POL00400101

Post Office Audit, Risk and Compliance Committee Agenda

Date
28th September 2016

Start Time	Finish Time
14.30hrs	17.30hrs

Location
Room 1.19 Wakefield

Present	In Attendance			Apologies
• Carla Stent (Chair) • Richard Callard • Tim Franklin • Ken McCall	• Paula Vennells • Al Cameron • Jane MacLeod • Nick Kennett • Alwen Lyons • Mike Morley-Fletcher • Peter McIver, EY • Elena Belyaeva, EY	• Kevin Gilliland (item 3) • Jonathan Hill (item 3) • Owen Woodley (Item 3) • Amanda Bowe – POMS (Items 3.1) • Susie Hayward – POMS (Item 3.1) • Gordon Gourlay – BOI (Item 3.2) • Neil Fuller – BOI (Item 3.2) • Alec Hughes – BOI (Item 3.2)	• Julie George (Item 4) • Rob Houghton (Items 4 & 7) • Jonathan Waples (Item 7)	

	Agenda Item	Action Needed	Purpose	Lead	Time
1.	**Welcome and Conflicts of Interest**			Chairman	14.30
2.	**Minutes of the meeting held on 25th July 2016, Matters Arising and Actions List**	For approval	To approve the minutes of the meeting held on 25th July 2016, note the Matters Arising and update on the Actions.	Chairman	14.32
3.	**Financial Services Obligations**				
	3.1 POMS	For noting		Amanda Bowe/ Susie Hayward (POMS) Jonathan Hill / Kevin Gilliland / Owen Woodley	14.35
	• ARC Report		To receive a report from POMS ARC.		
	• POMS as Principal		Report on managing the AR relationship with POL for general insurance products.		
	3.2 BoI UK Report	For discussion	Report on managing the AR relationship with POL for banking products.	Jonathan Hill / Kevin Gilliland / Owen Woodley / Gordon Gourlay (BOI)/ Neil Fuller (BOI) / Alec Hughes (BOI)	14.45
	3.3 POL FS	For discussion	How POL meets its regulatory obligations.	Jonathan Hill / Kevin Gilliland / Owen Woodley	15.05
4.	**Cyber/ IT Security**	For discussion	To provide an update on Cyber/ IT security.	Julie George / Rob Houghton	15.30
5.	**Risk Report**				
	5.1 Group Risk Profile half year update	For discussion	To present to the Committee management's updates to their Top Risks and Key Further Actions.	Mike Morley-Fletcher	15.50
	5.2 Progress with Risk Management Framework	For noting	To update the Committee on progress on POL risk activity.		

POL00400101

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

Agenda Item		Action Needed	Purpose	Lead	Time
6.	**Internal Audit**				
	6.1 Quarterly Report and action	For discussion	To update the Committee on the POL Internal Audit activity and key outcomes.	Mike Morley-Fletcher	16.10
	BREAK				16.25
7.	**ARC Updates**	For discussion	To update the Committee on our resilience and lessons learned.		16.35
	7.1 Horizon Lessons Learnt			Rob Houghton	
	7.2 Business Continuity Planning			Jonathan Waples	
	7.3 AML CTF Framework and HMRC Audit			Jane MacLeod	
	7.4 BCV Lessons Learnt			Al Cameron	
8.	**Approval**				17.10
	8.1 Policies for ARC Approval (3)	Review and agree	ARC approval: Investigations, Physical Security, Business Change Management.	Jane MacLeod	
	8.2 Policies for ARC Approval to recommend to the Board (2)	Review and agree	ARC plus Board approval: Anti-Bribery & Corruption, Anti-Money Laundering.	Jane MacLeod	
	8.3 Insurance	Review and recommend to the Board	To agree the insurance cover for recommendation to the Board.	Al Cameron	
9.	**Items for Noting**:				
	9.1 Financial Reporting Update	For noting	To provide an update on the financial controls framework.		17.20
	9.2 Horizon Scanning	For noting	To provide an update on horizon scan of legal, regulatory or other external risks.		
	9.3 Contract Management	For noting	To update the ARC on the Contract Management work.		
	9.4 Property Compliance Update	For noting	To update the ARC on property issues.		
	CLOSE				17.30

POL00400101

Strictly Confidential

POLARC 16(5th)
POL ARC 16/37 – 16/40

POST OFFICE LIMITED
(Company no. 2154540)
('the Company')

Minutes of a meeting of the AUDIT, RISK AND COMPLIANCE COMMITTEE held at 12.30 pm on 25th July 2016 at 20 Finsbury Street, London EC2Y 9AQ

Present:

Carla Stent	Chairman
Richard Callard	Non-Executive Director (RC)
Tim Franklin	Non-Executive Director (TF)
Ken McCall	Non-Executive Director (KM)

In Attendance:

Paula Vennells	Chief Executive, (CEO)
Alisdair Cameron	Chief Financial Officer (CFO)
Jane MacLeod	General Counsel (GC)
Nick Kennett	Financial Services Director (NK)
Alwen Lyons	Company Secretary (CoSec)
Paul Hemsley	Financial Controller (PH)
Peter McIver	Ernst & Young (PM) by conference call
Elena Belyaeva	Ernst & Young (EB)
Mounia Mukina	Ernst & Young (MM) by conference call

POLARC 16/37 INTRODUCTION

(a) A quorum being present, the Chairman opened the meeting, and each Director confirmed that they had no conflicts of interest in relation to the business to be considered.

POLARC 16/38 MINUTES OF THE MEETINGS HELD ON 19TH MAY AND 5TH JULY 2016

(a) The minutes of the meetings held on 19th May and 5th July 2016 were approved as presented and the Chairman of the Committee was authorised to sign them as a true record.

POLARC 16/39 EY REVIEW AND REPORT OF THE BANKING FRAUD HIGHLIGHTED AT THE ARC ON THE 5TH JULY 2016

(a) The Chairman reminded the ARC of the five unresolved issues which needed to be resolved before the Annual Report and Accounts (ARA) could be signed, which had been highlighted at the meeting of 5th July:

1. That all comments from RC had been incorporated into the final ARA;
2. Final sign off of the pensions narrative to be received from Virginia Holmes;

POL00400101

Strictly Confidential

3. Confirmation from the Board Chairman that he was content with his statement;
4. A final report received from EY on the fraud issue discussed, and assurance from the CFO that remedial actions have been taken and processes have been put in place to prevent any further such fraud;
5. That the Letter of Representation could be finalised and would be signed after the EY investigation.

(b) Areas 1 to 3 had been completed, albeit the pension's narrative had been updated to reflect that a recommendation had now been made to the Trustee.

(c) The Chairman asked EY to report on the findings of their review. PM explained the forensic work undertaken by the EY forensic team and the recommendation highlighted in the report.

(d) The ARC considered the detail of the report, noting that EY had verified the accuracy of the reported fraud loss and asked if EY had considered any other the gaps in the sequences of BCV paying in slips. The CFO explained that a full reconciliation was carried out for all BCV related transactions and had cleared the suspense account. As the fraud was predicated on the time delay in carrying out that reconciliation and a full reconciliation between the BCV and the cash deposited had been completed, all instances of fraud would have been highlighted had further attempts been made.

(e) The CFO explained that the time taken for reconciliation, which in the past had been up to 3 weeks, had been reduced significantly, and that controls had been put in place to ensure that further attempts should be identified more quickly. EB confirmed that EY had reviewed the reconciliation process between the Horizon input and the IPSL input, and confirmed that this should highlight any cash discrepancies.

(f) The CFO explained that the long term solution to the issue would be to remove the need for a BCV with a direct electronic feed from Horizon to the banks. This solution was estimated to take about 3 months to implement and in the meantime additional controls would remain in place. It was therefore not possible to guarantee no further losses but they would be minimised, without interrupting the flow of customer deposits.

ACTION:GC (g) **The ARC asked the GC to ensure the Head of Security reengaged with police on the matter to understand what further could be done to support a prosecution.**

(h) The Chairman asked EY if they supported the signing of the ARA. PM did not believe that there were any further issues which should delay the signing.

(i) **The CFO promised to bring a lessons learned back to the September ARC meeting, to highlight what actions had**

POL00400101

ACTION: CFO

been taken to prevent any similar fraud; how the EY recommendations had been implemented; the status of the long term fix; and a review of the changes to culture of fraud management.

(j) The CFO stated that he was comfortable to sign the Letter of Representation as part of the ARA signing procedure.

(k) The ARC noted the EY report and agreed that the ARA be signed.

POLARC 16/40 **CLOSE**

(a) There being no further business the Chairman closed the meeting.

…… ……

Chairman **Date**

POL00400101

Strictly Confidential

Post Office Limited ARC Committee

Status Report as at: 16th August 2016

Action included on the ARC agenda
Action closed

REFERENCE	ACTION	Action Owner (GE Member)	Due Date	STATUS	Open/Closed
17 March 2016 POLARC 16/11 (f)	Report from POMS ARC The Committee asked for a paper for the September meeting explaining how POL had oversight of regulatory activity in branch and how issues are escalated.	**General Counsel**	September ARC	Agenda Item for **September ARC**	Open
22 January 2016 POLARC 16/03 (q)	Risk Update For the Executive to work with the external auditors to set out what a three year roadmap to benchmark against the UK Corporate Governance Code would like.	**General Counsel**	September 2017 ARC	Corporate Governance Capability - The Chairman of the ARC & GC have agreed to revisit the benchmarking with the UK Corporate Governance Code in a years time September 2017 ARC	Open
17 March 2016 POLARC 16/13 (d)	Risk and Control Update Consider how to make failure of any of the critical suppliers (e.g. ATOS, Fujitsu, BoI, RMG) more apparent on the Risk Profile, with an explanation of how Management are managing the risk.	**Mike Morley-Fletcher**	September ARC	Critical supplier failure will be made more explicit when the Top Risks are reviewed with GE members at the half year and reported to **September ARC**.	Open
17 March 2016 POLARC 16/13 (e)	Risk and Control Update Consider how to update the ARC/Board on the current risks facing the business at a point in time and relating these back to the 'top risks', giving greater clarity on the 'risks of the moment'.	**Mike Morley-Fletcher**	September ARC	'Risks of the Moment' will be considered when the Top Risks are reviewed with GE members at the half year and reported to **September ARC**	Open
17 March 2016 POLARC 16/13 (c)	Risk and Controls Update Description of top risks to be amended where relevant to identify the contribution to the top risks of issues such as Iris or Trinity.	**Mike Morley-Fletcher**	September ARC	The impact of issues such as Iris and Trinity will be considered when the Top Risks are reviewed with GE members at the half year, particularly in mitigation plans and reported to **September ARC**	Open
19 May 2016 POLARC 16/22 (e)	Report from POMS ARC A meeting of the POMS and POL ARC should be arranged in September.	**Company Secretary**	September	Meeting taking place on 28th September	Closed

POL00400101

REFERENCE	ACTION	Action Owner (GE Member)	Due Date	STATUS	Open/Closed
19 May 2016 POLARC 16/23 (f)	Horizon Outage The ARC asked internal audit to check the incident and recovery process to ensure it had worked correctly.	**Mike Morley-Fletcher**	September ARC	Agenda Item for **September ARC**	Open
19 May 2016 POLARC 16/23 (g)	Horizon Outage The CFO was asked to update the Board and come back to the ARC in September with a report on the root cause analysis of the incident.	**CFO**	September ARC	Agenda Item for **September ARC**	Open
19 May 2016 POLARC 16/27 (d)	Risk and Control Update The ARC asked that Physical Security be reported to the ARC, and Treasury Risk Management be recommended by the ARC for Board approval.	**Mike Morley-Fletcher**		Physical Security policy will be provided to **Sept ARC** for approval. Treasury Risk Management policy amended to return to the **ARC in Septembe**r for recommendation to the Board.	Open
19 May 2016 POLARC 16/27 (g)	Risk and Control Update To set up an arcchairman@ GRO email address and to quote the address in the whistleblowing policy.	**Company Secretary**	Before policy posted on website	emal in place and monitored by the GC	Closed
19 May 2016 POLARC 16/27 (i)	Risk and Control Update To carry out a further BCP test in due course and include the test in the Horizon report to the ARC in September.	**General Counsel**	September ARC	On **September ARC** agenda	Open
19 May 2016 POLARC 16/27 (j)	Risk and Control Update To provide the ARC with further detail of the business continuity capabilities of the top suppliers, by materiality and complexity.	**General Counsel**		On **September ARC** agenda	Open
19 May 2016 POLARC 16/28 (b)	Internal Audit Business Transformation Portfolio Management including the overall assurance plan would be presented at the September ARC.	**Mike Morley-Fletcher**	September ARC	On **September ARC** agenda	Open
19 May 2016 POLARC 16/28 (d)	Internal Audit To provide a report on the actions put in place to mitigate the risks highlighted in the Treasury report.	**CFO**		Treasury report included in follow up audit actions	Closed
19 May 2016 POLARC 16/28 (h)	Internal Audit To write to the members to explain what would be presented at the September ARC in relation to Contract Management.	**General Counsel**	September ARC	A paper on Contract Management is provided on Septemebr ARC agenda.	Open
19 May 2016 POLARC 16/28 (j)	Internal Audit EY were asked to pull out examples of where contracts were examined during the audit.	**EY**		EY to provide more detail on contracts included in the 2016/17 audit.	Closed

POL00400101

REFERENCE	ACTION	Action Owner (GE Member)	Due Date	STATUS	Open/Closed
19 May 2016 POLARC 16/29 (b)	AML & CFT Audit Activity To report any material findings of the Promontory Report to the September ARC.	**General Counsel**	September ARC	On **September ARC** agenda	Open
5 July 2016 POLARC 16/34 (l)	Banking Fraud committed by a former Subpostmaster The ARC asked for an internal audit of the processes involved with a report to the September meeting.	**MMF**		On **September ARC** agenda	Open

POL00400101

Report from the 13 September 2016 meeting of the Post Office Management Services Ltd (POMS) ARC

Author and Sponsor: Amanda Bowe, POMS ARC Chairman Meeting Date: 28 September 2016

1. Reporting Arrangements

1.1 The POMS ARC Chairman, Amanda Bowe, provides the Post Office ARC with a written report from each meeting of the POMS ARC, where timing allows.

1.2 In accordance with the terms of reference for the Post Office ARC, the latest set of approved minutes of the POMS ARC will be provided to each meeting. Minutes of the 19 May 2016 POMS ARC meeting are now provided.

1.3 I will be attending this POL ARC in person to present my paper. The financial services 'deep dive' with presentations from the POMS Executive (among others) will also provide a good opportunity to discuss the relationship between POMS and the Post Office and their relative responsibilities as Principal and Appointed Representative in the distribution of the relevant POMS' insurance products.

2. Summary

2.1 We are one year on from the completion of Project Hawk, the formation of the ARC and my appointment as Chairman. Good progress has been made in developing a risk management framework and the quality of reporting to the POMS ARC has improved over the course of the year. Core risk policies have been developed, approved or adopted from Post Office together with processes for supporting risk identification, assessment, reporting and acceptance, achieving the priorities set for the first year. Looking ahead, the ARC's focus will shift from risk management processes to the substance of the risks. In particular the ARC will monitor the Executive's embedding of the risk management framework and its use in day to day business decisions and operations.

3. Update from the 13 September 2016 POMS ARC

3.1 At its meeting on 13 September 2016, the POMS ARC's main focus was on the consideration of the risks posed by Post Office as the Appointed Representative (AR) for POMS. The FCA recently conducted a thematic review of Principals and their ARs in the general insurance sector. The FCA's report set out the issues identified and the regulator's concerns. The POMS ARC received a detailed report from the head of Risk and Compliance of the FCA's findings and any gaps in POMS oversight of POL. This was followed up by a discussion at the Board on 20 September with a paper from Post Office

POL00400101

colleagues on the action plan proposed to address the risks. This will provide a key focus for the deep dive of financial services on the September Post Office ARC agenda.

3.2 In relation to the AR risk, the POMS Board has made clear the need to identify, prioritise and progress the key actions required to ensure the risks are brought within risk appetite or removed if necessary. This will come back to the POMS ARC in November.

3.3 In addition to the discussion on the FCA thematic review the ARC also:

(a) discussed the development of the risk management framework, its evolution alongside the business strategy and how this should be utilised in business proposals;

(b) received an update on risk and compliance activities, including: the risk framework; an update on top risks; regulatory related management information including detail on compliance requirements and developments; information on incident reporting and control failures; and updates on new business developments and horizon scanning;

(c) noted a high level overview of cancellations data, prior to the submission of a more detailed paper to the POMS ARC in November 2016;

(d) approved the adoption of the following Post Office Group policies: Financial Crime; Anti-Bribery and Corruption; Anti-Money Laundering and CTF. Approved the following POMS policies and processes: Risk Acceptance Process; Risk Management Process; and Regulatory Breach Management Policy;

(e) noted progress against the compliance monitoring plan and received an update on any reviews and/or actions since the last meeting;

(f) received a report from the internal auditor on: (1) internal audit activities and the progress against the 2016/17 Plan; and (2) an update on progress against the actions arising from the internal audit findings on the follow up of the Hawk readiness review (undertaken by PwC); and

(g) recommended to the Board that Ernst & Young LLP should be reappointed as the external auditor for 2016/17.

4. Input Sought

4.1 The Committee is asked to note the report.

POL00400101

PARC 16/16 – 16/31

POST OFFICE MANAGEMENT SERVICES LIMITED
(the Company)

Minutes of an Audit, Risk and Compliance Committee
held at Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ
on Tuesday 10 May 2016 at 2.00pm

Present:	Amanda Bowe	Non-Executive Director and Committee Chairman (Chairman)
	Stephen Ashton	Chairman (SA)
	Jane MacLeod	Non-Executive Director (JM)
In Attendance:	Rob Clarkson	Managing Director (RC)
	Kevin Gilliland	Post Office Network and Sales Director (KG) (for 16/21)
	Susie Hayward	Head of Risk and Compliance (SH)
	Jonathan Hill	Post Office Financial Services Head of Risk, Banking Regulation and Strategy (JH) (for 16/21)
	Garry Hooton	Post Office Interim Head of Internal Audit (GH)
	Nick Kennett	CEO (NK)
	Victoria Moss	Deputy Company Secretary (VM)
	Colin Stuart	Finance Director (CS)
Apologies:	None	

PARC 16/16 WELCOME AND CONFLICTS OF INTEREST

(a) The Chairman welcomed everyone and declared the meeting quorate.

(b) There were no changes to the standard declarations of potential conflicts of interest recorded for directors.

PARC 16/17 MINUTES OF THE MEETING HELD ON 15 MARCH 2016

(a) The minutes of the meeting held on 15 March 2016 were approved as an accurate record and the Chairman was authorised to sign them.

PARC 16/18 MATTERS ARISING AND ACTIONS LIST

(a) **Action PARC 15/04(h)** – the Committee noted the need for a pricing policy but agreed that the action should be closed.

(b) **Action PARC 15/05(b)** – it was agreed that this action should be closed.

(c) **Action PARC 15/17(o)** – SH confirmed that the review of the complaints process was underway and that a workshop with stakeholders had been scheduled for the end of May 2016. It was agreed that SH would clarify the timetable for providing feedback to the Committee, which should occur prior to the next meeting of the Committee on 13 September 2016.

ACTION: SH

(d) **Action PARC 16/06(l)** – it was agreed that this action should be closed,

POL00400101

contingent on no issues being raised at the close of the external audit for 2015/16.

(e) **Action PARC 16/07(r)** – the Chairman confirmed that she had discussed with SH the definitions of what regulatory breaches were reportable. It was agreed that SH would document the proposed approach for submission to the Committee in September 2016. NK confirmed that if any material regulatory breaches or concerns arose outside the cycle of meetings they would be submitted to the Board.

ACTION: SH

(f) **Action PARC 16/08(h)** – it was agreed that once the cancellations paper had been drafted for submission to the Committee in September 2016, assuming it fully addressed the action, the action could be closed.

