, Agent Assistants, members of the public and employees (permanent staff, temporary including agency staff, contractors, consultants and anyone else working for or on behalf of Post Office). The statutory protections offered under the Public Interest Disclosure Act 1998 only apply to employees, however Post Office Limited will consider extending these protections to other individuals where they have acted in good faith in raising concerns.

POL00423693

Post Office will take all reasonable steps to ensure that whistleblowers do not suffer any detrimental treatment as a result of raising a concern. Detrimental treatment includes disciplinary action, dismissal, threats or other unfavourable treatment connected with raising a concern. Serious action will be taken against any individual who threatens or retaliates against whistleblowers in any way.

If an individual believes that they have suffered any such treatment, they should inform the Whistleblowing Officer immediately. The Whistleblowing Officer should take steps to address any victimisation, which may include working with the HR team to put appropriate measures in place. If the matter is not addressed the whistleblower should raise it formally using Post Office's Grievance procedure.

In all cases the individual's concerns will be treated sensitively and in confidence.

1.8. Whistleblowing Officer and 'Speak Up'

Post Office has a appointed the General Counsel as the Whistleblowing Officer who can be contacted on whistleblowing GRO

The Whistleblowing Officer will review concerns raised and determine the best course of action, if any. They may ask for further information in order to make this decision.

It is recognised that sometimes raising a concern directly with the business may not be possible. In such instances individuals should contact the "Speak Up" line, a confidential reporting service which is run by an independent company InTouch MCS Ltd.

Contact details for the Speak Up line are:

- GRO
- http://www.intouchfeedback.com/postoffice which is a secure on-line web portal:

All reports to the Speak Up line will be acknowledged within five working days and will be passed to the Whistleblowing Officer.

It is also possible that individuals may whistleblow via a complaint to a front line team, e.g. Customer complaints, NBSC and Grapevine. These may be verbal or written communications.

In all instances any whistleblowing reports, regardless of reporting method, will be passed onto the Whistleblowing Officer. The whistleblower may be kept informed of any action taken, however, this information may be limited if it is required to keep the confidence of other people.

1.9. External Disclosures

The aim of this Policy is to provide an internal mechanism for reporting, investigating and remedying any wrongdoing in the workplace. In most cases individuals should not find it necessary to alert anyone externally.

However, the law recognises that in some circumstances it may be appropriate for individuals to report their concerns to an external body such as a regulator. The independent Whistleblowing charity, Public Concern at Work have a list of prescribed regulators for reporting certain types of concerns. Their contact details are as follows:

Helpline: GRO

POL00423693

E-mail: GRO
Website: www.pcaw.co.uk

Public Concern at Work operates free, confidential advice to people concerned about crime, danger or wrongdoing in the workplace. Post Office strongly encourages advice is sought out from Public Concern at Work before reporting any concern to an external party.

Post Office Money Services (POMS) is directly regulated by the Financial Conduct Authority (FCA). Individuals may decide to whistleblow directly to the FCA, and can do so by using one of the following channels.

Helpline: GRO
E-mail: GRO
Website: www.fca.org.uk/site-info/contact/whistleblowing
Address: Intelligence Department (Ref IDA), Financial Conduct Authority, 25 the North Colonnade, London E14 5HS

POL00423693

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 an action may still sit outside the agreed Risk Appetite.

2.2. Policy Framework

Post Office has established a suite of policies and procedures, on a risk sensitive approach which are subject to an annual review. The policy suite is designed to comply with applicable legislation and regulation. The Whistleblowing Policy should be considered and read in conjunction with other policies where relevant. These may include the Financial Crime Policy, the Anti-Bribery & Corruption Policy, Health & Safety Policies and HR Policies where relevant.

2.3. Who Must Comply?

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.

Any investigations will be carried out in accordance with the Investigations Policy which is available on the Post Office Intranet

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

POL00423693

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
Receipt and investigation of whistleblowing reports	Failure to meet legal and regulatory requirements	Directive Control: Post Office must nominate a Whistleblowing Officer to receive reports, ensure that all reports are fully investigated and that any appropriate corrective action is undertaken.	Post Office CEO and Board	Ongoing
		The whistleblowing officer must provide a whistleblowing report to the R&CC and ARC at least annually.	Whistleblowing Officer	Annually
		Any serious whistleblowing concerns must be promptly escalated to the Chairman of the Post Office Audit and Risk Committee.	Whistleblowing Officer	Ongoing
		Preventative Control: All employees are trained and the policy is available to them	Whistleblowing Officer	Training must be provided at least annually

POL00423693

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		The Whistleblowing Officer must ensure that appropriate arrangements are in place to ensure that whistleblowing reports are addressed promptly including during absences	Whistleblowing Officer	Ongoing
Breach of confidentiality	Failure to ensure confidentiality for the whistleblower	Preventative Control: Whistleblowing Policy Confidential Speak Up line reports are shared only with the Whistleblowing Officer Whistleblowing email inbox with restricted access Whistleblowing Officer must put arrangement in place to protect the confidentiality of the whistleblower during investigations Corrective Control: All incidents of breaches are escalated to the Whistleblowing Officer to review and take necessary actions.	Whistleblowing Officer Whistleblowing Officer Whistleblowing Officer Whistleblowing Officer Whistleblowing Officer	Ongoing Ongoing Ongoing Ongoing Ongoing
Incorrect handling of whistleblowing report	An individual may raise a whistleblowing report with other individuals in the Group. Details may then be shared with various stakeholders before being	Preventative Control: Training provided to contact teams to identify potential whistleblowing reports and ensure these are correctly handled, e.g.: • Grapevine,	Whistleblowing Officer	Annually