ACTION: SH/ VM

(g) **Risk workshop** – it was agreed that the actions from the Board risk workshop would be reviewed, closed where appropriate, and submitted to the next risk workshop on 14 June 2016. Any actions which remained open would be added to the Committee's actions list.

ACTION: SH/ VM

(h) The Committee noted both the actions list from previous meetings and the list of actions arising from the Board risk workshop.

PARC 16/19 **INTERNAL AUDIT UPDATE**

(a) GH introduced his paper which presented an update on the activities provided by Post Office internal audit for the Company, approved at the March 2016 meeting of the Committee, particularly on the positive progress with planning for 2016/17 internal audit reviews.

(b) GH continued that internal audits had been planned for 2016/17 to look at the following three areas: the financial reporting process; the effectiveness of the Company's risk and compliance function; and oversight of outsourced activities, the appointed representative and third parties. The paper also provided information on the planned internal audits of Post Office covering areas which impacted the Company's risks.

(c) GH explained that the internal audit budget for 2016/17 was still an indicative draft which was being worked through. The Chairman asked that the budget be represented in terms of technical expertise required and in 'person days', split between internal resource and PwC. It was also asked that 'person days' be included in the compliance plan.

ACTION: GH/ SH

(d) Since the understanding was that internal audits should focus on key risk areas, SA asked whether financial reporting (the first planned audit for 2016/17) was a key risk. SH explained that the end of the Company's first financial year was a good opportunity to review financial processes and controls. The Committee agreed to this inclusion.

(e) The Committee considered the draft scope of the scheduled Post Office internal audit on training and competence in branch network sales, as set out in appendix 1 to the paper. It was confirmed that this work would set a helpful benchmark, against which any future assessments could be set, in addition to documenting any gaps and putting in place a formal plan as appropriate. The scope of the audit covered all sales touch points where assurance was required and included a whole range of financial

POL00400101

services products.

(f) The Committee noted the update on the progress with the 2016/17 internal audit plan.

PARC 16/20 **INTERNAL AUDIT COMPLIANCE READINESS REVIEW OF POST OFFICE MANAGEMENT SERVICES LIMITED (PWC REPORT)**

(a) GH introduced his paper which provided an update on the follow up of the progress with the audit actions raised in the compliance readiness review of the Company dated October 2015. This follow up had been carried out by internal audit with the support of PwC, the co-source provider of assurance services.

(b) GH reported that good progress had been made to date. No increased risk to the Company from a regulatory perspective had been identified and the review had been carried out with good diligence. He confirmed that, as interim head of internal audit, he was content with the progress made.

(c) GH referred the Committee to the 71 actions listed in the paper and gave an update to some of the figures. Of the actions listed, 21 had now been closed, 38 were open and on track, one was overdue (to be addressed by KG's paper later on the agenda) and 11 had been reopened for further review. Of these 11 actions, five concerned the review of the terms of reference (ToR) of the Committee or of the Company's executive committees. These actions were neither urgent nor material and would therefore be reviewed as part of the next scheduled reviews. The ToR action for the Committee was *"Management to consider whether the POMS ARC should also clearly signpost its responsibility for compliance"* which would be considered at the Committee's annual ToR review in September 2016.

ACTION: VM

(d) The Chairman asked for all actions to be prioritised by importance rather than by deadline.

ACTION: GH

(e) Regarding compliance, GH confirmed that the quality and quantity of second line reporting management information was reviewed on a constant basis. The Chairman had given feedback to SH on what second line information was particularly useful and noted that revisions to this reporting would be in place by the next meeting of the Committee in September 2016.

(f) GH confirmed that his team was following up on all actions with an aim of completion by the September 2016 meeting of the Committee. The Committee requested a comprehensive update on risk management to be submitted to the July 2016 meeting of the Board.

ACTION: GH/ SH

(g) SA referred to page 6 of the PwC report which stated that some identified actions were not recorded in the Company's action plan. SH explained that this concerned how things were presented and GH confirmed he was content that all issues had been covered. The Committee was reminded that the status of the report was still draft. PwC had been quite slow in completing the work and the executive was now keen to close down the report as soon as possible and to focus on the resulting actions.

POL00400101

(h) The Committee agreed that the overall structure of the PwC review should be used to develop a framework for the assessment of all projects. This framework should address the following questions: what are the risks of the current situation? What are the risks within the risk appetite and those outside? What is the timing for addressing the actions and in what order should they be addressed? Are the management actions to address them providing comfort? Use of the framework should result in an end state level of mitigated risks with correctly prioritised actions.

ACTION: GH

(i) The Committee noted the progress made with confirming the actions resulting from the follow up review and with agreeing a correctly prioritised timetable to address them. The Committee further noted that the actions were in the three key areas of: Appointed Representative risk; complaints processes; and company policies.

PARC 16/21 **OVERSIGHT OF POST OFFICE LIMITED**

(a) KG and JH joined the meeting.

(b) The Chairman welcomed KG and JH to the meeting and thanked them for the comprehensive paper. KG was asked for his view on the key risks arising from Post Office's role as appointed representative (AR) of the Company, focussing on the regulated financial services activity conducted within the branch network, and the timescales for reducing the level of risk.

(c) KG noted the context of increasing levels of industry regulation and confirmed his recognition that any regulatory breaches would be very damaging to brand and reputation, Post Office's most important asset. He also recognised that managing risk cost effectively over more than 11,500 branches was a significant challenge. The largest potential risks were in those branches with greater sales volumes and he assured the Committee that in those branches good controls were in place with branch reports and audits from Bank of Ireland. Previously 20-25 per cent of identified risks had been recorded as 'red' but this figure had now reduced to below 10 per cent. Concentrating on embedding the right culture across Post Office Group was key to ensuring the right customer outcomes.

(d) KG explained that 50-90 per cent of financial services transactions took place in the largest 700 branches where there were customer validation processes in place. Of greater concern was the remainder of the network where currently there was a lack of appropriate management information (MI). However, the number and nature of complaints and cancellations were being examined to develop and implement branch plans. To date, the Criminal Records Bureau checks carried out on agents had not been linked to log ins or passwords but enhancements were being made to secure a complete line of sight.

(e) JH reminded the Committee that travel and over 50s life were the only two of the Company's products sold over the counter in branch, all other products were sold through financial services specialists and could therefore be tracked.

POL00400101

(f) KG confirmed that on a weekly basis he received compliance and conduct statistics for the network and to date was not seeing anything in those statistics to indicate high levels of risk. He had been working closely with JH's team to review the customer mystery shopper videos. Training records were also checked and there was engagement with local area managers.

(g) KG continued that there was underway a planned reduction of 66 financial services specialists which would present a leadership challenge. The customer relationship manager initiative had been rolled out to around 25 per cent of branches but there was a concern about knowledge fade if products were being sold infrequently. There was a focus on the bottom performing 25 per cent of branches to establish whether special support could be given, for example, providing cards which could be read to the customer to protect against knowledge fade.

(h) SA asked, specific to the Company, which risks, and at what level, were anticipated to be running in the distribution network in a year's time and what actions were being taken to ensure at that point the risks were within appetite. He was especially interested in the travel and life products and the treatment of vulnerable customers. RC stated that until certain pieces of work, such as examining the statistics on distribution, had been concluded it was difficult to assess residual risk and to decide appropriate levels of investment to mitigate that risk.

(i) The Committee discussed the travel product and noted KG's view that it was a good, high quality product. However, despite this quality, travel presented a particular risk as 45 per cent of branch sales of the product were made outside the top 700 branches, although the branch Horizon system did provide a number of checks and balances. The Committee was informed of a recent example of a travel product form being completed incorrectly in branch resulting in the Company becoming liable for a financial claim. Despite these challenges, KG strongly believed that the product should continue to be sold across the network and noted that the greater use of technology was minimising certain risks.

(j) KG continued that he was comfortable that the right MI and first line controls were in place for the biggest branches with the greatest sales volumes but implementing consistency of MI across the network was a challenge. He did not believe there was a risk for the life product. JH and his team had been engaging with senior management over culture, MI and training and the resulting action plan was thematic, with a concentration on culture and approach, as well as containing specific actions. The Chairman confirmed that it was not necessary for the Committee to see the detail of the plan if GH and SH had seen it and were comfortable. However, the Committee agreed that a prioritised action plan would be submitted to the July 2016 meeting of the Board, which would anticipate that the actions would address, over the course of 2016, the risk presented by the AR's activity and the timetable to 2017 for Post Office to address the distribution risk

ACTION: JH/ SH

(k) The Committee also requested that a consolidated picture setting out the first, second and third lines of defence be submitted to its next meeting in September 2016. This should include a third line review of branch sales by 2017.

ACTION: JH/ SH

POL00400101

(l) The Committee further agreed that a deep dive would be undertaken with the Committee at its meeting in November 2016, which KG and JH would be asked to attend. This deep dive would include a more developed action plan with clarity over the key actions to take collectively, prioritised according to the risk, identifying what needed to be done, by when, how and what the impact and residual risks would be. The Committee noted the importance of agreeing the appropriate level of mitigated risk, in a timely manner and, as the regulated Principal, the Company required an holistic picture, identifying those risks which it was unable to directly address and which would need to be accepted.

ACTION: JH/ SH

(m) RC added that it was hoped that the risk acceptance process would be ready for June 2016, with a breakdown by channel and sales. SA asked for practical examples around branch distribution to be used at the Board risk workshop on 14 June 2016.

ACTION: SH

(n) The Committee was encouraged by the progress in Post Office's management of its oversight of the regulated activity in the branches. The Committee thanked KG and JH for their attendance and looked forward to their provision of a further update in November 2016.

(o) KG and JH left the meeting.

(p) SA noted the general progress outlined by KG and JH in their update and asked for NK's and JM's views on the broader challenges across Post Office Group. NK reported that there had been a definite change in the last few months with a realisation in Post Office, particularly in KG's area, that it was essential to get the oversight of regulated activities right. This was a cultural change and while the issue had yet to be satisfactorily addressed, it had been recognised and prioritised. KG wanted to sell an appropriate range of good products and did not want to lose those products due to regulatory failures resulting from insufficient oversight and he had acknowledged the challenging work ahead to address this.

(q) JM added that there had been a realisation of the type of work required and that it needed to be proportionate and effective. The Post Office Board had a conservative risk appetite, which it was due to review in September 2016, 18 months on from its previous discussion in January 2015. The Post Office Board needed to consider the consequences of its risk appetite position and how to implement control frameworks to meet the risk appetite. A series of steps would be needed and there would be a level of residual risk.

(r) The Committee debated, following KG's presentation, whether the rating of the AR oversight risk should be reviewed. The Committee agreed with SH's view that the AR risk continue to be viewed at the same level until the detailed action plan, with an implementation timetable to address the issues in the agency network, was received and accepted by the Company's Committee or its Board. NK added that JH and KG were developing better communication regarding the provision of MI, the importance of which was being realised, to ensure it was cascaded appropriately to area managers.

POL00400101

PARC 16/22 **RISK MANAGEMENT AND COMPLIANCE**

(a) SH introduced her paper on risk management and compliance which provided an update on the risk framework and second line compliance activity in the period, including conduct risk management information and the identification of top risks.

(b) SH commented that increased oversight from insurers and underwriters was expected, due to the FCA's thematic review on appointed representatives (AR). It was likely the FCA would review how Principals oversee their ARs. The Committee noted that this was also a priority for the Company.

(c) Associated with the oversight issue was the risk of mis-selling in branch which had been raised recently concerning the travel product and referred to by KG in his update earlier on the agenda. SA referenced the example as set out in paragraph 7a of the paper. He commented that complaints handling needed further consideration and it would be important to obtain appropriate management information from suppliers from which the required information could be extracted to identify specific risks and to inform the decision over whether the risk should be accepted or the business model revised.

(d) RC explained that from a conduct perspective it was challenging to secure complete visibility along the value chain. For example, it was difficult for the Company to present as customer centric if there was no influence over the claims data and how the process was handled. The team was pushing BGL to obtain more information but this process had proved to be difficult and slow, also the model was restricted with the contractual relationship being with BGL rather than direct with the Company.

(e) The Chairman asked if the operational problems with sales of the travel product were likely to damage the reputation of the Company such that there would be a reduction in opportunities to meet the Company's targets once the new platform was in place. SH confirmed that a travel workshop had been held in the previous week which had provided comfort that actions were being addressed through, for example, the completion of Project Zeus and the review of policy documents.

(f) RC confirmed that the risk assessment of the strategy was on track for completion in time for the meeting of the Board on 17 May 2016.

(g) RC commented on commercial risk performance and the need to consider what actions had been taken historically, for example, widening margins. There was a need for the Company to consider how to respond to commercial risks and the scale of residual risk remaining as a result of selling the travel product over the counter.

(h) It was agreed that an update would be provided on the actions taken to address the risks identified, particularly from the customers' experience and especially for Travel.

ACTION: SH

Key Company Policies Framework

(i) SH introduced the proposed key company policies framework and explained that a two tier approach had been taken to approvals with

POL00400101

policies split between non-executive and executive level.

(j) It was agreed that those policies to be approved at a non-executive level would be divided between those to be approved by the Board (policies covering business operation and strategy) and those to be approved by the Committee (policies covering risk management and compliance matters). The required amendments would be made to the policies framework, matters reserved to the Board and any other required documentation.

ACTION: SH/ VM

(k) The Committee noted that the paper set out the proposed communications and implementation plan for the policies. For some policies it would be appropriate to work with Post Office, for example, around vetting.

(l) The Committee discussed the required policies for data management and the importance of the developments in data protection. It was agreed that some aspects of data management were covered in the Information Security Assurance Group policies but others would fall under records retention. SH was asked to clarify the difference between organisational record keeping and the management of customer data in the policies.

ACTION: SH

(m) The Committee approved the key company policies framework, subject to the requested change as set out in paragraphs 16/22(k) and 16/22(m), and asked that the executive roll out the Company's policies over the next quarter.

ACTION: SH

Incident Reporting

(n) The Chairman stated that in future there needed to be a better balance between the reporting of the customer impact as opposed to the commercial impact of incidents, currently there was too much concentration on commercial implications.

ACTION: SH

(o) The Committee noted the risk management and compliance papers and updates.

PARC 16/23 **UPDATE ON COMPLIANCE MONITORING**

(a) SH updated the Committee on progress against the compliance monitoring plan, which the Committee had approved at its previous meeting in March 2016.

(b) The Committee discussed whether or not the appointed representative risk, currently red, should be downgraded in severity following the presentation earlier in the meeting. It was agreed that while it was not yet appropriate to change the RAG status, the risk should be re-examined in light of the earlier discussions and the Appointed Representative action plan, to develop an understanding of the actions needed to reduce to amber. The dashboard should also be revised to clarify the difference between strategy design and strategy delivery.

ACTION: SH

ACTION: SH

(c) The Committee noted the progress against the compliance monitoring plan.

POL00400101

PARC 16/24 **OTHER ASSURANCE WORK**

(a) **Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) Framework Report – Findings and Proposed Responses**
The Committee noted that an update on vulnerable customers and AML/CTF would be provided to the Board at its meeting in July 2016.

(b) **Information Security Assurance Group (ISAG)**
The Committee noted the paper on the work of the ISAG and requested that an annual update from the ISAG be scheduled for each May meeting of the Committee.

ACTION: VM

(c) The Committee noted the update provided.

PARC 16/25 **EXTERNAL AUDIT (period ending 27 March 2016)**

(a) CS provided a verbal update on the progress of the external audit for the 16 month period ending 27 March 2016 which was underway with Ernst & Young LLP (EY) and nearly complete. No issues of substance had been raised at the time of the Committee. Due to the timing of the audit process, the EY audit partner was scheduled to attend the meeting of the Board on 17 May 2016 to provide a full update, at which point the Board would also be asked to approve the accounts.

(b) CS explained that resolution was outstanding on the treatment and presentation of certain intangible assets, specifically the IT assets in construction and the goodwill related to the purchase of the Post Office Insurance business. He explained that at a Group level all intangible assets were impaired to zero immediately, however, this was not a usual approach for a profit making business. The Company's proposed approach was for the IT assets to be amortised over a number of years and for an annual impairment to be run on the goodwill. This proposed approach had been discussed with the CFO of Post Office who was in agreement but EY disagreed as the audit partner believed that there should be consistency across the Group in treatment of assets. Further clarification of this issue and any other points raised by EY, would be provided to the Board on 17 May 2016.

(c) The Committee noted the verbal update provided.

PARC 16/26 **FCA END OF YEAR RETAIL MEDIATION ACTIVITIES RETURN**

(a) CS introduced the paper which set out the information to be used for submission of the FCA end of year Retail Mediation Activities Return (RMAR). He explained that the source of data for the financial returns was the unaudited period 12 data which had been reviewed by the Executive Committee in April 2016.

(b) The Chairman asked whether anything in the data was inconsistent with the interim return. CS confirmed that he had worked with SH on the provision of the risk related information, that the data had been compared to the interim data and that he believed no concerns would be raised over the data provided.

POL00400101

(c) The Committee reviewed the information to be used for submission of the FCA end of year RMAR and recommended to the Board that it approve the use of this information and authorise submission to the FCA.

PARC 16/27 ANNUAL REPORT AND ACCOUNTS

(a) CS provided a verbal update on the progress of the annual report and accounts for the 16 month period ending 27 March 2016.

(b) The Committee noted the update and that, due to Group reporting timing constraints, the annual report and accounts would be considered in detail at the meeting of the Board on 17 May 2016 when the auditors would be in attendance.

PARC 16/28 BOARD RISK WORKSHOP – JUNE 2016

(a) It was agreed that the Board risk workshop, to be held on 14 June 2016, would focus on reviewing the Company's top risks and the relevant risk appetites, following the anticipated approval of the Company strategy at the meeting of the Board on 17 May 2016 and the required engagement with the Post Office Board.

PARC 16/29 REPORT TO THE BOARD AND TO THE POST OFFICE AUDIT, RISK AND COMPLIANCE COMMITTEE

(a) It was agreed that the Chairman's report from the meeting to the Board and to the Post Office Audit, Risk and Compliance Committee would include: the presentation from KG and JH on the oversight of Post Office as Appointed Representative of the Company; the internal audit findings on the follow up of the Hawk readiness review (undertaken by PwC); approval of the company policies framework; and review of the information to be used for submission of the FCA end of year Retail Mediation Activities Return.

PARC 16/30 ANY OTHER BUSINESS

(a) There being no further business the Chairman declared the meeting closed at 4.05pm.

PARC 16/31 DATE OF NEXT MEETING

(a) The Committee noted that its next meeting would be held on Tuesday 13 September 2016 at 2.00pm.

..... **Amanda Bowe**
Chairman

.....13 September 2016
Date

POL00400101

Report from POMS as Principal

Author: Susie Hayward, POMS Head of Risk and Compliance Sponsor: Nick Kennett Meeting date: 28 September 2016

Executive Summary

Context

Post Office Management Services (POMS) was established as a wholly owned subsidiary and Insurance Intermediary for the sale and administration of Insurance products. POMS is regulated by the Financial Conduct Authority (FCA). Post Office Limited (POL) is the Appointed Representative (AR) of POMS to provide sales and distribution of insurance products.

As the AR, through POMS as its "Principal", POL is required to comply with FCA regulation, however, regulatory responsibility sits with POMS. While gaps have been identified in the compliance controls across the branch network, extensive work has been carried out to improve the position; however there is still more work to be done.

POMS has identified the risks presented by the branch network as its top risk; it is currently red rated and is outside POMS' appetite for regulatory risk.

This paper was requested by the POL ARC to provide clarification of the roles and responsibilities of each party together with POMS' expectations of standards of conduct and performance of POL. It identifies where additional focus is required and the implications of non-compliance.

Questions addressed in this report

1. How and why is POL an AR of POMS?
2. Who is responsible for compliance with regulation?
3. What were the findings of the recent FCA Thematic Review?
4. What is the current status and future actions?