POL00423693

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
	passed onto the Whistleblowing Officer	• NBSC, • Customer Support, and • Executive Complaints. Communications and awareness provided to all employees and Policy document published on the Intranet. Corrective Control: All incidents of breaches are be escalated to the Whistleblowing Officer to investigate and take appropriate actions.	Head of Financial Crime Whistleblowing Officer	Annually Ongoing
Insufficient Information	Failure to capture/report sufficient information about the issue may mean that the underlying issue cannot be properly investigated and resolved	Directive Control: Employees are encouraged to report issues and provide full information and their contact details, where they feel able to do so Corrective Control: All reports, including those where insufficient information has been provided and no further action was taken are recorded on the Whistleblowing database, which is reviewed for trends and issues.	Whistleblowing Officer Whistleblowing Officer	Ongoing Ongoing
The 'Speak Up' Service	Failure to effectively record whistleblowing reports and pass onto the Whistleblowing Officer, due	Preventative Control: The Whistleblowing Officer must review the effectiveness of the service provided by InTouch Ltd at least annually	Whistleblowing Officer	Annually

POL00423693

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
	to factors such as resource or IT failure.	The Whistleblowing Officer must review the effectiveness of the processes operated by each of Grapevine, NBSC, Customer Support, and The Executive Complaints Team at least annually to ensure that whistleblowing reports are identified and communicated promptly.	Whistleblowing Officer	Annually
Treatment of Whistleblowers	Breach of whistleblowing guidelines such that a whistleblower suffers prejudice as a result of making a report	Preventative Control Training must be provided to all people managers as part of their induction process as a manager and on appointment to Post Office	Whistleblowing Officer and HR Training Manager	Ongoing
		Annual training must be provided to all Post Office staff to remind them of the protections available to whistleblowers and the importance of identifying and reporting wrongdoing	Whistleblowing Officer and HR Training Manager	Ongoing
		The Code of Business Standards must refer to the whistleblowing policy and must be provided to all new joiners as part of their induction programme.	Whistleblowing Officer and HR Training Manager	Ongoing

POL00423693

3. Definitions

3.1. Definitions

Grapevine
24/7 Security Support Centre provided by Kings Ltd. Grapevine provide security advice and record all security incidents across the business, this includes burglaries, robberies and the reporting of suspicious activity.

Telephone Number: GRO
E-mail: GRO

NBSC
Network Business Support Centre (NBSC) is a helpline and the first port of call for Post Office branches if they have any operational query or require assistance.

Telephone Number: GRO
E-mail: GRO

Customer Support Team
Complaints handling team based in Chesterfield. The team address complaints reported into Post Office via various channels, including post and telephone.

E-mail: GRO

Executive Complaints Team
This team handles all complaints addressed directly to the Group Executives. The team liaise with various stakeholders within the business in order to resolve complaints.

E-mail: GRO

POL00423693

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. Whistleblowing can be reported via the following channels:

- 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 Whistleblowing Officer, who can be contacted by email at: whistleblowing@postoffice.co.uk or by telephone on: GRO
- Alternatively staff can use the Speak Up service available on 0800 0484531 or via the secure on-line web portal: http://www.intouchfeedback.com/postoffice

In some instances it may be appropriate for the individual to report in the form of a complaint to Grapevine, the Customer Support Team or the Executive Complaints Team.

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.

POL00423693

5. Governance

5.1. Governance Responsibilities

As at the date of approval of this Policy, the General Counsel is both the Policy Sponsor and Policy Owner, responsible for oversight of the Policy.

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.

POL00423693

6. Control

6.1. Policy Version

Date	Version	Updated by	Change Details
27th April 2016	1.4	Jane MacLeod	Sponsors review and sing-off
21st August 2017	1.5	Vitor Camara	Annual Review and update.

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: Whistleblowing Officer

Policy Author: Head of Financial Crime

Next review: August 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.

POL00423693

Protecting Personal Data Policy

Author: Chris Russell Sponsor: Jane MacLeod Meeting date: 13 September 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.

POL00423693

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.

POL00423693

GROUP POLICIES

Protecting Personal Data Policy

Version – V1.2

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.

POL00423693

1. Overview 3
1.1. Introduction by the Policy Owner 3
1.2. Purpose 3
1.3. Core Principles 3
1.4. Application 4
1.5. Data Privacy Risk 5
1.6. Legislation 5
2. Risk Appetite and Minimum Control Standards 6
2.1. Risk Appetite 6
2.2. Policy Framework 6
2.3. Who must comply? 7
2.4. Minimum Control Standards 8
3. Tools 12
3.1. Data Protection Impact Assessment 12
4. Where to go for help 13
4.1. Additional Policies 13
4.2. How to raise a concern 13
4.3. Who to contact for more information 13
5. Control 14
5.1. Policy Version 14
5.2. Policy Approval 14

POL00423693

1. Overview

1.1. Introduction by the Policy Owner

The General Counsel has overall accountability to the Board of Directors for 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 govern 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 and associated legislation (lawfulness).

2. Purpose Limitation

Post Office can only use Personal Data for the purpose that it was originally collected and limit any further Processing of that Personal Data according to the purposes notified to the Data Subject.

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.

POL00423693

4. Accuracy

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

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 by removing contacts that are no longer using Post Office products or services.

5. 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.

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).

6. Integrity & Confidentiality

Post Office must Process Personal Data in a manner that ensures appropriate security 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.

7. 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 subject to either internal audit or external regulatory scrutiny, and can demonstrate their compliance with this Policy, its corresponding standards and guidance 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 Protection 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.

POL00423693

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.

All investigations into breaches of this Policy, will be managed and controlled by the Data Protection Function. All investigations will be conducted in conjunction with the Security Operations Centre.

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

POL00423693

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 will establish and maintain a suite of Data Protection policies and standard operating procedures (SoPs) and guidance, 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 suite of documents 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

POL00423693

2.3. Who must comply?

Compliance with this policy is mandatory for all Post Office Employees. 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 offence.

POL00423693

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

POL00423693

		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

POL00423693

		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

POL00423693

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

POL00423693

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)

.

POL00423693

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

POL00423693

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: September 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.

POL00423693

Post Office

Code of Business Standards

POL00423693

Contents

Forward by our Chief Executive	3
Our Heritage and Values	4
Introducing the Code	4
Observing the Code	4
Our Brand	5
Customer Excellence	5
Our People	6
Business Behaviours	6
Personal Behaviours	7
Valuing Diversity and Inclusion	7
Creating and Maintaining a Safe and Healthy Place of Work	8
Health and Wellbeing	9
Protecting the Environment	9
Use of Alcohol, Tobacco and Illegal Drugs	9
Use of Computers, Internet, Phones and Email	10
Social Media	10
Engaging with the Media	11
Political Activity	11
Conflicts of Interest	11
Gifts and Sponsorship	12
Hospitality and Entertainment	12
Fraud and Financial Crime	13
Risk Management	13
Modern Slavery	13
Consequences of Non-Compliance for the Code of Business Standards	14
Making Proper Decisions and Seeking Help	14

POL00423693

Forward by our Chief Executive

Dear Post Office 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.

Our Code of Business Standards sets out our enduring commitment to ethical behaviour and ensures our policies and processes are relevant and appropriate to today's dynamic operating and regulatory environment. Regardless of the challenges that arise in achieving our ambitions, our commitment to how we do business is unwavering.

I expect everyone at Post Office to read this document carefully 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 the Post Office. And, most importantly, thank you for your commitment to ensure our customers and the communities we serve, continue to place their trust in us.

GRO

Paula Vennells

POL00423693

Our Heritage and Values

The Post Office has thrived at the heart of communities across the UK for over 370 years. We are one of the country's most trusted brands and we take our commitment to provide essential services very seriously. We are 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.

Introducing the Code

Our Code of Business Standards defines how we operate.

In developing the Code of Business Standards, we have drawn inspiration from our heritage and values as well as the law. It is intended to guide the way we behave and give us standards to measure ourselves**.** It sets out what people can expect when working for and with the Post Office. It is designed to provide guidance and support in making decisions and carrying out work in a way that is compatible with our values, policies and processes and the law. As the legal and regulatory environments evolve, the Code will adapt to accommodate such changes.

By consistently adhering to this Code we will continue to foster and strengthen a culture that will help us to continue to be a business to be proud of – a **'Great place to work'** that is **'Simpler to run'** and **'Better for customers'.**

Observing the Code

Everyone employed by, acting on behalf of, or representing, Post Office (including contractors, consultants, and other service providers) is required to adhere to the Code; they are expected to operate in line with it and the corresponding Group Policies.

As a Post Office colleague, you are required to:

- Read and understand the Code of Business Standards and work-related policies and incorporate them into your work and behaviours;
- Complete all mandatory training on time;
- Report potential unlawful behaviour or breaches of the Code or company policies;
- Cooperate fully with company investigations;
- Never victimise colleagues for 'calling it out';
- Ask questions when you're unsure.

If you are a manager, you have additional responsibilities to:

- Promote the Code of Business Standards and work-related policies, incorporating them into the work of your direct reports;
- Set a fitting example for others though your own behaviour;
- Ensure that your team members know they can come to you with questions or concerns and that you'll listen to them and respond appropriately;
- Never make promises or make commitments to partners, suppliers or your direct

POL00423693

reports beyond your authority;
- Not create policies, rules or guidelines that are less restrictive than the Code or any other company polices;
- 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 Performance Development Reviews.
- Ensure that bullying and harassment is not tolerated in our workplace. See Bullying and Harassment Policy and Grievance Policy and Procedure.
- 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.
- 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 on time 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 Trial Policy and Procedure.

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

Our Brand

Our brand experience, for employees, customers, partners and stakeholders is 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, and we use them as a guide to improve our people processes including recruitment, learning and development, talent and performance management.

In short, it's how we do things to deliver our brand commitment to customers.

Customer Excellence

Our customers are at the heart of everything we do.