Conclusion

1. As an AR, POL is exempt from authorisation under the Financial Services & Markets Act but is required to follow the regulatory requirements for activities as advised by its Principal; in this case POMS. POMS has set its expectations of how regulated activity should be managed through the Regulatory Governance Manual.
2. POL is responsible for conduct risk management in all branches where regulated activity takes place, including sales and introductions by agency counter staff of insurance products.
3. The recent FCA Thematic Review of the general insurance industry and enforcement actions highlight the need to ensure robust systems and controls are in place and that these can be evidenced.

POL00400101

4. While work has been carried out to improve standards of conduct risk management across the network, more work is needed, requiring time and resource commitment.
5. If POL is unable to make the necessary changes, POMS will need to consider withdrawing products from sale, impacting customer benefit and POMS/POL income.

Input Sought

Paper for information and discussion

POL00400101

The Report

Background

1. The acquisition of the insurance business from Bank of Ireland (BoI) under "Project Hawk" completed on 1st October 2015. As part of the project POMS was established as a wholly owned subsidiary and an Insurance Intermediary. POMS is authorised and regulated by the FCA to provide sales and intermediary services of General and Life Insurance products.

2. In preparation for Project Hawk, legal and regulatory advice was sought regarding the relationship with POL as a distributor of the Insurance products. Due to POL's unique size and structure careful consideration was given to its appointment as an Appointed Representative (AR) of POMS. As an AR, POL is required to comply with FCA regulation, however, regulatory responsibility and relations with the regulator sit with POMS as Principal.

3. Each Post Office agency branch is a separate business entity with its own ownership and management and is responsible for the conduct of its business. POL's agency contracts ensure that POL remains the AR for all branches including its agents. POL must ensure that its agents and their staff meet all compliance requirements.

Regulatory Responsibility

4. A business operating as either a Principal or AR must comply with the FCA Handbook, Principles and Policies. For an AR, compliance is required wherever it is conducting regulated activity (for example selling insurance).

5. As an AR, POL has a responsibility to its Principal to ensure the business is managed to achieve good conduct risk outcomes (see slide deck); this applies to all branches where regulated activities occur. POMS, as Principal, must ensure that its AR is fit and proper to deal with customers on its behalf and to ensure that customers dealing with the AR are afforded the same level of protection as if they had dealt with the principal itself. This is currently set out in the Regulatory Guidance Manual in the POL/POMS Distribution Agreement.

6. The Principal is responsible for anything done (or omitted) by the AR in carrying on the business for which the Principal has accepted responsibility. POMS' role is to ensure it has oversight, can evidence that this is being achieved and can take action where it is not. The Principal is responsible for ensuring any issues are identified and any customers who may have suffered detriment are afforded appropriate redress.

7. Customer detriment and mis-selling are not the only measures by which firms are measured for compliance. Lack of systems and controls, senior management culture and attitude, lack of supervision, ability to evidence and govern compliance have all seen enforcement by the regulator, irrespective of whether customers were directly impacted. Examples of recent enforcement action taken are included in the slide deck. Suspicion of bad practise or lack of control could result in a higher level of supervision and review by the Regulator. Sanction or enforcement not only has a financial impact on firms and individuals but can have significant reputational and brand damage.

POL00400101

FCA Thematic Review

8. In July 2016 the FCA published the findings of its Thematic Review "Principals and their appointed representatives in the General Insurance sector". The Review uncovered widespread shortcomings with many principals not having appropriate control frameworks for monitoring their ARs, nor enforcing compliance.

9. The FCA found examples of potential mis-selling and customer detriment and has taken early intervention against five firms.

10. Although neither POL nor POMS was assessed as part of the review, many of the examples cited relate to multi-location, non-specialist distribution models.

11. The most serious findings of the review were that many principals did not understand their obligations and that there was little or no oversight by the principal or AR; this is not the case for POL and POMS.

12. The high level findings from the Review include:

    a. Business model and risk management – A majority of firms lacked effective risk frameworks with AR alignment to and impact on wider business model not considered.

    b. Governance and oversight before appointment – Solvency and suitability of the AR. A majority of firms did not have an adequate understanding and resources to oversee and control their ARs.

    c. Governance and oversight, contracting – The review identified shortcomings in contracts relating to scope of activities, which included issues such as Multiple Principal arrangements, categorising of ARs, implementing Approved Persons regime and client money rules.

    d. Governance and oversight, control and monitoring – The review identified shortcomings in understanding and oversight of regulated activities of ARs, with many risks not identified or addressed. Firms lacked effective monitoring activity and control.

    e. Consumer Outcomes – The review identified potential mis-selling with customers buying products they did not need, not eligible for or without adequate information.

13. The results of the findings are so widespread the FCA may undertake further reviews or changes to the AR regime which could impact the POMS/POL structure.

POMS/POL Current status and future actions

14. POMS, working with the POL FS Risk and Network teams (who also work with POL's other Principal; BoI), has assessed POL's capabilities and compliance by the branch network of its obligations. While many gaps have been identified in the standards of conduct risk management, extensive work has been carried out to improve the position. In particular the regulatory and compliance performance of Financial and Mortgage Specialists has improved considerably. Agency branches have performed less well raising concerns at recent POMS Board meetings.

15. Below are some of the gaps identified and key areas of concern:

    a. Sales Model/Business Targets
    The concern is that the branch sales model could cause the wrong conduct behaviours (e.g. a product push culture) by counter colleagues, potentially

POL00400101

resulting in customer detriment and that POL might not have the right oversight to identify failings or adequately remediate.

POMS needs to ensure that where weaknesses in controls, incidents and trends are identified, appropriate and timely action is taken and that outcomes can be evidenced.

b. Culture and Training
The concern is to ensure that the customer is at the heart of POL's culture and incentives and targets are designed to deliver fair treatment for customers.

POL has identified incidents in branch where colleagues have felt "pressured" to perform sales or achieve product targets which have resulted in inappropriate behaviours (although no evidence of customer detriment); POL has taken action where this has been identified to prevent recurrence and this is being monitored.

POMS is also concerned that there is insufficient or timely management information to help identify conduct performance in branch and understand areas of improvement or concern. POMS and POL are working on improving the information available.

c. Performance Management
Management of sales performance, including post-sales measures (complaints and cancellations) should form the basis of regular reviews by management and actions taken where necessary. A gap has been identified in relation to the management of branch related complaints and taking action and improvements as required. POMS is working to develop effective complaints MI that can be shared with POL so that it can take action.

d. Monitoring
Quality Assurance is not applied to all products or all branch types i.e. there is currently no mystery shopping for counter colleagues for Travel Insurance. Ensuring counter colleagues receive supervision and oversight for the sale of regulated products will identify gaps in controls and development needs. POMS, BoI and POL have met recently to reinstate mystery shopping of counter staff across the network using MI provided by POMS and BoI.

e. People
POL needs to ensure that its customer facing staff (and those who manage them) are appropriately vetted, trained and monitored. Whilst this is done effectively in Crown branches and for CRMs, POL is unable to provide assurance to POMS that its agents and their staff are meeting these requirements. This is particularly important for POMS as it uses agency branches for counter sales of Over 50s Life and Travel Insurance. While a risk-based approach can be taken to oversight, staff vetting and training is mandatory for all staff conducting regulated activities.

f. Risk Management
A gap has been identified in POL's second line of defence compliance capacity to advise and oversee the agency network first line. As a result, POL cannot provide assurance to POMS (or to itself) that the agency network meets its regulation obligations.

POL00400101

g. Management Information
POMS is concerned that there is limited and inconsistent information to measure and monitor the performance of key conduct risk indicators.

16. In response to these issues POL has developed a wide-reaching Network Conduct Risk Action Plan of assurance and supervision for counter staff and products. This should provide evidence of a risk-based approach to monitoring, commensurate with the level of activity and size and scale of POL's network.

17. While POL is tabling a more detailed analysis to the meeting, the core actions relating to POMS' requirements include:

    a. The "enhanced user management" project to give all Horizon users a unique identifier; this will provide evidence of activity and training records at an individual agency staff level. POMS needs this to be delivered in January 2017 to avoid having to suspend network sales of Travel Insurance and Over 50s Life outside of FS/MS and CRM branches.

    b. POL FS Risk and the Network teams are developing more robust processes to ensure corrective actions are carried out, including identifying training needs and suspending staff licences.

    c. POL is rolling out "Success Factors" training to all counter staff that will include conduct, regulatory and product knowledge tests. The system should provide regular reports that counter colleagues have completed mandatory training. POMS is seeking commitment from POL that this will be delivered in 2016/17.

    d. POMS is withdrawing counter sales for Over 50s life in c9,000 branches that have not sold the product and only allow branches with Financial Specialists or CRMs (this will amount to c1,000 branches). This project is being run by POMS to tie in with the introduction of a new life provider in January 2017.

18. The activities that POL is undertaking should enable POMS to have confidence that POL will meet its obligations as the AR.

19. If POL is unable to make the necessary changes, POMS will need to consider withdrawing products from sale, impacting customer benefits and POMS/POL income.

POL00400101

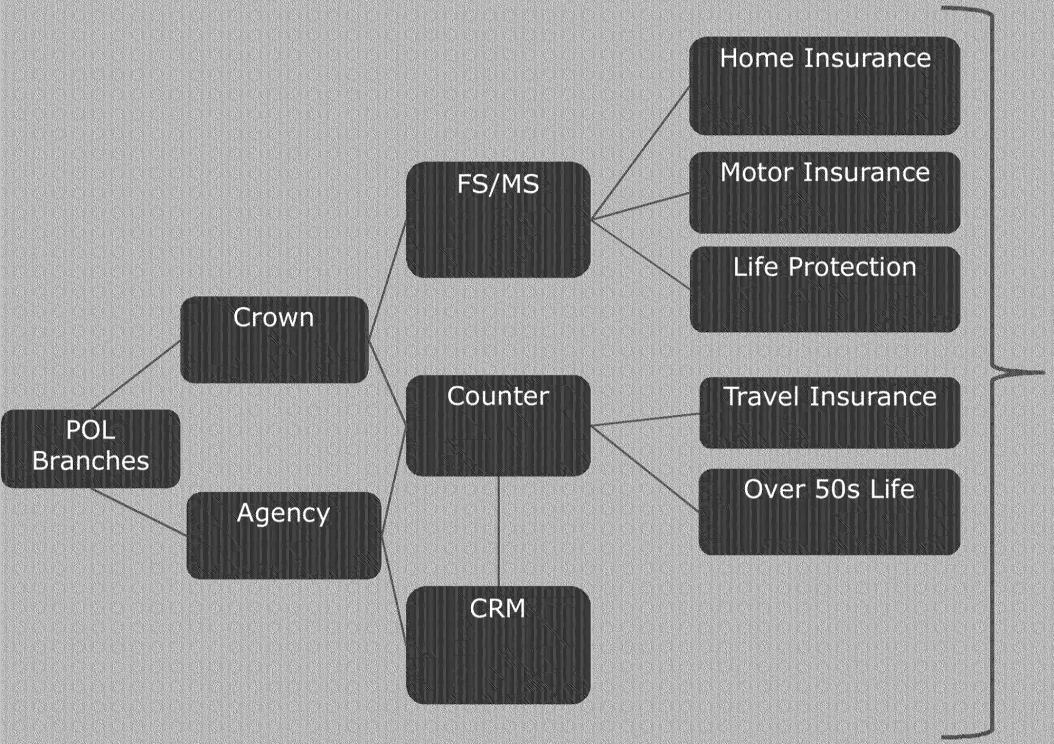
POMS as Principal for Insurance

POL ARC

September 2016

POL00400101

Regulated Insurance Activity



Conduct Risk Outcomes – applicable to all branches

- All staff are suitably qualified and trained
- All staff are subject to ongoing performance and competence reviews
- Sales processes and procedures are effective and reviewed
- Incentives are performance rather than sales driven
- Sales performance and product knowledge is tested through quality assurance
- Financial Promotions and support documents are up to date and accurate
- Complaints are handled and root cause analysed and actioned
- Risk based assurance is conducted across the network
- Action planning to ensure processes and performance subject to continuous improvement
- Management information, including post sales, measures conduct risk and is reviewed by management
- Governance includes reporting and escalation
- Incidents and breaches are recorded, managed and lessons learnt
- Operational Risks are identified and managed
- Treating customers fairly is at the heart of the culture of the organisation

POL00400101

Regulatory Compliance Role and Responsibilities

Role

PRINCIPAL

POST OFFICE MANAGEMENT SERVICES LIMITED

Distribution Agreement/Regulatory Governance Manual

APPOINTED REPRESENTATIVE

POST OFFICE LIMITED

Responsibilities

OVERSIGHT AND ASSURANCE

- Assurance Reviews
- Supervision and sign off
- Oversight of branch performance
- Challenge
- Support and Advice

MANAGEMENT AND PERFORMANCE

- Compliant Culture
- Conduct Risk Management
- Training and Competence
- Quality Assurance
- Key Risk Indicators
- Performance Management
- Incident Management
- Management and Governance

Measures

- Branch Reviews
- Thematic Reviews
- Sign off Processes
- Review of MI reporting
- POL/POMS Governance forum

- Training programs and reporting tools
- Management Information, incl post sales
- Incidents & Breaches processes
- Action and Improvements plans
- Conduct Risk Management Committee
- Risk based QA program
- Customer based incentives schemes
- Sanction and Discipline

POL00400101

POMS Conduct Risk Outcomes

STRATEGY	CULTURE AND BEHAVIOUR	CUSTOMER	PRODUCT	GOVERNANCE AND OVERSIGHT
Our business strategy reflects our customer values and approach to product design, distribution and service.	Treating Customers Fairly is central to the corporate culture of the firm whenever decisions need to be made about conduct and what is acceptable.	We are growing our business based upon the needs of our customers	We design and price our products to deliver value for our customers and to perform as expected	Our board regularly discuss Conduct Risk at its meetings and is able to evidence those discussions.
Our approach to business planning encompasses long term decision making and sustainable growth.	Our management support the board in establishing a corporate culture which pays due regard to the interests of customers	We organise ourselves in an appropriate and controlled manner with customer satisfaction central to our ethos	Our Product Committee includes individuals to provide customer challenge, review impact on customers and document the discussions and decisions.	Our board set appropriate Conduct Risk objectives for directors and staff and ensure that these are assessed.
Our Customer Strategy drives product design, decision making and marketing.	Our staff understand and support the customer centric culture led by the Board	We train our staff to provide informative customer service and post sales experience	We assess the product risk of each product and change and decide whether and how to sell that product depending on its product risk	We effectively manage any conflict of interest which might lead to the unfair treatment of Customers.
We take a forward looking approach to strategy and business planning including conduct risk objectives.	Treating Customers Fairly is central to the behaviour of our staff in product, sales and post sales roles	We market and sell our products through all our channels in the most appropriate way to ensure customers understanding and satisfaction	We assess the Customer Risk of a Product having careful regard to the attitudes and behaviours of the Customer to whom it is intended the Product will be sold.	Our whistleblowing policy includes disclosure for the unfair treatment of Customers.
We manage a robust framework of Risk Management including the assessment, control and monitoring of conduct risk	We incentivise our staff on a balanced scorecard including customer service and compliance with the firms policies and principals	We strive to ensure that customers receive a high quality service when they deal with us or where things go wrong	We continually monitor and assess the product risk of products during their respective lifecycle	We provide oversight and governance forum for third party product providers, distributors and underwriters.

POL00400101

Three Lines of Defence

PRINCIPAL

Post Office Management Services Limited

1st Line

Managing Director – Rob Clarkson

Head of Commercial – Russ Tavener

Head of Travel – Paul Jones

Head of General Insurance – Gerry Barrett

Head of Protection – Ryan Griffin

2nd Line

Head of Risk & Compliance – Susie Hayward

APPOINTED REPRESENTATIVE

Post Office Limited

1st Line

Network Director – Kevin Gilliland

Sales Director – Owen Woodley

Head of FS Risk – Jonathan Hill

2nd Line

3rd Line

Head of Internal Audit – Mike Morley-Fletcher

POL00400101

Recent FCA enforcement

Towergate July 2016 £2.362m	For lack of segregation and management of client and insurer monies. Note, no actual loss and shortfall was rectified when discovered. The FCA's concerns were over governance, reporting, monitoring and competence of key individuals
WH Ireland Feb 2016 £1.2m	For infective systems and controls to protect against risks. Week detection controls, deficient compliance oversight, management information, risk management and poor governance. WHI did not have a formal way of identifying and recording what training had been given and to whom. No processes for managing conflicts of interest. Concerns over a *Risk* of market abuse occurring, no evidence of market abuse actually occurring.
Mr S Reches Feb 2016 £14.18m (fine and costs)	Mr R had links to entities providing insurance. Ineffective management of insurer monies led to cover failing, 2 insurers going into administration and the FCSC having to pay out over £9m. SR was not himself an approved person with the FCA but was considered instrumental and therefore liable. His company, Milburn Insurance was also fined £1.1m.
Swinton July 2013 £7.38m	Failing to provided sufficient information at point of sale, particularly in relation to add-ons. Week controls including monitoring too narrow, MI inadequate to identify poor compliance, business strategy of maximising sales at the cost of customers including complaints and incentives. Also ordered to repay £11m to customers mis-sold and some of the Senior individuals also fined and banned. At the time Swintons was Britain's largest broker with a wide distribution of Face to face sales.
5 unidentified firms	Following the Thematic Review into the relationship of Principals and AR's in general insurance, enforcement action has been taken against 5 insurance intermediaries.

POL00400101

Bank of Ireland UK & Post Office Partnership

BOI conduct & regulatory risk management

September 2016

Classification: Red

POL00400101

Contents

POL00400101

Executive summary

- Significant conduct issues and breaches are rare, with no indication of systemic issues in the network
- Day-to-day risk management and oversight of conduct and regulatory risks is effective
- Where isolated KRI exceptions have been identified, actions have been taken to address these
- BOI and POL remain aligned on the conduct agenda and the relationship between the parties is good
- However, we must not be complacent, as there remain a number of significant challenges and areas requiring continued focus:
  - fully embedding the conduct agenda at all levels of the organisation and in all parts of the network
  - ensuring that steps continue to be taken 'at pace' to develop more robust controls and mitigate risks in the wider network
  - significantly improving the robustness of Mortgage Adviser and FSAM 'fitness and propriety' checks
  - providing Bank's senior managers with the necessary assurance that Post Office provides an effective first-line-of-defence
  - ensuring that mortgage advisers maintain competence in periods where activity levels are low

POL00400101

Three lines of defence – branch distribution

Bank of Ireland UK

1st **Gordon Gourlay** (Managing Director of Post Office Businesses)

Post Office

1st **Kevin Gilliland** (Network and Sales Director)
- Owen Woodley (Sales Director)

Nick Kennett (Director - Financial Services)
- Jonathan Hill (Head of FS Risk and Strategy)

Martin George (Commercial Director)
- Glynn Williams (Head of Marketing)

2nd **Jane MacLeod** (GC & Corporate Services Director)
- Mike Morley Fletcher (Head of Risk & Assurance)
- John M Scott (Head of Security & Financial Crime)

3rd **Jane MacLeod** (GC & Corporate Services Director)
- Garry Hooton (Head of Post Office Internal Audit)

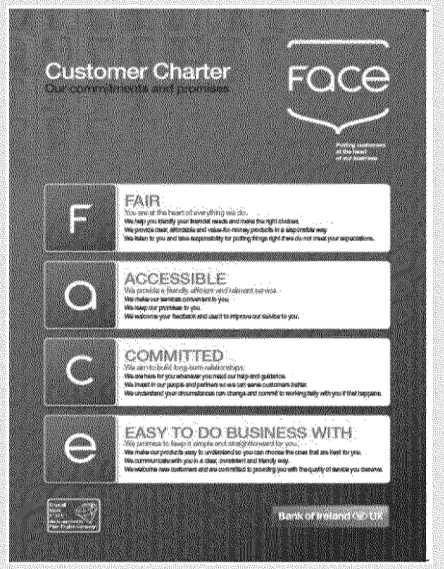
2nd **Richard Holden** (Head of Conduct & Regulatory Risk Management)
- Deb Codack (Head of Regulatory Operations and Assurance)
- Alec Hughes (Head of POJV Compliance)

3rd **Steve Sanders** (Group Internal Audit Managing Partner)

POL00400101

BOI/PO partnership – conduct risk management model

FACE Customer Charter



Our FACE Customer Charter captures the key commitments and promises the Bank and Post Office make to our customers. The Charter underpins our organisational conduct risk arrangements.

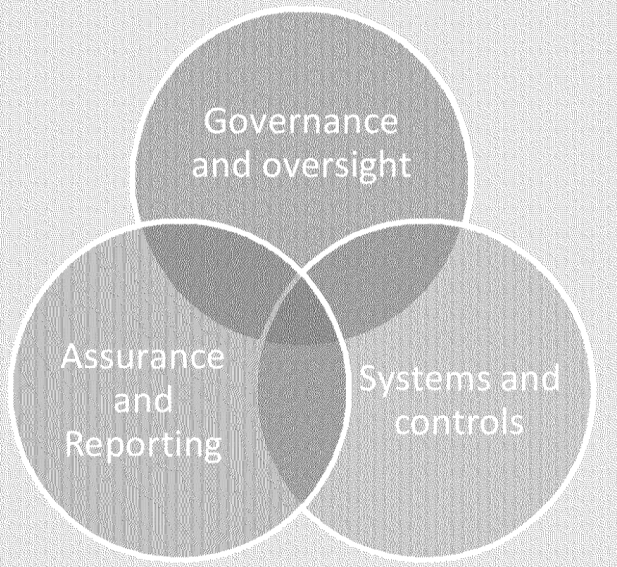
As the regulated entity, BOI is accountable to the FCA for the non-insurance related distribution activities of POL, which acts as its Appointed Representative.

Thus, BOI has established a high level conduct and regulatory risk management model, designed to ensure Post Office acts in accordance with the Bank's regulatory obligations.

The risk management model is underpinned by our FACE Customer Charter and our customer promises and commitments.

The model consists of three core elements:

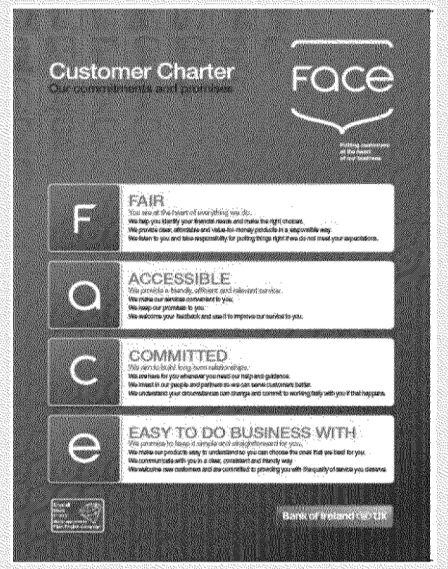
- Governance and oversight
- Systems and controls
- Assurance and reporting



POL00400101

Governance and oversight

FACE Customer Charter



Our governance and oversight arrangements are designed to ensure that we meet the promises and commitments we make to our customers and that we meet our overall conduct obligations.

Post Office Partnership Board

The Partnership Board is the Senior Joint Management Committee, where BOI and POL oversee all aspects of the joint venture, including conduct risk.

Customer & Conduct Risk Committee

The Customer and Conduct Risk Committee (C&CRC) is a joint BOI(UK)/POL committee, responsible for the operational oversight of Post Office financial services distribution.

The C&CRC acts as the escalation and decision making body for regulatory and conduct issues and receives detailed regulatory and conduct risk management information and key risk indicators.

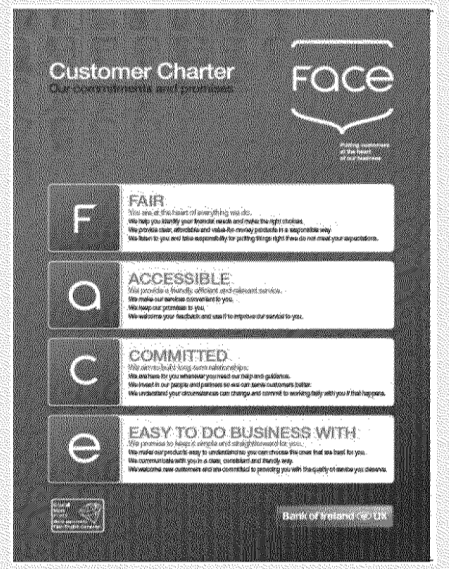
Sales Oversight Compliance Forum

The joint BOI(UK)/POL Sales Oversight and Compliance Forum (SOCF) is responsible for considering operational regulatory and conduct risk issues in relation to Post Office's distribution of financial services products.

POL00400101

Systems and controls

FACE Customer Charter



The Charter underpins our conduct obligations and the systems, controls, policies and procedures we put in place to ensure that customers are at the heart of everything we do.

Conduct and regulatory standards - The Bank provides Post Office with clearly defined regulatory and conduct risk standards and policies. In addition, all marketing, internal communications, sales support and training material is approved by Risk.

Conduct toolkit - Our conduct toolkit ensures that the principles of good conduct and our commitment to placing customers at the heart of our business are met in our day-to-day activities.

Risk assessment - Customer detriment risk assessments are used to predict the customer detriment potential of in-branch distribution. Robust action is taken to mitigate or eliminate any residual risks.

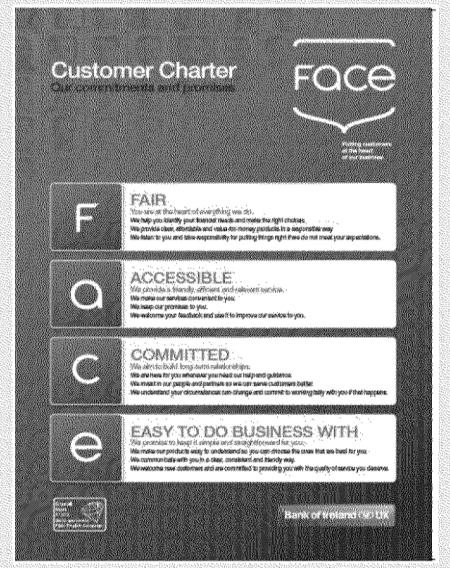
Staff awareness and capability - Post Office carries out regular conduct and regulatory risk training and testing with their key sales and sales-support staff. Training and competence schemes and supervision are in place to support those involved directly in financial services sales.

Staff incentivisation - Staff incentive schemes are designed to reward behaviours that support our conduct obligations, and include qualitative, as well as quantitative, targets and measures.

POL00400101

Assurance and reporting

FACE Customer Charter



Our FACE Customer Charter underpins our conduct assurance and reporting, and provides a framework for our risk assurance and reporting, and our root-cause-analysis and action planning.

Key Risk Indicators - KRIs are used to monitor conduct performance in relation to Post Office branch distribution. These include metrics relating to mystery shopping, mortgage advice, customer complaints, customer insight, and staff knowledge and awareness.

Risk assurance - Risk assurance reviews are used extensively to monitor the performance and capability of branches and branch staff and to validate the effectiveness of conduct controls. The use of video mystery shopping, branch reviews and staff testing is key to this.

Customer insight - Customer feedback, including complaints and compliance surveys, is reviewed on an ongoing basis. This includes monthly reporting on the levels, types and root causes of complaints , which is supported by 'deep-dive' thematic or trend-based reviews.

Root- cause-analysis – RCA is used to identify the underlying causes of, and trends in, conduct related issues and breaches.

Action planning - Action plans are used to ensure that issues identified through root-cause-analysis are addressed and to ensure that the effectiveness of remedial action taken is robustly validated.

POL00400101

BOI conduct & regulatory risk – KRI performance

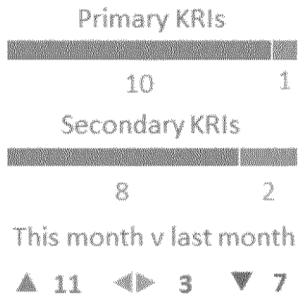
We use 21 Key Risk Indicators (KRIs) to measure Post Office distribution conduct risk.

The KRIs are linked to the FACE Customer Charter, our customer promises and commitments and to our key risks. We set targets and tolerances against each KRI, which are aligned to our overall Risk Appetite Statement.

Each month, we measure POL's performance against each KRI target and rate it either green, amber or red. We also use the KRIs to provide an overall risk rating. Where any of the KRIs raise concerns, further root-cause-analysis is undertaken to investigate this and remedial action is taken where necessary.

KRI performance and the actions being taken as a result are captured on the monthly Post Office Money Branch Distribution Conduct Risk Dashboard – see annex A.

Current performance



In August 2016, 18 of our indicators were rated green and 3 were rated amber. None were rated red.

In comparison, in June no indicators were rated red and in May only one was rated red.

This is consistent with performance over the last 6 months.

While we identify isolated exceptions where our KRI targets are not met, these are not indicative of systemic or material underlying issues.

POL00400101

BOI conduct & regulatory risk – KRI performance

In August 2016, all our KRIs were within tolerance. 18 of our indicators were rated green and 3 were rated amber. None were rated red.

August KRI risk rating (previous five month's ratings also shown):

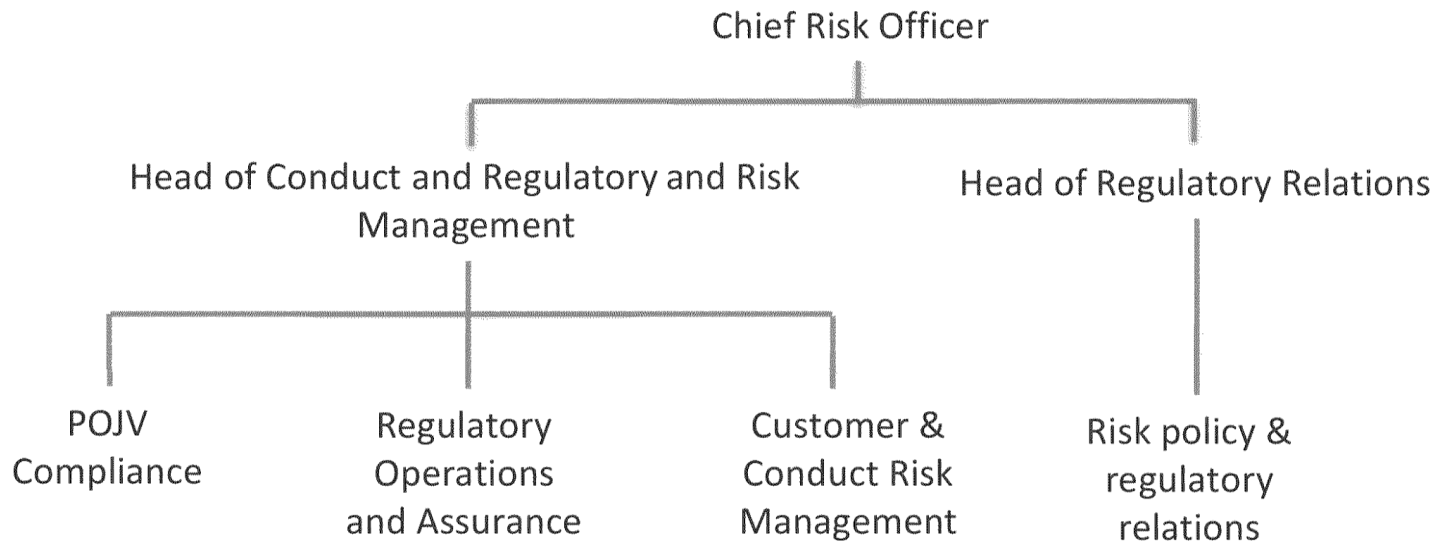
- Red rated mystery shops (10.8%)
- Black rated mystery shops (0)
- FS/MS with >1 red/black rated shop (0.9%)
- A/B rated QAT mortgage case checks (93%)
- D rated QAT mortgage case checks (1.1%)
- MS meeting QAT benchmark (90.7%)
- Complaints per 1,000 sales (1.14)
- Upheld complaints v sales growth (19%)
- Growth in upheld complaints (6%)
- Conduct customer survey results (96%)
- NPS customer survey results (98%)

- BOI branch product knowledge reviews (100%)
- BOI branch regulatory knowledge reviews (100%)
- POL MS/FS knowledge assessments (99%)
- BOI branch financial promotions reviews (97%)
- Material financial promotions breaches (0)
- Savings cancellations (0.76%)
- Credit card usage (29%)
- FS/MS signed off as competent (87%)
- Supervisor spans of control (96%)
- BOI FSAM review results (96%)

POL00400101

BOI conduct and regulatory risk function

BOI has a risk function, which is responsible for establishing high level regulatory and conduct risk policy, providing regulatory compliance related advice, guidance and support and deploying second-line-of-defence oversight, controls and risk assurance



POL00400101

BOI conduct and regulatory risk - responsibilities

POJV Compliance

- Defining and communicating regulatory and conduct risk standards and controls
- Overseeing the deployment of branch regulatory and conduct risk controls
- Providing regulatory and conduct risk advice, guidance, support and approval
- Overseeing the resolution of regulatory and conduct risk issues and KRI/other breaches
- Providing regulatory and conduct risk management information and reporting
- Managing regulatory and conduct risk relationships with POL

Risk policy and regulatory relations

- Identifying, communicating and supporting the business to address the impact of current and future regulatory risks and developments
- Ensuring regulatory developments are reflected in the appointed representative arrangements
- Managing relationships with regulatory bodies

Regulatory Operations and Assurance

- Validating the effectiveness of branch network regulatory and conduct risk controls through Risk Assurance monitoring and reporting
- Overseeing the resolution of regulatory and conduct risk issues and breaches
- Reviewing and approving Post Office Money Financial Promotions

Conduct and Regulatory Risk

- Providing internal conduct risk advice, guidance and support
- Producing and maintaining conduct risk toolkit
- Reviewing and challenging monthly Conduct Risk Scorecards, risk assessments, root cause analysis and action planning
- Producing monthly Executive level conduct risk reporting pack
- Escalation of material conduct risk issues
- Identifying emerging conduct risk issues and providing early warning to Executive level management

POL00400101

Historic conduct and regulatory risk issues

Multiple growth bond sales

In 2011, Post Office reviewed a number of growth bond sales made by Financial Specialists, where customers had opened multiple bonds on the same day. The review considered whether customers had been advised to take this action, either to generate additional income for the Specialist or to by-pass anti-money laundering cash limits. As a result of the review, three Specialists and one Supervisor were subject to disciplinary proceedings and remuneration arrangements were amended.

Life insurance

In 2014, video mystery shopping identified that a number of Specialists had been by-passing important compliance controls during life insurance sales. This may have resulted in customers being left uninsured. As a result, all Specialists were de-accredited in this area and were subject to formal retraining and reassessment. Systems changes were also made to reduce the risk of reoccurrence.

Travel insurance

In 2014, following an investigation into a customer complaint, it was identified that a relatively small proportion of in-branch customers may have purchased excessive or insufficient travel insurance for their intended destination of travel. As a result, in-branch sales processes were enhanced and around 10,000 customers were offered a refund.

POL00400101

Current key conduct risks

- Customers receive **unsuitable mortgage advice** from in-branch Mortgage Specialists
- Customers **buy products which do not meet their needs**, as the result of Financial Specialists or other branch colleagues providing inaccurate or incomplete product information, or providing unauthorised advice
- Customers buy products which do not meet their needs, as the result of **financial promotions** material which is misleading, unclear, unfair or out-of-date, or which is otherwise non-compliant
- **Customers best interests are compromised** as the result of inadequate conduct controls or as the result of conduct or regulatory failures which are not corrected

POL00400101

Current key conduct risks and mitigation

Customers receive unsuitable mortgage advice from in-branch Mortgage Specialists

Mitigation:

- ✓ All Mortgage Specialists are subject to fitness and propriety checking
- ✓ All Mortgage Specialists are fully qualified and are subject to formal Training and Competence arrangements and supervisory oversight
- ✓ Detailed mortgage advice standards are published and maintained
- ✓ Mortgage advice files are subject to regular independent review by an Quality Assurance Team
- ✓ All Mortgage Specialists are subject to regular video mystery shopping reviews and other risk assurance activities
- ✓ KRIs are monitored on an ongoing basis to provide early warning of potential customer detriment
- ✓ A formal structured CPD programme is in place to maintain adviser competence

POL00400101

Current key conduct risks and mitigation

Customers buy products which do not meet their needs, as the result of Financial Specialists or other branch colleagues providing inaccurate or incomplete product information, or providing unauthorised advice

Mitigation:

- ✓ Sales processes are designed to ensure that customer information needs are met
- ✓ Branch sales activity is primarily focused on accredited crown Financial Specialists (FSs) and agency Customer Relationship Managers (CRMs)
- ✓ All sales activity is non-advised, with Financial Specialists engaging in assisted sales and all other activity being introductory-only
- ✓ FSs and CRMs are subject to Training and Competence arrangements and supervisory oversight
- ✓ Products are designed to be bought on a non-advised basis and to be low risk, simple and easy to understand
- ✓ All Financial Specialists and CRMs are subject to regular video mystery shopping reviews and other risk assurance activities
- ✓ KRIs are monitored on an ongoing basis to provide early warning of potential customer detriment

POL00400101

Current key conduct risks and mitigation

Customers buy products which do not meet their needs, as the result of financial promotions material which is misleading, unclear, unfair or out-of-date, or which is otherwise non-compliant

Mitigation:

- ✓ All financial promotions material is subject to formal regulatory review and approval by BOI
- ✓ Controls are in place to ensure material is regulatory re-reviewed and withdrawn if out-of-date
- ✓ Risk assurance activity is undertaken to identify instances of unapproved or out-of-date material being used
- ✓ Guidelines are in place in relation to the use of un-approved promotional material and the use of the internet and social media for promotional purposes

POL00400101

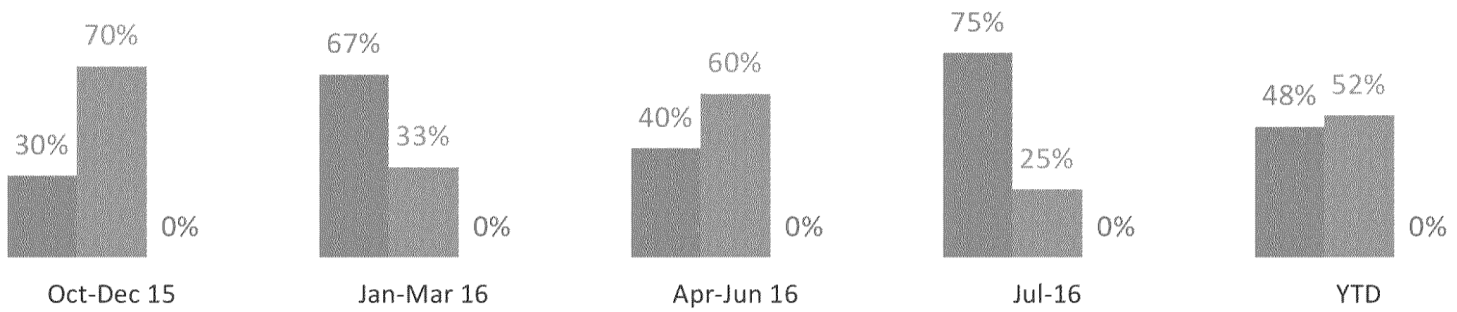
Current key conduct risks and mitigation

Customers best interests are compromised as the result of inadequate conduct controls or as the result of conduct or regulatory failures which are not corrected

Mitigation:

- ✓ Risk assessments are routinely used to identify potential risks to customers and to ensure that appropriate processes and controls are deployed
- ✓ Sales processes, training material, sales support material and variable remuneration and incentive arrangements are subject to review and approval by BOI and POL Risk Teams
- ✓ Extensive risk-based assurance activities, including branch and FSAM reviews, are undertaken by BOI Risk Assurance Teams (see below)