We all know what it feels like to experience good and poor customer service. We need to ensure that we deliver great service for all customers, every time they interact with us. 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 and understanding their needs and expectations
- by communicating respectfully, leaving out the jargon, providing them with the best service and products that meets their needs
- by always thinking about them and not the process
- by keeping it simple and straightforward to reach us - in branch, online, mobile

POL00423693

Our People

With a diverse range of backgrounds, talents and perspectives, Post Office is in a unique position to understand our customer needs.

At Post Office, we differentiate ourselves through the dedication of our people. Our rich and diverse cultures and experiences help us make connections with our customers and sustains the continued success of our brand. To maintain this, we treat each other with respect, even when our differences may set us apart.

We aspire to provide a positive work environment. This means that regardless of our differences, we can work without fear of discrimination, harassment or victimisation.

Employment decisions - whether they be related to hiring, promotions, transfers or terminations – are based on merit, equity and fairness.

Post Office operates a **zero tolerance** to any form of discrimination, including based on:

- Race
- Colour
- Religion or Faith
- Age
- Sexual orientation, gender, or gender identity expression
- National origin, geographical or demographic background
- Pregnancy or Maternity
- Any other classification protected by UK law

We do not tolerate any form of bullying or harassment, whether written, verbal, visual or physical, including:

- Sexually suggestive statements or actions
- Inappropriate or offensive comments or 'jokes'
- Inappropriate conduct or contact
- Threats

If you have a concern 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.

Business behaviours

Our behaviours are based on our core values of Care, Challenge and Commit.

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.

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

POL00423693

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.

Personal Behaviours

We expect high standards of personal behaviour at work

Behaviour which damages service to customers, or the reputation or efficiency of Post Office, is unacceptable. This extends to poor attendance, lateness, dishonesty, drunkenness, use of illegal substances, and violent or disorderly behaviour or abusive language.

Maintaining our standards means we:

- Conduct ourselves appropriately and professionally
- Act as an ambassador for the company
- Operate within the law
- Do not bring Post Office into disrepute
- Do not claim money for hours you did not work, a journey you did not make or an expense you did not incur
- Do not use inside information about a company transaction for personal profit

We should all demonstrate:

- Honesty and integrity
- Efficiency and reliability
- Punctuality and good attendance
- A smart and clean appearance - and where uniform is provided by Post Office, it should be worn as intended
- A credible image to the public

Valuing 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 workforce 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 professional and positive work environment
- Promote a culture of inclusivity where differences are accepted, valued and celebrated
- Inform their line manager of any instances of apparent discrimination or any

POL00423693

perceived problem in relation to employment
- 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.

Language:

The common language of business should be English (English or Welsh in Wales). However, so long as it doesn't jeopardise the job or health and safety of colleagues or members of the public and doesn't deliberately exclude people, colleagues should be able to communicate in their own language within reason.

Creating and Maintaining a Safe and Healthy Place of Work

We strive to work as safely as possible.

Everybody has the right to work in a safe and healthy environment. We will fulfil our promises without compromising the safety of our customers, colleagues, suppliers and all those affected by our activities.

Pursuing this aim reflects the high value we place on our employees and all those touched by our business activities:

- 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.

POL00423693

Health & 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, safety and wellbeing
- My HR provides expert advice and guidance for all managers on any HR related issue. Visit www.myHRhelp.co.uk for more information.
- Speak Up Whistleblowing hotline where our colleagues can raise concerns internally in confidence. See Whistleblowing Policy for more information.

Protecting 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 and maximising recycling opportunities
- The use of sustainable materials.

Use of Alcohol, Tobacco and Illegal Drugs

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.

Smoking (including vaping and e-cigarettes) is not allowed on company premises.

POL00423693

Use of computers, internet, phones and email

The security of our information and IT systems is critical.

Many 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 when working in public areas.

To help protect our systems and information, you should:

- 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 or 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 GRO or email postofficeservicedesk GRO

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.

Social Media

Digital and social media is a key part of modern life.

New digital technologies can help us engage actively with our customers. We can promote what we do and draw on innovative ideas. However, with these benefits comes greater responsibility.

As more colleagues can access the internet at work both on personal and official devices, it is important that we maintain the highest levels of propriety at all times. We must always act in a way that does not compromise the trust and confidence of our customers or the standards of behaviour expected of us.

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 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

POL00423693

- 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
- You must not appear to be endorsing any product or service (including retweeting comments)

The simple rule to remember is that the principles covering the use of social and other digital media in both work and in a personal capacity are the same as those contained in this Code of Business Standards and company policies that apply for any other activity.

Engaging with the Media

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 GRO GRO or pressoffice GRO

Political Activity

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.

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 or agent 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 or agent at work 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

POL00423693

- 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

Gifts and Sponsorship

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

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 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

We seek to comply fully with relevant legislation.

POL00423693

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, either committed on Post Office, or where Post Office might be used unknowingly to facilitate such action.

- 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 supported by mandatory training to develop their understanding of financial crime risks including Anti-money laundering, Politically Exposed Persons and Anti-Bribery & Corruption regulation.

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. Full details are available at <link TBC>

Risk Management

Effective risk management is integral to the management of our business.

Our risk management processes and practices are intended to help you make better informed decisions; increase the likelihood of meeting our strategic objectives, achieve customer excellence and safeguard our business interests.