Results of BOI FSAM Manager Reviews – August 15 – July 16



POST OFFICE Money

Bank of Ireland UK

POL00400101

Current key conduct risks and mitigation

Customers best interests are compromised as the result of inadequate conduct controls or as the result of conduct or regulatory failures which are not corrected

Mitigation:

- ✓ Formal notification processes exist to ensure that the Bank is advised of any issues and breaches
- ✓ Issues and breaches are formally investigated, resolved and reported to senior management
- ✓ Root-cause-analysis is routinely used to identify the underlying causes of issues and breaches, to ensure that processes and controls are enhanced to avoid repetition and to ensure that customers do not suffer detriment

POL00400101

Areas of conduct focus

- **Video mystery shopping** results have historically been a cause for concern and, despite significant improvement, continue to be an area of ongoing focus
- The **performance management, incentivisation and remuneration of sales staff** has come under intense regulatory scrutiny
- The introduction of the **Senior Managers Regime** has highlighted the importance of ensuring that the Bank's first-line risk oversight of Post Office is robust and effective
- There is a need to demonstrate that a **conduct culture is fully embedded within Post Office** and work is needed to ensure that the regulatory risks inherent in the wider network are being effectively mitigated
- The BOI Risk Improvement Roadmap has highlighted the need to ensure that the **three-lines of defence are documented and understood** across the partnership
- Significant improvements are required in the deployment of **fitness and propriety vetting protocols** for Mortgage Advisers and FSAMs

POL00400101

Areas of conduct focus

Video mystery shopping results have historically been a cause for concern

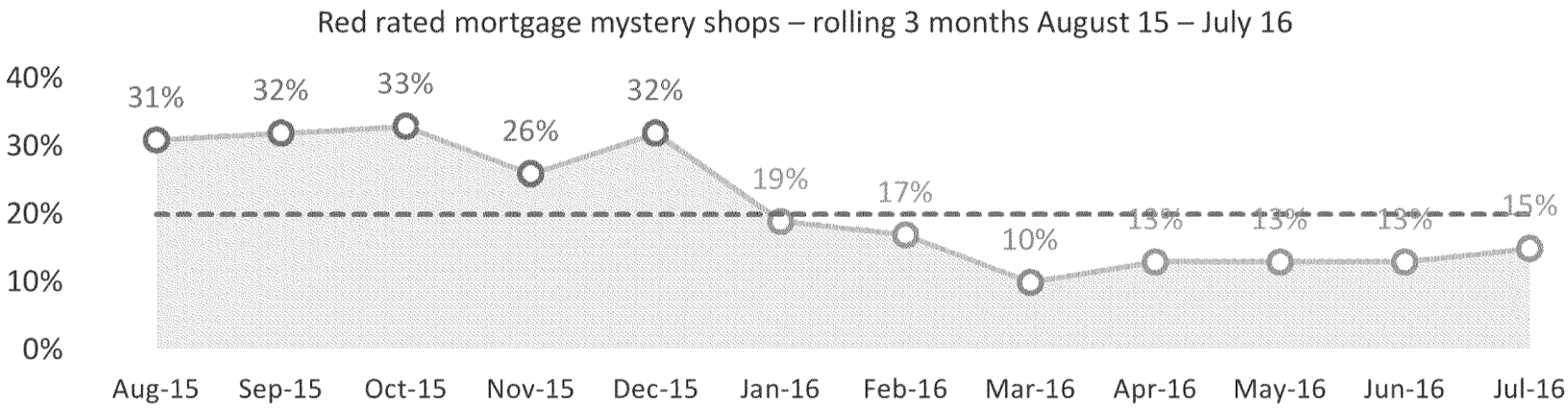
- Results have improved over the last 12 months, with overall levels of red shops falling from 18% in August 2015 to 10.8% in July 2016, against a target of <20%
- For the three months ending July 2016, only 9% of Specialists shops and 14% of Agency CRM shops were rated red
- These performance improvements are now consistently replicated on a month-to-month basis (see below)

POL00400101

Areas of conduct focus

Video mystery shopping results have historically been a cause for concern

- However, while mystery shopping results overall have improved:
  - Levels of red-rated mortgage mystery shops were a cause of concern in late 2015
  - There have been three black-rated mortgage mystery shops during 2016, indicating unsuitable advice
  - An action plan was implemented in late-2015 to reduce the level of red-rated mortgage mystery shops
  - Levels of red rated mortgage shops reduced as a result, but maintenance of competence remains a challenge while sales activity levels are low



POL00400101

Areas of conduct focus

The performance management, incentivisation and remuneration of sales staff has come under intense regulatory scrutiny

- The performance management, incentivisation and remuneration of sales staff has become a key area for the regulator
- FCA have published guidance in this area, and we have followed suit, updating and enhancing our regulatory guidance for POL
- All POL variable incentive schemes, which related to financial services products, are subject to regulatory review and approval by BOI
- POL MS, FS and FSAM incentive schemes have been reviewed and updated, with enhanced oversight and governance arrangements deployed
- There is no evidence to suggest that MS, FS and FSAM incentive schemes have resulted in poor outcomes for customers or non-compliant sales activity
- Work continues as part of the Wider Network Action Plan to ensure that staff at all levels understand how poor performance management can lead to poor customer outcomes

POL00400101

Areas of conduct focus

The introduction of the Senior Managers Regime has highlighted the importance of ensuring that the Bank's first-line risk oversight of Post Office is robust and effective

- The Senior Managers Regime (SMR) came into force on 7 March 2016
- Senior managers now have a statutory duty of responsibility to take 'reasonable steps' to prevent regulatory breaches in their area of responsibility
- Senior managers need to actively demonstrate that they have their 'finger on the regulatory compliance pulse' for their area of responsibility and that they are fully aware and in control of all the regulatory risks and issues relating to these functional areas
- Given the current operational reliance placed on Post Office to provide Bank of Ireland's first line of defence, both organisations are investigating how current C&DM resources can be better utilised to provide the Bank's senior managers with the assurance that they need

POL00400101

Areas of conduct focus

There is a need to demonstrate that a conduct culture is fully embedded within Post Office and that regulatory risks in the wider network are being mitigated

- An action plan has been implemented to ensure that the conduct culture is fully embedded within Post Office and that the behaviours of staff at all levels are aligned with this
- Significant progress has been made:
  - the network lead team have attended engagement sessions on conduct risk, understand the importance of this and are committed to its deployment throughout the network
  - the branch sales model has been reviewed and found to be fit for purpose
  - Customer Relationship Managers have been introduced in the wider Agency network
  - guidance has been provided to line managers in relation to performance management, and enhanced incentive scheme governance and oversight arrangements deployed
  - staff training programmes have been updated and are being rolled out
  - robust risk assessment processes have been deployed by the POL FS Risk function

POL00400101

Areas of conduct focus

There is a need to demonstrate that a conduct culture is fully embedded within Post Office and that regulatory risks in the wider network are being mitigated

- Good progress is being made, however, significant work is still required to improve systems and controls in the wider branch network, in particular:
  - staff retraining on the branch sales model focusing on the role of senior/middle managers
  - rolling out updated regulatory and conduct training across the network and improving training-related record keeping
  - providing staff with greater access to compliance procedures and guidance
  - improving the effectiveness of internal communications
  - improving the format and usability of conduct-related management information
  - deploying effective POL first/second line risk assurance controls in the wider network
  - improving significantly the deployment of Mortgage Adviser and FSAM fitness and propriety verification processes
  - improving staff awareness of, and access to, whistle-blowing policies

POL00400101

Areas of conduct focus

Significant improvements are required in the deployment of fitness and propriety vetting protocols for Mortgage Advisers and FSAMs

- A recent review by BOI Risk Assurance has identified significant shortfalls in the fitness and propriety (F&P) records maintained by Post Office in relation to Mortgage Advisers and FSAMs
- This review has been rated red, indicating numerous breaches and control framework weaknesses
- In particular, the review concluded that:
  - while robust F&P processes are in place, these are not being deployed effectively; and
  - governance and oversight arrangements are inadequate
- This follows an earlier review by Bank Internal Audit and two earlier internal reviews by the Post Office FS Risk Team, which also identified weaknesses

POL00400101

Conclusions

- Generally, significant or material conduct and regulatory issues and breaches are rare, with no indication of systemic issues in the network
- Day-to-day risk management and oversight of conduct and regulatory risks is generally effective
- Conduct and regulatory KRIs confirm that conduct and regulatory risk management targets are generally being met, with only isolated exceptions being identified
- While there have been shortcomings against some KRI targets – e.g. mystery shopping - actions have been taken to address these and these appear to have been effective
- BOI and POL remain aligned on the conduct agenda and the relationship between the parties is good

POL00400101

Conclusions

- However, we must not be complacent
- There are significant challenges and areas requiring continued focus:
  - demonstrating that the conduct agenda is fully embedded at all levels of the organisation and throughout all parts of the network
  - ensuring that steps continue to be taken 'at pace' to mitigate the risks in the wider network
  - significantly improving the robustness of fitness and propriety checking for Mortgage Advisers and FSAMs
  - providing Bank's senior managers with the necessary assurance that Post Office provides an effective first-line-of-defence
  - Ensuring that mortgage advisers maintain competence in periods where activity levels are low

POL00400101

Annex 1

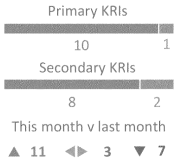
Post Office branch distribution conduct risk dashboard – August 2016

POL00400101

Post Office Money branch distribution

How we performed against our aims in August 2016

Our aims describe how we will meet our FACE Customer Charter commitments and promises. Using a range of key risk indicators, we measure our performance against each of our aims. This tells us how well we're doing against our targets and highlights areas where we could improve our performance. We also use our performance to give ourselves an overall risk rating. This month, we rated our overall performance as Amber. Finally, the risk ring shows the relative ratio of green, amber and red rated key risk indicators.



Our customer charter	Our aims	Our performance			
Our commitments and promises	**How we meet our commitments and promises**	**We use a range of key risk indicators to measure our performance against our aims and to highlight areas where we need to improve**			
		How we measure ourselves	Our targets	How we're doing Jul-16	Jun-16
Fair - you are at the heart of everything we do	We provide information and advice that our customers can rely on	We use **mystery shoppers** to test how well our staff are meeting our conduct risk requirements and our customer's needs	Fewer than 20% of mystery shops are rated red in the quarter	**10.8%**	12.2% ▲
			No shops are rated black in the month	**0**	0 ◀▶
			Fewer than 10% of our Specialists have more than one red or black shop in the preceeding six months	**0.9%**	0.8% ▼
		Our Quality Assurance Team assess the **quality of the mortgage advice** we give customers to ensure it's suitable to their needs	At least 80% of cases are rated A or B by the QAT in the month	**93%**	91% ▲
			Fewer than 5% of cases are rated D by the QAT in the month	**1.1%**	2.3% ▲
			At least 85% of MSs meet the QAT benchmark in the month	**91%**	86% ▲
		We use branch reviews and monitor breaches to ensure our **financial promotions** are compliant and up to date	90% or more of our branch reviews are rated green or amber for financial promotions in the quarter	**97%**	100% ▲
			We record fewer than 11 material financial promotions breaches in the quarter	**0**	1 ▲
	We do our best to get things right first time and act quickly to put it right if we don't	We monitor customer **complaints** to understand what we're getting wrong and why, and to ensure we get it right in the future	We uphold fewer than 21 significant complaints for every 1,000 products we sell	**1.14**	0.94 ▼
			Upheld complaints grow no more than 21% faster than sales	**19%**	-5% ▼
			Upheld significant complaints increase no more than 21% month-on-month	**6%**	10% ▲
Accessible - we provide a friendly, efficient and reliable service	We listen to our customers and act when they tell us we could do things better	We use **customer feedback** to tell us whether we met their needs at the point-of-sale	At least 90% of compliance survey questions confirm customer's needs and compliance standards are met in the quarter	**96.5%**	96.4% ▲
			At least 90% of NPS surveys confirm customers receive the information they need in the quarter	**98.2%**	97.4% ▲
Committed - we aim to build long-term relationships	We have staff with the requisit levels of skill, knowledge and expetise	We use the results of **knowledge tests** to ensure our staff have the skills, knowledge and expertise to meet our customer's needs	At least 80% of BOI product knowledge reviews are rated green or amber in the quarter	**100%**	100% ◀▶
			At least 80% of BOI regulatory awareness reviews are rated green or amber in the quarter	**100%**	100% ◀▶
			Specialists pass at least 80% of POL knowledge tests in the quarter	**99.2%**	99.2% ▼
		We monitor our **training and competence** arrangements to ensure staff are maintaining their competence and are being adequately supervised	At least 80% of Specialists are signed off as fully competent	**87.3%**	87.8% ▼
			At least 80% of FSAMs are within agreed spans of control	**96%**	100% ▼
			At least 80% of BOI FSAM reviews are rated green or amber in the quarter	**96%**	100% ▼
Easy to do business with - we promise to keep it simple and straightforward for you	Our products are easy to understand and meet customer's needs and expectations	We monitor the **retention and use of our products** by customers to ensure they meet their needs and expectations	Customers cancel no more than 1.5% of savings products in the cooling-off period	**0.76%**	0.75% ▼
			No more than 40% of credit cards remain unused after the first six months	**29%**	29% ▲

▲ Performance improving from previous month ▼ Performance worsening from previous month ◀▶ Performance unchanged from previous month

POL00400101

Post Office Money branch distribution key risk indicators

How we measure ourselves

We use a range of primary and secondary key risk indicators to measure our conduct risk performance. Primary indicators are designed to provide direct insight into customer experience and secondary indicators are designed to provide indirect insight into customer experience. We measure each of these indicators on a monthly basis and rate our performance either green, amber or red based on the metrics shown below.

Primary indicators

KRI description		Our metrics		
		Green	Amber	Red
We use **mystery shoppers** to test how well our staff are meeting our conduct risk requirements and our customer's needs	The proportion of shops rated red in previous three months	0.00% - 10.99%	11.00% - 20.00%	20.01% - 100.00%
	The number of shops rated black in previous month	0		1 or more
	The proportion of Specialists with multiple (>1) red/black shops in the previous six months	0.00% - 5.99%	6.00% - 10.00%	10.01% - 100.00%
Our Quality Assurance Team assess the **quality of the mortgage advice** we give customers to ensure it's suitable to their needs	The proportion of mortgage cases rated A or B by the QAT on initial review in the previous month	100.00% - 90.00%	89.99% - 80.00%	79.99% - 0.00%
	The proportion of mortgage cases rated D by the QAT on initial review in the previous month	0.0% - 5.00%		5.01% - 100.0%
	The proportion of Mortgage Specialists with 80%+ A/B grades on initial review in the previous month	100.00% - 90.00%	89.99% - 85.00%	84.99% - 0.00%
We monitor customer **complaints** to understand what we're getting wrong and why, and to ensure we get it right in the future	The number of upheld significant complaints per 1,000 products sold over a rolling 3 month period	0 - 10.9	11 - 20.9	21.0 or more
	The variance in upheld significant complaints compared with the variance in sales in the last month	Up to 10.99%	11.00% - 20.99%	21.00% or more
	The month-on-month variance in significant upheld branch complaints	Up to 10.99%	11.00% 20.99%	21.00% or more
We use **customer feedback** to tell us whether we met their needs at the point-of-sale	The proportion of customer responses to compliance surveys confirming compliance requirements were met at the point of sale in the previous 3 months	100.00% - 95.00%	94.99% - 90.00%	89.99% - 0.00%
	The proportion of customer responses to NPS surveys that confirm adequate information was provided at the point of sale in the previous three months	100.00% - 95.00%	94.99% - 90.00%	89.99% - 0.00%

Secondary indicators

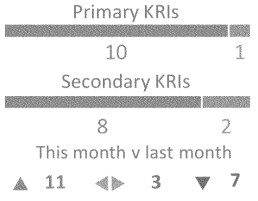
KRI description		Our metrics		
		Green	Amber	Red
We use the results of **knowledge tests** to ensure our staff have the skills, knowledge and expertise to meet our customer's needs	The proportion of 'product knowledge' assessments rated green/amber during BOI branch reviews completed in the previous three months	100.00% - 90.00%	89.99% - 80.00%	79.99% - 0.00%
	The proportion of 'FCA' assessments rated green/amber during BOI branch reviews completed in the previous three months	100.00% - 90.00%	89.99% - 80.00%	79.99% - 0.00%
	The proportion of POL knowledge tests passed by Specialists and FSAMs in the previous three months	100.00% - 90.00%	89.99% - 80.00%	79.99% - 0.00%
We use branch reviews and monitor breaches to ensure our **financial promotions** are compliant and up to date	The proportion of 'advertising' assessments rated green/amber during branch reviews completed in the previous three months	100.00% - 95.00%	94.99% - 90.00%	89.99% - 0.00%
	Material financial promotions breaches recorded in the previous three months	0 - 5	6 - 10	11 or more
We monitor the **retention and use of our products** by customers to ensure they meet their needs and expectations	The proportion of savings products cancelled within the cooling-off period in the previous month	0.00% - 1.00%	1.01% - 1.50%	1.51% - 100.00%
	The proportion of credit cards opened over a six month period, which remain unused by customers	0.00% - 20.99%	21.00% - 40.00%	40.01% - 100.00%
We monitor our **training and competence** arrangements to ensure staff are maintaining their competence and are being adequately supervised	The proportion of current Specialists signed-off as fully competent	100.00% - 90.00%	89.99% - 80.00%	79.99% - 0.00%
	The proportion of FSAMs within supervisory spans of control	100.00% - 90.00%	89.99% - 80.00%	79.99% - 0.00%
	The proportion of close supervision, ongoing supervision and T&C knowledge related assessments rated green/amber during branch reviews completed in the previous three months	100.00% - 90.00%	89.99% - 80.00%	79.99% - 0.00%

POL00400101

Post Office Money branch distribution - conduct risk dashboard for August 2016

The overall risk rating provides an indication of the conduct risk represented by Post Office branch distribution. It is based on the cumulative outcome of all key risk indicators, weighted to reflect the results of 'primary' indicators - providing direct insight into customer experience and annoted (P) below – and 'secondary' indicators – providing indirect insight into customer experience and annoted (S) below. This gives an overall Amber risk rating for the month.

The risk ring illustrates the relative ratio of green, amber and red rated key risk indicators, with primary indicators accounting for twice as much of the ring as secondary indicators.