Effective risk management is demonstrated by how we behave - considering risk in everything we do - from decision making, to operational management. We encourage people to consider and assess risks, manage them and be transparent throughout.

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 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.

POL00423693

Consequences of Non-Compliance for the Code of Business Standards

Compliance to Post Office Code and policies is not optional.

It is everyone's responsibility to follow our Code of Business Standards and the various related policies.

- Failure to comply with company policies and the law can carry profound consequences for Post Office and potentially 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.

Making Proper Decisions and Seeking Help

At Post Office, we set ourselves exacting standards. All our stakeholders, and others with whom we work, have an expectation that they will be treated professionally.

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 GRO

Please be aware that any breach of this Code may be dealt with under our Conduct Code,

POL00423693

and that gross misconduct could result in your dismissal.

POL00423693

9.1 Corporate Governance Reforms

Author: Natasha Wilson | Sponsor: Martin Kirke | Meeting date: 13 September 17

Context

This paper is to note a recent publication by the Government on Executive Remuneration and Corporate Governance intended to raise the public's trust in business.

In November 2016, BEIS issued a Green Paper on Corporate Governance and Executive Pay. The Green Paper recommended reform in the following areas:
- Executive pay;
- Strengthening the employee, customer and wider stakeholder voice; and
- Corporate governance in large privately held businesses.

The document published on 29 August contains the Government's response to the Green Paper consultation and a number of firm proposals.

Questions

1. What is the timing of the proposals?
2. What are the key proposals affecting Post Office?

Conclusions

1. Implementing the reform proposals will require a combination of changes to the UK Corporate Governance Code, voluntary industry action and secondary legislation.
2. The FRC intends to consult on amendments to the Code in late Autumn; the Government intends to lay draft legislation before Parliament before March 2018.
3. The Government's current intention is to bring the reforms into effect by June 2018 to apply to company reporting years commencing on or after that date.
4. The key proposals affecting Post Office:
    a. CEO: Employee pay ratio - the Government response confirms that the disclosure regulations will be amended to improve transparency with regard to directors' remuneration. The requirement will be to disclose the ratio of CEO pay to the average pay of a company's UK workforce, along with a narrative explaining changes to that ratio from year to year and how the ratio relates to pay and conditions across the wider workforce. This work is currently being looked at and will be discussed by the GE and Remuneration Committee.
    b. Strengthening of the employee, customer and wider stakeholder voice - the response states that the Government will introduce secondary legislation to require all companies of a significant size (private as well as public) to explain how their directors comply with the requirements of section 172 (Companies Act 2006) to have regard to employee interests and to fostering relationships with suppliers, customers and others.

POL00423693

This work is currently being looked at by members of the GE and other senior leaders to understand how we can incorporate this proposal within our current and future forums.

c. Other proposals relating to Remuneration Committees and pay will be discussed by the Remuneration Committee.

Input Sought

The Committee is asked to note the contents of this paper.

The Report

On 29 August, the government published a package of corporate governance reforms intended to raise the public's trust in business. Whilst executive remuneration forms much of the response, it does extend beyond pay and into broader considerations around wider stakeholder involvement and corporate governance in large private businesses.

The press and TUC have criticised the government of what they see as a watered-down set of proposals, however, I believe this a good opportunity for Post Office and we can address the requirements in a positive and pragmatic way.

In summary:

- Disclosure of the ratio of CEO pay to the average pay of the company's worker, along with a narrative explaining the changes to the ratio from year to year and how the ratio relates to pay and conditions across the wider workforce.

  Whilst the Government will give further consideration to the methodology for calculating the ratio, at present, it proposes that it should be calculated based on the CEO's total annual remuneration (ie as we disclose in the ARA) relative to the average total remuneration of the UK workforce.

- Strengthening the employee and wider stakeholder voice – the initial proposal back in April to require an employee representative on the Remuneration Committee or Board is not being taken forward. The FRC is to consult upon on different mechanisms (NED representation, employee advisory councils…).

- Corporate governance: The FRC will work with IoD and others to develop a voluntary set of corporate government principles which is likely to apply to companies with more than 2,000 employees.

- Boardroom diversity – the FRC is expected to take forward the BEIS Select Committee recommendations that from May 2020, at least half of all new appointments to senior and executive managements positions in the FTSE 350 and all listed companies are women.

There are other proposals that are specifically related to pay and these will be discussed by the Remuneration Committee.

POL00423693

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

POL00423693

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.

POL00423693

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.

POL00423693

(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** ……

POL00423693

Company no. 8459718 – Strictly Confidential

RCC 17/59 – 17/68

POST OFFICE MANAGEMENT SERVICES LIMITED (Company)
RISK, COMPLIANCE AND CONDUCT COMMITTEE (RCCC)
(A committee of the Executive)

Minutes of an RCCC meeting held at
Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ
On 31 July 2017 at 12.00pm – 1.30pm

Present:	Stephen Gaines (SG)	POMS Compliance Manager (Chair)
	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
	Mike Lowe (ML)	Project Manager
	James Dingwall (JD)	Interim Head of Compliance
	Alberto Zanatta (AZ)	Audit Manager
In Attendance		
Apologies:	Gerry Barrett (GB)	Head of General Insurance
	Gill Craig (GC)	Deputy for Head of Travel
	Elizabeth McMenemy (EMM)	Compliance Advisor
	Ann Young (AY)	Compliance Advisor

RCC17/59 **WELCOME, QUORUM AND CONFLICTS OF INTEREST**

The Chairman declared the meeting quorate and open.

RCC17/60 **MINUTES OF THE MEETING HELD ON 26 June 2017**

(a) The minutes of the meeting held on 26 June 2017 were approved and the Chairman was authorised to sign them as a true record of the meeting.

RCC17/61 **RISK MANAGEMENT**

(a) POMS ExCo Dashboard – ST discussed the five risks which remain outside of risk appetite.

(b) JD highlighted the potential risks and liability faced by POMS in reference to the Product Distribution risk. Specific concerns centred on what actions were being taken to mitigate customer detriment for identified challenges within WebHelp.

Action RT (c) RT agreed to check the Professional Indemnity (PI) policy.

(d) SG confirmed that a sample (17) upheld complaints closed by WebHelp had been subject to 2nd line checks which showed complaints were being closed down correctly.

POL00423693

Action RT/SG

(e) It was agreed by all that the need to review the process for tracking FOS complaints was required. RT/SG to review and agreed process.

(f) FC asked whether the risk rating for the Appointed Representative (AR) was likely to change once the EUM project concluded in September 2017.

(g) JD stated that the most likely outcome at best would be an 'Amber' rating. However, the impact of EUM would see an improvement in 1st line defence from a POL perspective in terms of T&C and improved monitoring in branches. JD concluded that a Risk Acceptance Note may be required.

RCC 17/62 **INCIDENT MANAGEMENT**

Action ST/RT/MB

(a) ST confirmed that the incident management definition and process is scheduled to be reviewed in August with the assistance of the Operations team.

RCC17/63 **1st LINE COMPLIANCE REPORT**

(a) QA results for Travel reported at 42. Actions are already underway to address identified issues. These are being addressed as part of Project Calibre.

(b) The increase in reported Travel claims and repudiation was attributed to seasonality.

(c) Cancellation reasons – identified trend highlighted issues of conduct relating to the sale of Travel Insurance both within branch and the contact centre due to errors. Volumes remain relatively low compared to the number of policies sold within the month.

(d) Complaints showed an increase in overall dissatisfaction in June (13.5%) and complaints volumes also increased by 13.3%. % of upheld complaints rose from 34.0% reported in May to 50.6% in June. Sharp rise attributed to the increase in closed complaints reported for Travel Insurance.

(e) Complaints trends identified continued issues in relation to the travel refund process, non-receipt of policy documentation and incorrect/insufficient information in branch.

Action RT/MB

(f) RT/MB to facilitate the process for reviewing the refund process and issues associated with the non-receipt of policy documentation for Travel Insurance.

RCC 17/64 **2nd LINE COMPLIANCE REPORTING**

(a) SG informed the RCC that 2nd line monitoring of calls have ceased temporarily while issues in WebHelp are being resolved. EMM will continue to support the delivery of Project Calibre.

(b) POMS Monitoring team – overall generic branch visits have ceased.

POL00423693

Decision to cease monitoring was taken as a result of the same issues being identified to which findings have already been shared and discussed with POL.

(c) SG stated the POMS Monitoring team with now focus on carrying out focused and targeted thematic reviews within the POL branch network.

RCC 17/65 **ASSURANCE ACTIVITY**

Action RT/MB

(a) RT advised that two complaints audits have been carried out by the Operations team. The audit rating for Cardif Pinnacle recorded a 'satisfactory' rating. The audit for BISL Ltd (Junction) recorded an 'unsatisfactory' rating. Copies of both reports to be circulated once signed off.

(b) Collinson audit on POMS is nearing its conclusion. SG informed that actions relating to venerable customers was the only outstanding issue. However he did envisage that Collinson may return in October 2017 to carry out a further audit.

Action JD

(c) JD to review the T&C requirement for Collinson.

(d) JD stated that the PWC audit report was 'acceptable' and very achievable.

RCC 17/66 **POLICIES AND PROCEDURES**

(a) JD - Senior Management Certificate (SMR) first draft is ready for review to which a draft training presentation will set out the program of embedding into POMS. A project manager has been assigned to manage the timings for rollout and relevant communications.

RCC 17/67 **MATTERS ARISING AND ACTIONS LIST**

(a) Agreed by all that Action Log will be circulated with required responses actioned.

RCC 17/68 **ANY OTHER BUSINESS**

(a) Ehtsham Ali, Senior Compliance Manager, ISAG to be invited to attend the next RCC meeting in August 2017.

(b) There was no other business raised. There being no further business the meeting was closed.

(c) The next meeting of the RCC will be held on 31 August 2017 at 10.30am.

Chairman…….. **Date** ……

POL00423693

9.3 Post Office Insurance renewal

Author: Mark Dixon Sponsor: Alisdair Cameron Meeting date: 13 Sept 2017

Executive Summary

Context

The business has a series of insurance policies due for renewal on 1 October 2017.

Question addressed in this report

1. What level of cover is proposed and how has this changed from last year?

2. Are RCC members aware of any claims bought in respect of risks under our Professional Indemnity or Directors & Officers Liability insurance or of regulatory investigations that should be disclosed to insurers?

Conclusion

A summary of the policies and cover can be found in the Broker's Pre-renewal Update Report, attached.