						Feb-16	Mar-16	Apr-16	May-16	Jun-16	Jul-16
Mystery shopping (P)	Red shops 10.8% (12.2% ▲)	Black shops 0 (0 ◀▶)	>1 red/black 0.9% (0.8% ▲)	Shops rated red in previous quarter (red: >20%)		8.6%	7.3%	10.2%	9.9%	12.2%	**10.8%**
				Shops rated black in last month (red: 1 or more)		1	0	1	0	0	**0**
				FS/MS multiple red/black shops (red: >10%)		0.0%	0.4%	0.4%	0.7%	0.8%	**0.9%**
Quality of mortgage advice (P)	Cases rated A/B 93% (91% ▲)	Cases rated D 1.1% (2.3% ▲)	MS at 80% A/B 90.7% (86.2% ▲)	Cases rated A or B by QAT (red: <80%)		95%	96%	92%	92%	91%	**93%**
				Cases rated D by QAT (red: >5%)		0.0%	0.0%	2.1%	2.2%	2.3%	**1.1%**
				Specialists meeting QAT benchmark (red: <85%)		93.1%	92.2%	84.0%	89.4%	86.2%	**90.7%**
Significant customer complaints (P)	Per 1,000 sales 1.14 (0.94 ▼)	Complaints v sales 19% (-5% ▼)	Complaints variance 6% (10% ▲)	Upheld complaints per 1,000 sales (red: 21 or more)		0.59	0.84	0.94	0.98	0.94	**1.14**
				Complaints v sales variance (red: +21% or more)		-22%	41%	12%	4%	-5%	**19%**
				Month-on-month complaints variance (red: +21% or more)		-19%	35%	13%	19%	10%	**6%**
Customer insight (P)	Compliance surveys 97% (96.4% ▲)	NPS surveys 98% (97.4% ▲)		Compliance survey responses (red: <90%)		97.7%	97.4%	97.3%	97.3%	96.4%	**96.5%**
				NPS survey responses (red: <90%)		96.4%	95.9%	96.8%	97.8%	97.4%	**98.2%**
Knowledge and awareness (S)	Product knowledge 100.0% (100.0% ◀▶)	Regulatory awareness 100.0% (100.0% ◀▶)	FS/MS knowledge 99.2% (99.2% ▼)	BOI branch product knowledge reviews (red: <80%)		100.0%	100.0%	100.0%	100.0%	100.0%	**100.0%**
				BOI branch regulatory awareness reviews (red: <80%)		100.0%	100.0%	100.0%	100.0%	100.0%	**100.0%**
				POL knowledge and awareness reviews (red: <80%)		97.6%	98.3%	99.0%	98.7%	99.2%	**99.2%**
Financial promotions (S)	BOI branch reviews 97% (100% ▲)	Significant breaches 0 (1 ▲)		Branch financial promotions reviews (red: <90%)		100%	100%	100%	100%	100%	**97%**
				Material financial promotion breaches (red: 11 or more)		1	1	2	1	1	**0**
Product retention and usage (S)	Saving cancellations 0.76% (0.75% ▼)	Credit card usage 29% (29% ▲)		Savings cancellations (red: >1.5%)		0.80%	0.62%	1.06%	1.12%	0.75%	**0.76%**
				Credit cards unused after 6 months (red: >40%)		28.6%	30.4%	30.7%	30.0%	29.5%	**29.3%**
Training and competence (S)	Competent FS/MS 87% (88% ▼)	Spans of control 96% (100% ▼)	BOI FSAM reviews 96% (100% ▼)	Fully competent specialists (red: <80%)		87%	87%	84%	86%	88%	**87%**
				Supervisors within span of control (red: <80%)		94%	97%	97%	100%	100%	**96%**
				FSAM reviews rated green/amber (red: <80%)		93%	100%	100%	100%	100%	**96%**

Performance ratings: ▲ Performance improving from previous month ▼ Performance worsening from previous month ◀▶ Performance unchanged from previous month

BOI Group classification : **Red** (confidential)

POL00400101

Post Office Money branch distribution - analysis and exceptions summary for August 2016

 Mystery shopping	Specialists - Work is ongoing in an effort to continue improvements in mortgage (Action 010) and savings mystery shops. Following an earlier increase in red rated savings shops in the three months to the end of July, this figure has now reduced. CRMs - Red rated savings mystery shops for CRMs have increased. In four instances, CRMs made comments which could have been interpreted as advice, and there were instances of customers being encouraged to apply immediately and being provided with incorrect information. A range of remedial actions have been undertaken to address the issues identified. (Action 018)
 Quality of mortgage advice	Following a deterioration in results over the previous 4 months, the initial pass rate improved in July. In addition, all regions acheieve an initial pass rate of 90% or more for July. 49% of cases were rated 'A' against a target of 60%, a reduction of 3% from June. All regions were rated 'green' this month for D rated cases. The number of MSs with fewer than 80% of their cases rated A or B decreased from 9 in June to 4 in July and, overall, the proportion of MSs meeting this benchmark improved from 86% in June to 91%. The Northern region had three MSs below this benchmark. As in previous months, low levels of submissions for some MSs resulted in single fails having a disproportionate effect on their figures.
 Significant customer complaints	Significant upheld complaints rose marginally to 36 in the three months to the end of July, compared to 34 for the three months to the end of June, an increase of 6%. Unfortunately, sales figures for credit cards were not available at the time of reporting. As such, a sales figure of 1,900, based on the average number of sales made in each of the previous 6 rolling 3 month periods, has been used. This will be updated when the actual figure becomes available. On this basis, the complaint versus sales variance was rated amber this month, with sales falling 13% and complaints increasing by 6%. The most notable percentage increase in complaints related to credit cards, although the 200% increase related to an increase of only 2 complaints.
 Customer insight	No 'hot spots' or issues identified. NPS survey results were not available for July at the time of reporting. Thus, the 'NPS survey response' KPI results relate to calls made in May and June only. The dashboard will be updated when the data for July becomes available.
 Knowledge and awareness	No 'hot spots' or issues identified.
 Financial promotions	No material breaches were recorded by POL as a result of their website and social media usage monitoring or by the BOI Financial promotions Team in July. One branch was rated red in relation to financial promotions during July. This was due to a member of staff not being aware of the consequences of producing homemade posters and the amount of out-of-date product literature that was found to be available to customers.
 Product retention and usage	Savings cancellations - No 'hot spots' or issues identified. Credit card usage - This metric has been rated amber for some time as a result of the usage of the Platinum card. This card is designed and promoted for holiday use and the C&CRC acknowledges that other management information and KRIs in this regard are not suggestive of systemic branch mis-selling. Data for July 2016 was unavailable at the time of reporting. The dashboard will be updated once the data is made available.
 Training and competence	The proportion of Specialists yet to be signed off as 'fully competent' is above the target of 80% for both Financial and Mortgage Specialists, but is amber rated for both populations. In the last month, two requests to progress Financial Specialist's to ogoing competence have been rejected by POL T&C due to the FS having multiple red VMSs. It has been necessary to extend the CSPs for all FSs currently in close supervision, as there is insufficent evidence to demonstrate their competence at this stage. The number of Mortgage Specialists in extended periods of Close or Enhanced Supervision has improved slightly as a result of the additional measures being taken to support earlier sign-off. 11 Mortgage Specialists are on extended CSPs, with a lack of activity continuing to result in MSs being unable to demonstrate the required level of competence.

POL00400101

POST OFFICE

AUDIT, RISK AND COMPLIANCE COMMITTEE

Financial Services - How Post Office meets its regulatory obligations

Author: Jonathan Hill Meeting date: 28 September 2016

Executive Summary

Context

1. Financial Services (FS) are a key part of Post Office achieving its sustainability. FS operates across a number of diverse products and services with significant regulation. It is therefore crucial that FS manages its risks to protect Post Office while seeking to deliver targeted growth. The Committee requested an update on how Post Office meets its FS regulatory obligations.

2. This paper focuses on the key regulations required by the Financial Conduct Authority (FCA), Post Office is also regulated by the HMRC for Anti Money Laundering (AML) and Counter Terrorist Financing (CTF). A separate item at the September meeting of the ARC addresses these controls. In addition, the business is also subject to the information requirements of the newly formed Payment Systems Regulator (PSR). The PSR's main requirements are directly focused on firms offering payment systems, such as MasterCard and Link rather than Post Office. But as a payment provider Post Office may be required to provide information on an ad hoc basis to assist with the PSR's strategic competition objectives. In addition, FS along with the rest of the Post Office, is required to follow data protection rules and the requirements of the Information Commissioner.

3. For FCA regulation, Post Office is an appointed representative (AR) of Bank of Ireland UK plc ("BoI") and Post Office Management Services Limited ("POMS"). BoI and POMS are Post Office's regulatory principals. The appointed representative agreements allows Post Office to be exempt from authorisation under the Financial Services and Markets Act to undertake Financial Conduct Authority (FCA) regulated activities provided certain conditions are met, including that the principals will take regulatory responsibility for Post Office in respect of such activities.

4. As an AR, Post Office needs to understand and comply with the regulatory requirements applicable to them for the activity they carry out. Services are contracted under a Financial Services Joint Venture Agreement (FSJVA) for BoI and a Distribution Agreement for POMS, which both include Regulatory Guidance Manuals (RGM) to govern the conduct of regulated activity.

POL00400101

Questions this paper addresses

A. What are the key obligations that Post Office needs to meet as an AR?

B. How Post Office meets these obligations

C. Next steps

Conclusion

5. There are defined responsibilities, governance, oversight and monitoring in place. These are well established and developed with BoI and form the basis of the approach within POMS. These controls are focussed on the areas of greatest risk which are Mortgage/Financial Specialist (MS, FS) and Customer Relationship Manager (CRM) activity. For the wider network, there are sources of assurance, which we are building on through the actions of the 'Network conduct risk action plan'.

6. Conformance with compliant customer journeys have seen significant progress been positive progress, e.g. Video Mystery Shopping ("VMS") results have markedly improved over the last 2 years (in spring 2014 red rated VMS were trending at over 50%, in October 2015 this had fallen to 33% and in July 2016 we experienced only 10.8% red VMS) reflecting improved competence and culture.

7. The strategy to improve engagement through the CRM programme has been risk assessed at every stage to mitigate conduct risk and includes a bespoke Training and Competence programme. We have also seen a step change in the awareness of FS regulation and conduct risk in the senior leadership team in Network. The monthly conduct report (attached in the Appendix) produced for the BoI/Post Office Customer and Conduct Risk Committee highlights the current position of Post Office meeting its regulatory obligations.

8. The detail of actions to mitigate conduct and compliance risk are included in the paper. Our progress on these actions are regularly shared with BoI and POMS.

Input Sought

The ARC is asked to note these developments.

POL00400101

The Report

Post Office's Appointed Representative responsibilities

9. The requirements of both Principals are outlined in the respective RGMs. The focus of Principal oversight is Post Office branch distribution as the Principals receive oversee themselves compliance management information in respect of call centre and internet distribution.

10. The RGMs outline the compliance requirements to be followed in key areas covering the FCA handbook together with relevant product related schedules. These include:

- Training and Competence
- Performance Management and Incentives
- Data Protection
- Financial Promotions
- Reporting
- Conduct
- Customer complaints
- Financial Crime
- Perimeter guidance for introducing and selling products

Governance

Post Office and BoI

11. Post Office Risk reports into the monthly Sales Oversight Compliance Forum (SOCF), this is a joint forum with the BoI to review compliance and conduct risks. This meeting reports into the senior Committee Customer and Conduct Risk Committee (CCRC) which also meets monthly. The CCRC is represented by the respective teams from risk and compliance. It has business representation from the Director of FS, the Network and Sales Director and senior business representation from BoI including the Chief Risk Officer.

12. The CCRC has a dotted line into the Post Office Partnership Board which is the senior joint management committee where BoI and Post Office oversee all aspects of the joint venture, including conduct and compliance risk.

POL00400101

Post Office and POMS.

13. POMS has a monthly Risk & Compliance Committee. This is attended by the Post Office FS Risk team, POMS Head of Risk and Compliance and the Post Office Network and Sales Director. This forum reports into the POMS ARC.

Post Office/POMS/BoI tripartite meeting.

14. This does not report into a formal structure but is used to discuss current shared issues of interest and co-ordinated working, for example to ensure that monitoring and audit activity is co-ordinated. It aligns to the principles of the 'multi-principal' arrangements between POMS and BoI, as required by the regulators.

Three lines of defence

15. The model used is set out in the following table. Both Principals consider Post Office as their first line for sales distribution and marketing.

	BOI/POMS	**Post Office**
1st line	Product team (POMS/BOI and third party providers) Capability Development Managers Financial Promotions teams	FS Product teams Branch Sales Supervisory Structure Marketing and PR teams FS Risk and Training and Competence function
2nd line	Risk and Compliance Monitoring Financial Promotions Monitoring Regulatory Horizon scanning	Post Office Risk (Corporate Services)
3rd line	Internal Audit	Internal Audit supported by PWC

Management Information

16. The typical MI reviewed included as part of governance meetings (SOCF, CCRC) includes:

- Training and Competence reports
- Risk registers
- Regulatory Horizon scanning
- Reports into incident breaches

POL00400101

- Complaints reporting
- Compliance monitoring reports and planned activity, e.g., video mystery shopping, customer validation calls, branch audit visits etc. (*see appendix 1 for example of Customer and Conduct Risk Committee MI)*

Current Key Conduct Risk Issues for BoI and POMS

Vetting and Fit and Proper

17. Both FS Risk and BoI Compliance have undertaken reviews of the processes followed in respect of HR vetting of Mortgage Specialists and their managers. Significant gaps have been found in terms of being able to evidence the checks that have been undertaken to ensure that these individuals are 'fit and proper'. Whilst subsequent 'back checking' has confirmed that Post Office did not employ anyone that was not 'fit and proper' we need to work with the HR team to mitigate the issues raised and agree a timetable for agreement. It is likely that BoI will conduct a follow up review to gain assurance that control improvements have taken place.

18. The wider issue of establishing 'fit and proper' processes across the wider network is addressed below in the 'People' section of the action plan. One of the key gaps identified was the lack of credit checking. POMS compliance have worked with HR on the drafting of the new requirements; a key task will be to implement the policy effectively.

Compliance monitoring

19. The conduct risk assessment has identified that there are compliance monitoring gaps for Travel Insurance, Over 50s Life insurance and savings opening counter journeys. All of the sales journeys, materials and scripts have been reviewed and agreed by the Principals. We are, however, unable to provide any monitoring assurance on a risk basis that these counter conversations are being undertaken compliantly outside of the FS/MS and CRM structure.

20. As part of the conduct risk action plan we are working with our Principals to improve our counter monitoring and we will have a plan of risk based mystery shopping in place by the end of 2016.

Training compliance

21. Post Office is not able to confirm whether Postmaster staff undertake mandatory compliance training including product-specific training. A particular issue for POMS is the inability of Post Office to confirm that product training has been undertaken and understood for over 50s Life insurance and Travel Insurance.

22. The planned mitigation enhancements to the front end user system 'Horizon'. The planned Enhanced User Management for Horizon linked to 'success factors' training should be able to provide the training and control environment required.

POL00400101

FS Risk and the Principals need to ensure that the specification of the upgrade continues to keep this compliance requirement and to monitor the timescales (currently expected January 2017).

Network Conduct Risk Action Plan

23. During 2015, together with BoI, we assessed the wider selling risks in the Post Office network and whether further controls needed to be in place. Other reviews into conduct risk at the Post Office by Post Office Internal Audit, Alvarez and Marsal and BoI Internal Audit also encouraged Post Office to review the 'wider' conduct risks in the network and assess whether more should be done to mitigate them. This risk assessment work was undertaken by FS Risk, this identified key risks areas that were turned into a conduct risk action plan.

24. This action plan was shared with the Post Office network lead team this February. Since then we have worked with the network teams and others to both re-test our assumptions about the level of risk but also to follow up on agreed actions.

Progress on the Network Conduct Risk Action Plan

The following key risks areas were identified as part of the risk assessment

Risk Area	Why this is important?
Sales Model/Business Targets	The Sales Model is a key driver of behaviours in the network
Culture and Training	People know what they have to do and why and appropriate behaviours supported by 'tone from top'. Can we evidence training?
Performance Management	How we motivate, set targets and communicate to staff can have an impact on customer experience.
Monitoring	Are we able to monitor compliance performance to gain assurance?
Remuneration/Incentives	Remuneration and Incentives could drive inappropriate behaviours
Communications	Staff are equipped to communicate effectively to customers. Management communications to staff are balanced in respect of customer needs.
People	Are objectives and people management in line with good conduct risk principles, are staff 'fit and proper'?
Risk Management	Are we risk managing initiatives for customer and conduct risk?
Management Information	Do we have the MI to manage and monitor conduct risk?

25. As part of the action plan a detailed tracker is in place to record open actions at a granular level.

POL00400101

Network Sales Model

26. Revising the sales model is important as there is a risk that the existing model would drive inappropriate conduct behaviours, impacting on colleague behaviours with negative impacts on customers. This has been the case with other firms in financial services who have adopted a 'product push' culture.

27. The FS Risk team devised a risk assessment template to review the sales model. This covered the key risk areas identified by the FCA in their Performance Management Guidance. The risk areas identified included, performance meetings, warm ups, warm downs, coaching, conference calls, emails, sales reporting and MI. As part of the coaching out of the sales model the risks of inappropriate behaviours have been highlighted in the Crown training. The FS risk team and BoI have reviewed the sales model and confirm that it is appropriate and balanced from a customer perspective, reflecting customer experience, team development as well as sales opportunity.

Network Sales Model-Key actions

28. The Crown network has begun a series of cascade presentations, with input from FS Risk, to improve training of the sales model and to improve awareness of conduct risks to the sales model. These presentations have started at the Area Manager level working down to Branch Manager (Mike Elliot Crown October 2016).

29. Similarly the Agency network team is reviewing its sales model, risk assessing this and providing training to the branches with the support of FS Risk. (Colin Newton Agency October 2016).

Culture and Training

30. This was established as key, ensuring the right culture is key to mitigating conduct risk but this is a difficult thing to measure and change. FS Risk has had several engagement sessions with the Network Lead Team and these have been well received. These covered conduct risk, performance management (including reference to FCA paper FG 15/19 on managing the risks to performance management) and the regulatory context. These include:

- Post Office Group Executive team training on Conduct Risk and regulation supplied by PWC
- Performance Management Slides developed for network team by risk (Feb 2016)
- Presentation to Sales Trainers on conduct risk (May 2016)
- Presentation to Crown lead team on conduct risk (May 2016)
- Presentations to network lead team in February and March on conduct risk

POL00400101

31. During 2016 there has been a step change in the level of awareness of regulation and conduct risk. The CRM programme has been a good example of the network managing conduct risk with risk team oversight as we seek to grow the business.

Culture and Training-key actions

32. A key risk is that Post Office cannot currently confirm whether Postmaster staff undertake mandatory compliance training including product-specific training. A particular issue for POMS is the inability of Post Office to confirm that product training has been undertaken and understood for over 50s life insurance and Travel Insurance.

33. The mitigation to this are enhancements to the front end user system 'Horizon'. The planned Enhanced User Management for Horizon linked to 'success factors' training should be able to provide the training and control environment required. FS Risk and Post Office's principals need to ensure that the specification of the upgrade continues to keep this compliance requirement and to monitor the timescales (Business Sponsor Angela Van Den Bogerd currently expected January 2017).

34. In addition the detailed action plans highlight a number of training programmes for front line staff and middle management that have been either updated or are in the process of being revised to ensure that they fully cover customer risks. These should be completed by end October with Post Office Learning Academy.

Performance Management and Monitoring

35. How we motivate, target set and communicate to staff can have an impact on customer experience. We have reviewed Post Office HR performance management procedures: the review indicates that these are balanced, appropriate and do not 'punish' staff for poor sales performance. The 'Building a customer focussed culture' was delivered to the network earlier this year.

36. As part of the lead team training, the importance of ensuring appropriate messaging on performance has been understood and inappropriate email messaging, which had been an issue in the network, has virtually ceased. There is a commitment from the Network Lead team to take action if any inappropriate messaging is reported.

37. The recently updated sales model performance charts include People and Customer measures as well as Sales. People and Customer are treated just as importantly as sales. The strategy is to support our people in delivering an outstanding customer experience and the resulting sales performance is an output of how effective colleagues have been developed and how they engage with our customers.

POL00400101

Performance Management and Monitoring-Key actions

38. We need to improve monitoring and monitoring tools beyond the CRM/Specialists population. There are identified compliance monitoring gaps including reviewing the savings account journeys in branch and the sales of travel and over 50s life products. Neither Post Office nor the principals monitor the quality and compliance of these sales journeys. Therefore it is difficult to demonstrate compliance in the way the regulator would expect.

39. POMS/BoI and Post Office will mitigate these gaps with additional risk based mystery shopping reviews potentially supplemented by customer validation calls. Action owners FS Risk, BoI and POMS (December 2016).

Remuneration and Incentives

40. Remuneration and incentive schemes can be a key driver of inappropriate behaviours. Previously there had been issues raised by BoI Internal Audit about non-compliant schemes for Specialists. We have regularised the specialist schemes, and there is now appropriate governance in place. Scheme payments for Specialists are approved by FS Risk.

41. All schemes have relevant compliance gateways in place to mitigate conduct risk. We have also mitigated the risk of local incentive schemes in the CRM population through additional certification and training of Postmasters

Remuneration-key actions

42. The Post Office Sales Director is reviewing all network incentives schemes to ensure they drive and reward appropriate behaviours. Initial findings Are expected by the end of October 2016 (changing the schemes is likely to require trade union dialogue).