Insurances to be purchased are the same as last year. No significant changes are proposed. Coverage levels, with the exception of the extension to the Cyber policy coverage, have been kept in line with last year and all policy limits and deductibles for the current renewal are as per expiry.

These cover the business for most major risks albeit with high deductibles. We consider these levels of insurance to be reasonable and appropriate for the POL business.

POL has not made any claims against its insurers over the last year largely due to the significant levels of self-insurance (via deductibles).

The annual cost of insurance in 2016/17 was circa £1,230k, excluding IPT. We are finalising the cost for 2017/18 and expect small cost savings to be achieved, reflecting the reduction in size of our vehicle fleet and workforce, resulting in a total spend of **IRRELEVANT**, excluding IPT. It should be noted though that the rate of IPT has

POL00423693

increased from 10% to 12%. The overall net savings, after taking account of the IPT increase, are estimated at IRRELEVANT We propose using this saving to extend our Cyber insurance from the current coverage in relation to two specific contracts to cover the whole business.

Input Sought

The RCC is asked to approve the renewal as set out in the Brokers' report, for submission to the ARC and Board for approval.

POL00423693

The Report

What level of cover is proposed and how has this changed from last year?

1. IRRELEVANT were appointed as insurance broker to the Post Office in 2015 and have now worked with POL on its 2015, 2016 and 2017 renewals. They have helped achieve premium reductions of IRRELEVANT in 2015 and IRRELEVANT in 2016 as well as various improvements to our policies.

During 2016/17 we have re-aligned all expiry dates to ensure that all policies renew on 1 October.

2. POL purchases insurances expected for a business of its size and complexity. These comprise cover for: Crime; Motor; Combined Liability (Employers Liability and Public/Products Liability); Property Damage and Business Interruption; Directors and Officers Liability; Terrorism; Personal Accident/Business Travel; Professional Indemnity; and Cyber.

POL seeks to manage the cost of its insurance premiums through the size of the deductibles it takes (i.e. the amount that POL must pay before a claim can be made against the insurance provider). This effectively means that POL is "self-insured" for a portion of its risk. For example, under our Crime policy, which provides protection for POL against theft, fraud, and dishonesty committed by employees and third parties, in particular in relation to risks related to our cash centres, the deductible is set at IRRELEVANT. This implies that any individual loss would need to be in **IRRELEVANT** before a claim can be made against our insurers. The level of deductibles varies according to the class of insurance purchased. POL takes advice from its broker when deciding the level of these deductibles.

A summary of the policies and cover proposed for renewal, including details of deductibles and sums insured, can be found in the Broker's Pre-renewal Update Report, attached. A full Renewal Report will be provided by the Broker after renewal is concluded.

3. Insurances purchased are the same as last year. No significant changes are proposed. Coverage levels, with the exception of our Cyber insurance (see 7. below), have been kept in line with last year and all policy deductibles for the current renewal are as per expiry.

POL00423693

These cover the business for most major risks albeit with high deductibles. We consider these levels of insurance to be reasonable and appropriate for the POL business.

4. POL has not made any claims against its insurers over the last year largely due to the significant levels of self-insurance (via deductibles).

5. The annual cost of insurance in 2016/17 was circa IRRELEVANT, excluding IPT. We are finalising the cost for 2017/18 and expect small cost savings to be achieved, reflecting the reduction in size of our vehicle fleet and workforce, resulting in a total spend of IRRELEVANT, excluding IPT. It should be noted though that the rate of IPT has increased from 10% to 12%. The overall net savings, after taking account of the IPT increase, are estimated at IRRELEVANT We propose using this saving to extend POL's Cyber insurance from the current coverage in relation to two specific contracts to cover the whole business (see 7. below).

6. Motor, Combined Liability and Property Damage cover are all on multi-year agreements put in place last year to achieve cost savings.

7. Our existing Cyber coverage applies only to IRRELEVANT

IRRELEVANT

IRRELEVANT

In connection with the IRRELEVANT tender we explored extending coverage to a third contract. It was concluded that this was not possible in the market and that to satisfy the tender requirements we would need to extend coverage from the existing two contracts to the whole business.

Given that the need for Cyber insurance is increasingly likely to become a requirement under future tender processes, this seems a sensible approach.

The annualised premium at the time of the last renewal was IRRELEVANT At the time of the IRRELEVANT tender we obtained a quote to extend our Cyber coverage. It was estimated that this would IRRELEVANT the cost of the insurance.

POL00423693

We therefore propose that for the 2017 renewal we extend coverage to the whole POL business. We estimate that the additional cost of the Cyber coverage will be met from savings under other policies (see 5. above). We are obtaining quotes on this basis.

Are RCC members aware of any claims in respect of risks under our Professional Indemnity or Directors & Officers Liability insurance or of regulatory investigations that should be disclosed to insurers?

8. In connection with the renewal of POL's Professional Indemnity insurance we must make the following statement to insurers:

Following enquiry, we are not aware of any claims in respect of the risks to which this insurance relates ever been made against the business or any of the Principals, Partners or Directors. Furthermore, the Principals Partners or Directors, after full enquiry, are not aware of any circumstance which might give raise to any such claims.

We currently purchase IRRELEVANT The cover

IRRELEVANT

From our enquiries we do not believe that there is anything that is required to be disclosed to insurers. RCC members are asked to consider whether or not they are aware of anything that POL needs to disclose to the insurers as part of this process.

9. In connection with the renewal of POL's Directors & Officers Liability insurance we must make the following statement to insurers:

During the last 12 months, have any claims been bought against any insured persons or have there been any regulatory investigations into the company where an insured person has been required to attend?

Directors & Officers Liability insurance covers the cost of compensation made against POL's directors and key managers for alleged wrongful acts. Wrongful acts include: breach of trust; breach of duty; neglect; error; misleading statements; and wrongful trading.

We have already identified the following regulatory investigations:

- HMRC – VAT Audit
- HMRC – Anti-Money Laundering/Counter Terrorism Finance

POL00423693

- Proposed audit of Telecoms under Privacy and Electronic Communications Regulations (due in January 2018)

From our enquiries, other than the items set out above, we do not believe that there is anything that is required to be disclosed to insurers. RCC members are asked to consider whether or not they are aware of any additional claims or regulatory investigations that POL needs to disclose to the insurers as part of this process.

Appendix 1: Brokers Pre-renewal Update Report

POL00423693



Post Office

2017/18 Insurance Renewal

Pre-renewal Update Report

September 2017

LOCKTON
Broking done *differently*

POL00423693

Executive Summary

Background

This paper sets out a high level summary of outcome of the renewal of the Post Office insurances due for renewal on October 1st 2017. The key points to note include:

- This year we currently estimate to achieve like for like premium IRRELEVANT IRRELEVANT, adjusted to reflect reductions in the size of your business, again with some improvements to your policies.
- All policy cover, limits and deductibles remain unchanged from 2016/17.
- Post Office has not made any claims against its insurances in the past year, largely due to the significant levels of self-insurance (via deductibles) that you take*.

* Claims Commentary – Post Office has not had a claim that has breached the policy deductibles in recent years. You have relatively high deductibles which help the reduce premium spend - but you also have a low frequency of incidents below the deductibles for a company of your size. This might be regarded as a reflection on the quality of your risk management. Full details of your claims experience are available if required.

POL00423693

Programme structure chart

The chart below shows the various insurances Post Office currently purchase (details as proposed for renewal at 01/10/2017).

IRRELEVANT

Crime	Motor (Third Party Only)	Combined Liability	Property Damage & Business Interruption	Directors & Officers	Post Office Ltd Professional Indemnity	Post Office Management Services	Sabotage & Terrorism	Personal Accident & Business Travel	Cyber	Contingency
										IRRELEVANT

POL00423693

Summary of policy cover

Crime

This insurance is made up of a primary IRRELEVANT providing an overall limit of IRRELEVANT. The key risks are your IRRELEVANT but this policy also includes the IRRELEVANT risks you face.

Motor Liability

IRRELEVANT

Combined Liability

IRRELEVANT

Property Damage and Business Interruption

An IRRELEVANT although as with all insurances the policy does have exclusions. You only insure IRRELEVANT The policy is IRRELEVANT The policy also includes IRRELEVANT and a IRRELEVANT Indemnity Period.

Terrorism

Insurance against damage to your physical assets arising out of a terrorist incident, with a policy IRRELEVANT

Directors and Officers Liability

Covers the cost of compensation claims made against your IRRELEVANT and IRRELEVANT IRRELEVANT for alleged wrongful acts.

Wrongful acts include:

- IRRELEVANT

Professional Indemnity

Professional Liability arising out of certain specific activities – you have IRRELEVANT which IRRELEVANT and IRRELEVANT for IRRELEVANT Both policies were originally purchased in respect o IRRELEVANT IRRELEVANT.

POL00423693

Cyber

Applies IRRELEVANT such as IRRELEVANT . It also includes IRRELEVANT IRRELEVANT

Personal Accident/Business Travel

Provides fixed benefits following bodily injury for IRRELEVANT

IRRELEVANT

Provides IRRELEVANT IRRELEVANT

IRRELEVANT

Special Contingency

Details of this are not widely circulated.

POL00423693

Premium summary

Policy	2016/17 Premium	2017/18 Premium	Percentage Premium Saving 2016/17 – 2017/18	2017/18 Premium Comments
Crime	IRRELEVANT			
Motor				
Combined Liability				
PI – POL				
PI – POMS				
Cyber				
PD & BI				
D & O				
Terrorism				
Contingency				
PA & Travel				
Total				
Total inc. IPT				

- Since IRRELEVANT appointment in 2015 overall premium spend has decreased by circa 50% (£578k), not allowing for reductions in the size of your business. Whilst at the same time enhanced policy coverage including lower deductibles on certain policies have been achieved.

POL00423693

Post Office Ltd
Risk & Compliance Committee meeting
13 September 2017

Location:

Boardroom 1.19 Wakefield , Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ, United Kingdom

ATTENDANCE LIST

ATTENDEES	SIGNATURE
MacLeod, Jane	
Cameron, Alisdair	
Houghton, Rob	
Kevin, Gilliland	
Kirke, Martin	
Mark, Davies	
Martin, Edwards	
Nick, Kennett	
Paula, Vennells	

Also in attendance

CoSec	

Additional access

Regan, Avene	
Smith, Debbie	