Communications

43. There is an existing FS Risk and principal review and sign off process for all customer related communications. In addition an effective process has been developed for social media monitoring 'robo monitoring' and an internal process has been put in place to monitor 'chatter' communications (chatter is the internal facility for specialists, management and product managers to communicate with each other informally over the intranet). The FS Risk team review non-standard communications through the recently established FS Risk inbox.

44. Overall there have not been any significant financial promotions or other breaches. There are inevitably 'one-off' inappropriate communications that are picked up through monitoring and these are reported as breaches to the Principal.

Communications-key action plans

45. To simplify the Regulatory Guidance Manuals into easier to read compliance guidance and to agree the process to own and update Horizon help screens.

POL00400101

People

46. The key focus here is whether objectives and people management are in line with good conduct risk principles? Secondly are staff 'fit and proper'?

47. The updated Post Office 'Employee and Agents Vetting Requirements' Policy v11 was approved in June 2016. This will improve HR vetting standards particularly in respect of reference and credit checking (all roles are currently CRB checked). The Post Office revised 'Speak up' Policy was approved by Post Office ARC on 18th May 2016.

People-Key action plans

48. The FS Risk and BoI Monitoring teams have recently reviewed the processes for Fit and Proper on-boarding for Mortgage Specialists and their managers. A number of concerns have been raised about the on-boarding/vetting team being able to evidence the checks that have been made on specialists. FS Risk is working with the on-boarding team on the action plan to improve controls in this important area.

49. It is expected that HR will implement the wider staff vetting policy by December 2016.

50. Network to implement conduct risk objectives for staff. Owner Sales Director (October 2016). Corporate Services to make amends to and re-launch 'speak up' policy (October 2016)

Risk Management

51. Significant new business initiatives, products or distribution methods are risk assessed from a conduct risk perspective. There is an existing customer detriment risk assessment process (annual review just completed) that Bank undertakes. The FS Risk team has overseen risk assessment of CRM phases 1-4, tablets in network, sales force de-tokenisation, mortgage lead champions, customer digital journey etc.

Risk Management-Key actions

52. This is now business as usual for FS and the FS Risk team. Current work is focused on FCA cash savings remedies to implement regulatory requirement. Owners: Savings Product teams, supported by BoI Compliance and FS Risk (November 2016)

Management Information

53. There is robust MI for specialists and CRMs. There is a Quality of Sales MI (QoSMI) dashboard for the remainder of the network, this covers 'watch list' information sales spikes, cancellations and complaints. We have re-launched the QoSMI list with the network and re-iterated that we expect it to use this information as part of its management control.

POL00400101

Management Information-Key actions

54. More work is required to ensure that compliance MI is used across the network, beyond the Specialists/CRM populations to mitigate risk. It has been recognised that the QoSMI could be improved to make it easier to use/filter and to merge the 'watch list' with the complaints report.

55. It is anticipated that the MI improvements will enable the FS Risk team to be more pro-active in monitoring and taking action on potential conduct risk issues. Owner Network and FS T&C team (October 2016)

Other risk issues

Network partners and regulatory authorisation.

56. As part of network transformation it has been identified that there is a risk that agency partners could have either regulatory permissions directly or are acting as an Appointed Representative of another regulated firm. This is in breach of the Financial Services and Markets Act requirements that state that a firm cannot be both authorised and an AR of another firm and there are particularly regulatory permission restrictions on having more than one AR relationship.

57. It is Post Office policy that it will not enter into any network contracts with operators who are directly authorised or appointed representatives. However, the regulatory status of our agency partners can change and where this happens we require that the partner either:

    - Novates their contracts to another entity that is not directly authorised or an appointed representative
    - Contractually carve out Post Office FS products (which are BoI and POMS products)
    - Terminate contracts with operators.

58. The Post Office Legal team are in contact with our Principals with regard to communicating the latest status on this issue.

Jonathan Hill
Head of FS Risk

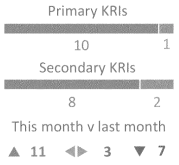
September 2016

POL00400101

Post Office Money branch distribution

How we performed against our aims in August 2016

Our aims describe how we will meet our FACE Customer Charter commitments and promises. Using a range of key risk indicators, we measure our performance against each of our aims. This tells us how well we're doing against our targets and highlights areas where we could improve our performance. We also use our performance to give ourselves an overall risk rating. This month, we rated our overall performance as Amber. Finally, the risk ring shows the relative ratio of green, amber and red rated key risk indicators.



Our customer charter	Our aims	Our performance			
Our commitments and promises	**How we meet our commitments and promises**	**We use a range of key risk indicators to measure our performance against our aims and to highlight areas where we need to improve**			
		How we measure ourselves	Our targets	How we're doing Jul-16	Jun-16
Fair - you are at the heart of everything we do	We provide information and advice that our customers can rely on	We use **mystery shoppers** to test how well our staff are meeting our conduct risk requirements and our customer's needs	Fewer than 20% of mystery shops are rated red in the quarter	**10.8%**	12.2% ▲
			No shops are rated black in the month	**0**	0 ◀▶
			Fewer than 10% of our Specialists have more than one red or black shop in the preceeding six months	**0.9%**	0.8% ▼
		Our Quality Assurance Team assess the **quality of the mortgage advice** we give customers to ensure it's suitable to their needs	At least 80% of cases are rated A or B by the QAT in the month	**93%**	91% ▲
			Fewer than 5% of cases are rated D by the QAT in the month	**1.1%**	2.3% ▲
			At least 85% of MSs meet the QAT benchmark in the month	**91%**	86% ▲
		We use branch reviews and monitor breaches to ensure our **financial promotions** are compliant and up to date	90% or more of our branch reviews are rated green or amber for financial promotions in the quarter	**97%**	100% ▲
			We record fewer than 11 material financial promotions breaches in the quarter	**0**	1 ▲
	We do our best to get things right first time and act quickly to put it right if we don't	We monitor customer **complaints** to understand what we're getting wrong and why, and to ensure we get it right in the future	We uphold fewer than 21 significant complaints for every 1,000 products we sell	**1.14**	0.94 ▼
			Upheld complaints grow no more than 21% faster than sales	**19%**	-5% ▼
			Upheld significant complaints increase no more than 21% month-on-month	**6%**	10% ▲
Accessible - we provide a friendly, efficient and reliable service	We listen to our customers and act when they tell us we could do things better	We use **customer feedback** to tell us whether we met their needs at the point-of-sale	At least 90% of compliance survey questions confirm customer's needs and compliance standards are met in the quarter	**96.5%**	96.4% ▲
			At least 90% of NPS surveys confirm customers receive the information they need in the quarter	**98.2%**	97.4% ▲
Committed - we aim to build long-term relationships	We have staff with the requisit levels of skill, knowledge and expetise	We use the results of **knowledge tests** to ensure our staff have the skills, knowledge and expertise to meet our customer's needs	At least 80% of BOI product knowledge reviews are rated green or amber in the quarter	**100%**	100% ◀▶
			At least 80% of BOI regulatory awareness reviews are rated green or amber in the quarter	**100%**	100% ◀▶
			Specialists pass at least 80% of POL knowledge tests in the quarter	**99.2%**	99.2% ▼
		We monitor our **training and competence** arrangements to ensure staff are maintaining their competence and are being adequately supervised	At least 80% of Specialists are signed off as fully competent	**87.3%**	87.8% ▼
			At least 80% of FSAMs are within agreed spans of control	**96%**	100% ▼
			At least 80% of BOI FSAM reviews are rated green or amber in the quarter	**96%**	100% ▼
Easy to do business with - we promise to keep it simple and straightforward for you	Our products are easy to understand and meet customer's needs and expectations	We monitor the **retention and use of our products** by customers to ensure they meet their needs and expectations	Customers cancel no more than 1.5% of savings products in the cooling-off period	**0.76%**	0.75% ▼
			No more than 40% of credit cards remain unused after the first six months	**29%**	29% ▲

▲ Performance improving from previous month ▼ Performance worsening from previous month ◀▶ Performance unchanged from previous month

POL00400101

4) Cyber Security and Information Assurance

Author: Rob Houghton Sponsor: Jane Macleod Meeting date: 28 September 16

Executive Summary

Context

1. Post Office's current information security operational model was designed in 2013 in light of the then proposed stand up of the Towers supplier model. Under this model, Atos was expected to be responsible for managing each of the 4 tower suppliers (Computacenter for EUC, Verizon for Network, Accenture for Back Office and IBM for Front Office). Each tower supplier would then manage a further chain of sub-suppliers. The Post Office Information Security Team was therefore responsible for setting policy and managing risk and assurance around this structure, rather than managing individual suppliers.
2. As has previously been discussed at the Board, the Towers model has not been fully stood up: particularly as a result of the decision taken under Trinity to terminate IBM and extend and modify the existing Fujitsu contract. In parallel, Atos' role in managing the towers structure has also never been fully implemented. Accordingly, the original information security operational model is no longer fit for the current and planned structure of the Post Office IT infrastructure.
3. Following the appointment of the new CIO (Rob Houghton) and with the recent articulation of the IT strategy, it is now possible to reconsider the appropriate information security operational model. Deloitte has recently undertaken an BTA audit (see appendix 1) and taken together with the new CIO's observations, an action plan has been agreed.
4. This report considers the risk to Post Office information, in any form via any medium, with respect to the confidentiality, integrity and availability of that information.

Questions this paper addresses

- What data does Post Office control?
- What are the current top information security risks to Post Office?
- What actions can we take to mitigate those risks and bring them within appetite?
- What are the risks in the meantime and how do we manage them?

POL00400101

Conclusion

5. Post Office is dependent on a largely outsourced model under which each supplier is responsible for the security of data within its domain. This includes 'Personal Data' (as defined under the Data Protection Act), as well as financial and transactional data owned by both Post Office and its clients. As a consequence Post Office directly holds very little third party data.

6. Despite the delay in standing up the Towers model, Post Office has implemented management controls around the most significant suppliers – being those that pose the greatest risk to Post Office from a data security perspective. There have been no known material data losses (including losses of Post Office or client data) by Post Office or its IT suppliers for over 3 years.

7. Nevertheless we remain outside of risk appetite in three key areas:

    a. The ability of anyone internally to be able to share, download of exchange data without any monitoring controls

    b. The ability to predict, detect and respond to cyber security events across our end to end environment

    c. The ability to assure ALL our end to end network of suppliers is maintaining a robust security profile and providing the minimum level of safety on our data and assets.

8. As outlined in the revised IT strategy it is important that Post Office implement the appropriate tools to enable it to predict risk, detect intrusion and respond to cyber security events to an acceptable standard given the business strategy and nature of Post Office's suppliers and clients. These have also been identified as part of the Deloitte review with an action plan agreed between ISAG and IT. It is expected that, subject to funding and prioritisation, the design and implementation of any project to begin to deliver minimum level of protection, prevention, and detection tools will take at least 6 months to implement and will be 6-18 months to get to a mature state.

9. Looking forward, since most of the data we collect is made up of personal data (including information that can identify an individual) forthcoming regulatory changes in the form of General Data Protection Regulation (GDPR), coupled with the newly adopted Network and Information Security Directive (NIS) (July 2016) will have a significant impact on our business. NIS and GDPR interlink and support each other and will determine, among other things, how we and our third parties monitor and report on threats, incidents and breaches to our IT network, the timelines in which we report breaches/incidents and how we collect and process personal information.

Input Sought

ARC is requested to note this paper and support the recommendations within, requesting an update in January.

POL00400101

Report

What data does Post Office control?

10. Post Office's outsourced model means that in today's environment, it directly holds very little third party data. However data passing through Post Office systems (including those operated by third parties/outsourcers) includes:

    - Transactional and customer data collected in branch through Horizon, through online transactions, and via call centres all of which is held by the third parties providing those services. This data includes transactional and financial data, as well as personal data.
    - In addition, this data is held in both "open" form and pseudonymised in Credence and MDM data stores for analysis purposes. Data is extracted and managed through a variety of analytical and MS Office tools for manipulation.
    - Data held on Common Digital platform from customer journeys through basic transactional services.
    - Post Office's own data (eg employee information, financial records etc) which is also held through third party products such as SAP etc which are in turn hosted by outsourcers such as Fujitsu and Accenture. This data is extracted and managed through many different MS Office tools (Excel/ Word) to provide Management information and data.

11. Post Office's outsourcers are subject to contractual provisions regarding data protection, information security and business continuity. Recent contracts adhere to Post Office's contractual house position, whereas older legacy contracts may not have up to data protections.

12. Depending on the nature of the data or the platform though which it is accessed, these contractual frameworks may in addition stipulate encryption or other enhanced security measures for both data in transit and that held by the outsourcer.

13. Post Office's Information Security Assurance Group ('ISAG') adopt a risk based approach to identify the 'Top 20' contracts being those which pose the greatest information security risk to Post Office, and those 20 suppliers are subject to an enhanced level of oversight by ISAG, including penetration testing.

14. Under certain contracts with government clients, Post Office is required to undergo regular audit and certification processes and has therefore been able to demonstrate compliance with the frameworks required for ISO 27001. Certification.

What are the current top information security risks to Post Office?

15. The most likely sources of risk to Post Office are:

    - Internal risk posed by colleagues (employees, contractors, suppliers) who have access to Post Office systems and information/data and are therefore able to share, download and exchange data without any monitoring or controls. Risks to an organisation's internal data are considered to increase during periods of significant change. This risk is exacerbated as remote access increases and

POL00400101

extension of 'bring your own device' technology. At present Post Office has no technical ability to detect or monitor data leaving our environment.

- Breach by, or failure of, outsourcers or others within our IT supply chain. The complexity of the legacy IT supply chain, the increasing risk associated with the evolving threat landscape and the sheer logistics of managing multiple suppliers, suggests that both the likelihood and impact of an incident are increasing. Post Office is dependent on suppliers to report loss and near miss incidents, but without appropriate IT tools in place, we are dependent on the provision of that information to understand the risk to Post Office data.
- External risk – Cyber Criminals/Hackers; the external threat across industry is increasing; Post Office is no exception, although we are yet to be recognised as a high profile target. However our increased footprint into Financial Services (FS), as an example, will heighten Post Office's profile in the hacking community.

16. In each case, the consequences to Post Office of any of these risks crystallising would include:

- Reputational and brand damage through loss of trust from customers, suppliers, clients, business partners (potential and current), employees, and shareholder.
- Direct financial loss caused by regulatory breach or contractual failings.
- Regulatory sanctions or fines levied by the Information Commissioner, and/or or by the FCA (in the case of loss relating to customers of FS products).
- Compromise of, or loss of integrity of personal data; and loss of intellectual property, or proprietary commercial and/or financial data.

17. Post Office does not currently have the ability to predict, detect and respond to cyber security events across the end to end environment, however the implementation of such a capacity is part of the Post Office plan to rectify these weaknesses.

18. Post Office has recently commissioned an assurance review from Deloitte in relation to its cyber security risks. The executive summary from that review is attached in appendix 1 (as well as included in the Internal Audit update paper). The review recognises that the operating model under which Post Office has been operating was designed for a different operating structure. Accordingly it has not been possible for Post Office to address a number of the recommendations set out in the 2013 Deloitte report. Post Office management agrees with the findings. Deloitte is supportive of Management's proposed action plan, confirming that it responds appropriately to its findings.

What actions can we take to mitigate those risks ?

19. We recognise that risk mitigation requires people, process and technological interventions, as the greatest threats are often a complex combination of people and technical risk. We will continue to develop our existing information security framework, but introduce technological controls along with the existing and evolving management controls to cohesively protect Post Office.

20. The development and implementation of the Post Office IT strategy will include upgrading the necessary systems and capabilities to enable Post Office to have better oversight of its security risks; this will include investment in both Post

POL00400101

Office's IT Security, people, additional capability and tools. In particular, the following have been identified as a priority for the next 180 days:

- recruitment of a security operations lead reporting into the CIO;
- enhancement of current identity and access management including enhanced joiner/mover/leaver controls;
- Data loss prevention tools and enhanced monitoring; and
- Establishment of a security operations centre to facilitate more effective oversight of key suppliers.

21. Governance in respect of information security also needs to be enhanced. At present the Information Security Forum meets bi-monthly, however attendance needs to be reviewed and strengthened, and reporting through to the Risk & Compliance Committee and ARC needs to be regularised.

22. With the General Data Protection Regulations coming into effect in May 2018 and the Network and Information Security Directive following almost immediately further training and understanding of data protection and information security requirements need to be embedded across Post Office.

How do we manage risks in the meantime?

23. Post Office has an Adverse risk appetite for any serious impact to the confidentiality, integrity and availability of information leading to financial loss, business disruption, public embarrassment or legal consequences. There have been no known material data loss incidents over the last 3 years.

24. Pending full implementation of these initiatives, we acknowledge that we are outside of risk appetite. The information security risk framework provides a level of assurance based on a combination of tools to manage and monitor risk in the current environment (detail is set out in Fig 4). These include:

    - reliance on IT suppliers to properly protect systems and processes used to transmit, store and process Post Office data. Due diligence is undertaken on prospective suppliers via on-site visits and/or Supplier Questionnaires; and contractual protections are built into new contracts using the Post Office House position which reflect industry good practice including contractual assurance rights (technical and non-technical testing and forensics in the event of a breach).
    - risk assessment of those suppliers which represent the greatest information security risk to Post Office; ISAG have regular meetings with 'Top 20' suppliers to monitor their compliance with requirements and understand any new risks that affect our business. Figure 1 at the back of this report, provides an update on the assurance reviews conducted on the Top 20 since March 2016; and
    - assessment of developing cyber threats at least weekly using security industry intelligence; these are reported internally and externally to suppliers and management (see risk log of current threat exposures as set out in Figure 2).

25. Post Office is regularly and successfully externally audited as part of certifications to leading industry standards such as Payment Card Industry Data Security Standard (PCI DSS) and ISO 27001, the Information Security Management System International Standard, and by partners and client (new and existing).

POL00400101

26. The emerging business strategy, the effect of the both the General Data Protection Regulations (GDPR) which are due to be fully implemented in the UK by May 2018, and the adoption by the UK of the Network and Information Security EU Directive (NIS) will require Post Office to substantially enhance its capability in this area this is subject to acceptance of Corporate Services proposed projects.

Next steps

27. The IT Strategic Plan will continue to develop along the core principles presented to the Board in [July] 2016. Implementation of these principles is addressed through Post Office's project prioritisation framework, however it is expected that, subject to a suitable business case being approved, these proposals will be approved and delivery should be from mid-2017.

POL00400101

Figure 1 – Top Twenty Suppliers and Status Report

Penetration testing of Suppliers (by third parties) on behalf of Post Office:

- 8 suppliers have been tested in last 12 months – Contractual.
  - Fujitsu (Horizon)
  - Accenture (CDP)
  - Computacenter (EUC Admin Tower)
  - NCR (SSK)*
  - Salesforce*
  - HPE (POca)*
  - BOI*
  - FRES*
- 6 suppliers on schedule for re-testing in next 6 weeks – Contractual.
  - Accenture (Back Office)
  - Fujitsu (PODG)
  - CSC (Safe Haven)
  - Digidentity (Verify)
  - 3M Cogent (AEI)
  - RAPP (Brands)
- 4 new suppliers – Scheduling planned for on boarding process as services become available and live – Contractual.
  - BT Airwatch (MDM Infrastructure)
  - Verizon (Network)
  - Computacenter (EUC Branch)
  - Accenture (Credence/MDM)
- 2 suppliers off-boarding – Scheduling planned for on boarding process as services become available and live – Contractual.
  - CGI (MDM)
  - CGI (Credence)

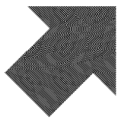
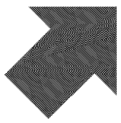
Risk assessments taking place to replace exiting suppliers on list and schedule testing.

*5 suppliers undertake their own testing (by third parties) to an ISAG agreed scope and verification – Contractual.

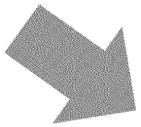
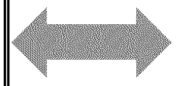
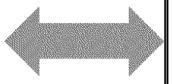
POL00400101

s

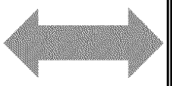
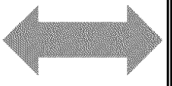
Figure 2 - Threat Landscape Indicators

Threat	Threat Group	Origin	Threat Priority	Assessment	Risk Indicator
Employee (general)	Adversarial	Internal	High	Increased unrest within the Unions as a result of job losses within Post Office and failure to secure suitable assurances for their membership, could motivate opportunist attacks where the correct security behaviours are lacking. Poor security controls within the EUC environment coupled with a lack of technical measures to prevent and detect non-compliance, increases likelihood of successful compromise by this threat group	
Employee (privileged)	Adversarial	Internal	High	Increased unrest within the Unions as a result of job losses within Post Office and failure to secure suitable assurances for their membership, could motivate opportunist attacks where the correct security behaviours are lacking. Poor security controls within the EUC environment coupled with a lack of technical measures to prevent and detect non-compliance, increases likelihood of successful compromise by this threat group	

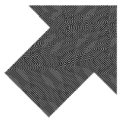
POL00400101

Threat	Threat Group	Origin	Threat Priority	Assessment	Risk Indicator
State Sponsored	Adversarial	External	High	Post Office is considered the 'thin skin' of Government, delivering services, but with less robust IT security infrastructure in place. We would be a softer, easier target to those considered hostile to UK Interests. As a result of BREXIT, the likelihood of such an attack has risen to MODERATE as some countries may seek to exploit UK Government instability; the threat strength remains HIGH. However, as the new PM sets out a new agenda the threat will reduce.	
Employee (general)	Accidental	Internal	High	Employees (to include contractors, Postmasters and their agents) making mistakes or non-compliance with Acceptable Use Post Officeicy remains the highest risk group to Post Office	
Employee (privileged)	Accidental	Internal	High	Employees who have increased account privileges making mistakes or failing to follow procedures are still considered a HIGH risk to Post Office. This includes Sharepoint site administrators and managers who fail to implement the correct JML process	
Competitor	Adversarial	External	Moderate	Whilst our competitors are deemed unlikely to target Post Office, their past history, capability and commitment presents them as a MODERATE risk group	
Customer	Adversarial	External	Moderate	There have been occasions where customers with grudges against Post Office have mounted attacks, however these have been maverick attackers, with low level skills which are	

POL00400101

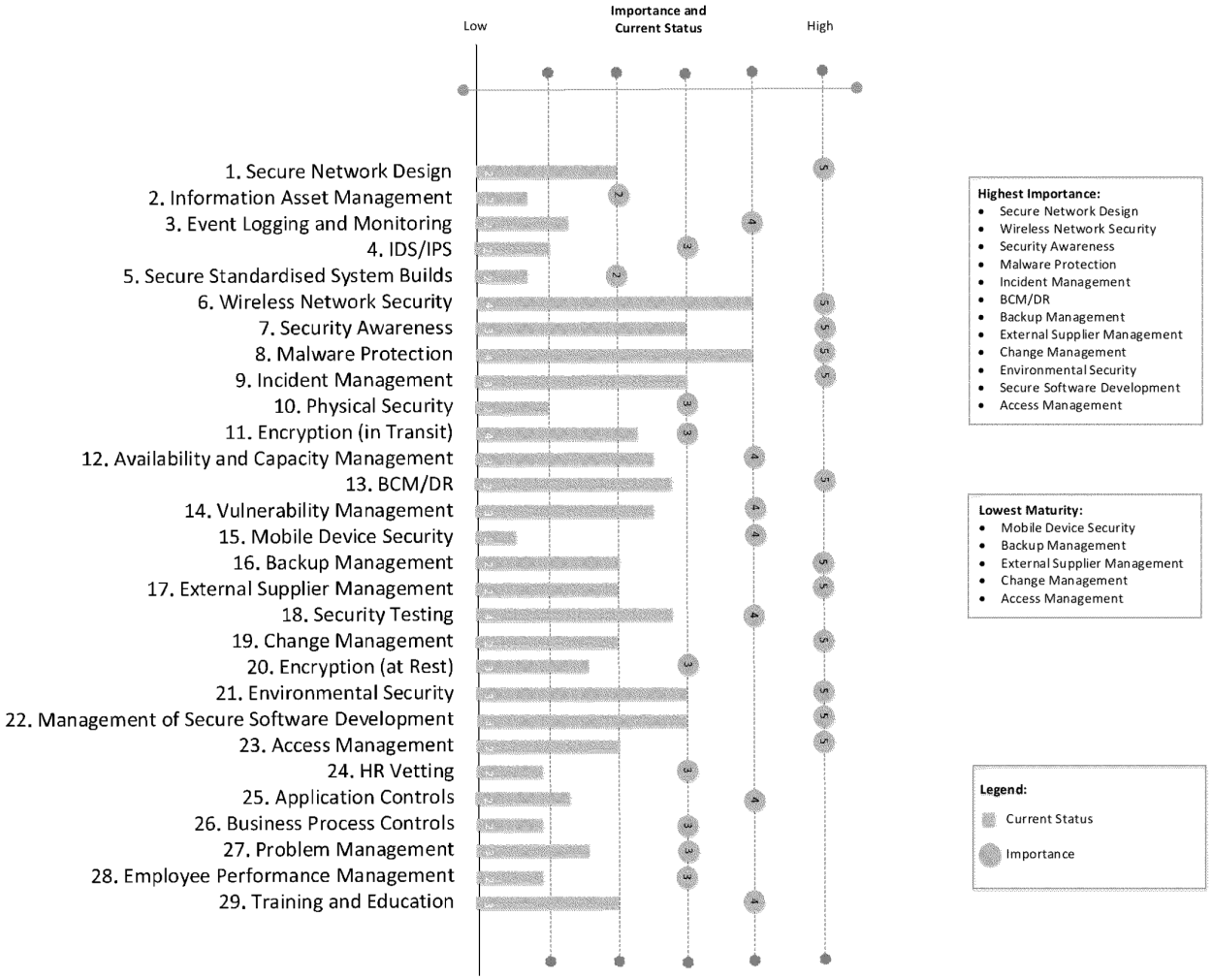
Threat	Threat Group	Origin	Threat Priority	Assessment	Risk Indicator
				relatively easy to contain and control	
Hacking Group	Adversarial	External	Moderate	Whilst Post Office deflect 95% of emails sent to our corporate system, phishing remains a very credible threat to Post Office. Malicious payloads, delivered to and activated by users may enable hackers to access data. The threat from this group remains MODERATE, however, the Financial Sector is currently being targeted by Anonymous are part of #OpIcarus.	
Individual Hacker	Adversarial	External	Moderate	Whilst Post Office deflect 95% of emails sent to our corporate system, phishing remains a very credible threat to Post Office. Malicious payloads, delivered to and activated by users may enable hackers to access data. The threat from this group remains MODERATE, however, control measures are in place to minimise the risk	
Organised Criminal Group	Adversarial	External	Moderate	The threat from Organised Criminal Groups, remains a MODERATE. Ransomware attacks are on the increase across several industries and the relative ease and anonymity of payment via BITCOIN makes it difficult to investigate	

POL00400101

Threat	Threat Group	Origin	Threat Priority	Assessment	Risk Indicator
Supplier/ Partner	Adversarial	Internal	Moderate	Given the increased unrest within the Unions, and ongoing legal action related to Sparrow, there is an increased risk that maverick supplier/partner employees may be motivated to target Post Office	
Supplier/ Partner	Accidental	External	Moderate	On occasion, mistakes or non-compliance within the supplier/partner environment, have occurred therefore they remain a MODERATE risk to Post Office	

POL00400101

Fig 3 - Controls Matrix



POL00400101

Appendix 1: extract from Deloitte Information Security Assessment review, Sept 2016

The Information Security Assessment has been awarded an overall risk rating of:	Adverse

Executive Summary

As with many organisations, Post Office has been facing substantial challenges around its information security landscape, but particularly as it attempts to implement its 2020 strategy. Developing revenue from delivering financial products means increasing and extensive regulation regarding cyber. Transformation will result in progressively capable digital platforms on new potentially untested digital technology which is provided by a large number of suppliers. Services increasingly accessible around the clock will require more resilient operations. As a key partner to government for the delivery of official services, the impact of any breach would be significant to the Post Office's reputation. As such the Post Office is exposed to significant cyber security risks, which will continue to grow over the coming years.

The information security operational model Post Office has been using was designed for an anticipated Towers supplier model. In consequence ISAG was set-up to act as an overseeing governance body to manage information security risk based on this blueprint of having services delivered through a range of third parties, with an overarching Systems Integrator to manage this as well as performing a variety of security operations. However this operating model has not proved possible to implement and has since been changed. As such many security operation activities have fallen to an assurance group not staffed, tooled or accountable to do this. In addition, changes to the CIO in recent times has naturally disrupted progress in addressing IS issues. In response to these changing circumstances, mitigations have been put in place and risks have been raised to the governance committees. It should be noted that during this time no material data losses have been recorded. In addition, Post Office has obtained and maintained compliance certification for PCI-DSS and ISO27001 for various systems.

Notwithstanding this, from our review of controls, we have identified several interrelated findings which indicate that these risks are not being managed appropriately and that controls are behind in maturity to where we would expect them to be. Three critical findings (i.e. fundamental to the Post Office) and five significant ones (i.e. for the attention of senior management) were raised in this review. Many of the findings have been raised in previous reports (external and internal) and have not been fully addressed.

Moving forward we support management in reviewing and addressing important cyber security operational controls both those operated by the Post Office and its technology suppliers. Elements of this have been included as part of the revised IT Strategy. As a priority this should include remote access, network monitoring, completion of penetration tests and incident reporting along with the processes associated with access to critical systems and applications. In addition, accountabilities/ responsibilities around cyber security should be reviewed. This should include those regarding third parties, which is currently unclear, as well as considering the balance between assurance and operational security activities. Deciding on the most appropriate reporting line for ISAG and ensuring a fit for purpose system is in place for managing security risks with the transformation programmes will also be important.

POL00400101

Key Findings

- Remote access controls (including usage of Office365 and single sign-on for access to multiple systems) are not configured in line with good practice. Leavers are not being removed in a timely manner and no data leakage technology is implemented. All of which increases the risk of the loss of sensitive data.
- Penetration tests of some critical infrastructure has not been completed or remediated in line with policy.
- The responsibilities of the ISAG have increased significantly over recent years to support the 2020 change strategy and increasing cyber security risk. However, ISAG remain under resourced and consequently are unable to fully deliver their current remit.
- Supplier contracts typically define some requirements for security operations. However, suppliers are not reporting security incidents to Post Office staff in a timely or consistent manner.
- Information security engagement into business transformation projects is ad-hoc and reliant on the security awareness of the relevant project management.
- Security policies have been re-written and restructured into a comprehensive set of policies, frameworks and standards (including how data is classified). However, they are yet to be fully adopted and embedded into the business and appropriately assured.
- Lack of timely action in response to findings raised in a 2013 review of Information Security, of which many have been included in this review.

Conclusion

Overall, we identified several material findings in this review, but we also noted that the Post Office have agreed action plans related to each of these findings. Many of these are based on the updated agreed IT Strategy. Plans include budgets for the implementation of a range of technologies and associated processes to manage security operations; completion of outstanding penetration tests; updating security assurance processes and reviewing accountabilities for all aspects of information security. Successful, timely implementation of these is fundamental to ensuring cyber risk is managed appropriately and controls are of sufficient maturity for an organisation such as the Post Office, with the 2020 strategic ambition. Action will be required by all senior business leaders as well as IT and ISAG.

Critical to the success of any Information Security strategy is building a resilient culture of cyber awareness and behaviour throughout its business structures and operational practices. The Post Office has started this journey, but we feel that further focus is needed in this area. Cyber security is a business risk and requires action by all staff as well as ownership and leadership by business management in addition to IT and assurance.

POL00400101

5a) Risk Update Report

Author: Mike Morley-Fletcher Sponsor: Jane MacLeod Meeting date: 28 September 2016

Executive Summary

Context

This paper updates the ARC on progress against the project plan for developing POL's Risk Framework, in particular how we have been developing POL's Group Risk Profile, General Control Environment, Assurance Mechanisms and Corporate Governance capability.

Questions this paper addresses

1. What has been the primary focus since the last ARC?
2. What else has been progressed?
3. Is implementation of the Risk Framework on target?
4. How is our resourcing?

Conclusion

1. This period has been primarily focused on working with GE Risk Owners (with assistance from their Risk Champions) in completing a half year refresh of their Top Risks (descriptions and evaluations) and update of Key Further Actions. Full details of proposed changes are provided in a separate paper (5b): suggested changes have been marked up on the Group Risk Profile.

2. In addition we have:

   - considered the ARC's request for providing additional information of a more immediate nature, **"risks of the moment"**. Following discussion with the CEO we would like to trial drawing on the risks identified in the CEO's Report to the Board (under headings of "what has not gone well" and "risk and concerns"). This would supplement the more medium term view provided by the GRP. The details of the current "risks of the moment" are included in the GRP paper 5b.

   - worked with P&E to update **GE job descriptions** with an accountability to manage risk, as follows: "to identify, document and agree actions with accountable owners to mitigate risks across all risk types within own Function, and contribute to identification and risk management cross functionally, ensuring compliance with the Post Office's risk management framework".

   - agreed with GE members that members of the Central Risk Team will attend **quarterly leadership meetings** with business areas to assist with their risk assessments, including expectation to facilitate at least one risk workshop a year.

POL00400101

- continued our review of our **Risk Appetite Statement** (per draft approved by Board on January 2015) and the establishment of measures, "key risk indicators", and "tolerances". Our approach is to road test our approach firstly with Business Transformation risks, before investigating how this can work for other Top Risks and business as usual, operational risks.

- started to review our approaches to approving and recording **"material" risk exceptions**, including policy exceptions, looking to standardise and consolidate them. These are also referred to as Risk Acceptance Notes. This will support use of our Risk Appetite Statement.

- progressed our work on **Business Continuity** capability (Major Incident Management Procedures tested via a Cyber Breach exercise) - see separate report 7b.

- progressed our work on **Key Policy** drafting: a further 5 policies for approval and policy intranet site starting to be populated, with communications to follow shortly directing colleagues to this and encouraging them to complete any relevant training see separate report 8.

- continued developing our mechanism for **self-assessment** of the **General Control Environment** and **Financial Reporting controls**. Implementation of control self-assessment is continuing per schedule with software introduced to make this activity more efficient to report, action and evidence. Internal Audit are developing an approach to provide an independent review over the process and check self-certifications on a sample basis. Our aim is to provide management and the ARC with enhanced, systematic assurance information for year end March 2017.

- organised, on a similar basis to 2015/16 year end's, a half year **Executives' Declaration** return for completion by General Executive members. This will ensure there is refined guidance on reporting requirements to ensure all material, non-previously disclosed items are considered and disclosed appropriately. The return has been further enhanced to incorporate lessons learnt at the initial dry run and new exposures such as contract obligations.

- clarified with the Chair of the ARC that if we are not looking to follow the UK **Corporate Governance** Code, we do not currently need to develop a Route Map to Corporate Governance Compliance. However, we will review this decision on an annual basis at the half year, next due September 2017.

3. We are using the high-level project plan, see appendix 1, to guide our workplan adapting as we operationalise it to business needs, colleague availability and our own resource capacity. For instance development of the Assurance Map has been moved further back to the second half of the year as we spend more time on the General Control Framework and self-assessment mechanisms. Next quarter the Central Risk Team will progress the Risk Appetite project and bring some worked examples to the ARC to review.

4. We are structured with 2 Business Risk Partners and 1 Risk Senior Manager, working with other risk professionals in Business Transformation and POMS, supported by the network of Risk Champions. The senior manager role was filled by a consultant who left earlier in the year. We have been unsuccessful

POL00400101

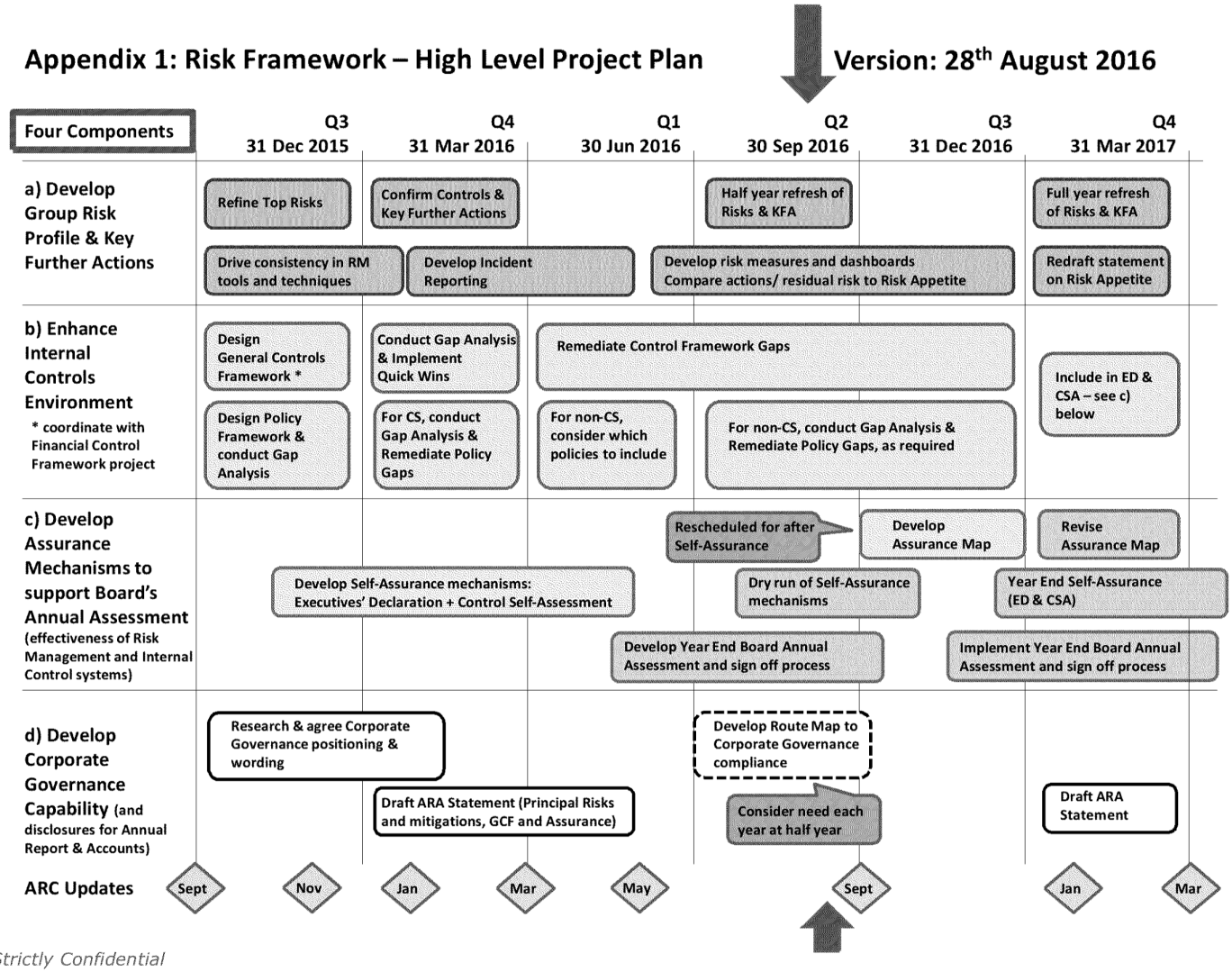
in finding the right quality candidate through our own research and so now will invest the savings we have made by not employing someone for a while to recruit. We have recently secured the services of an ex-colleague to cover the senior manager risk role on a temporary basis whilst we recruit.

Input Sought

The Committee is asked to review the attached papers and provide feedback, support and approval as appropriate.

POL00400101

Appendix 1 – Risk Framework project plan



POL00400101

5b) Group Risk Profile – 2016/17 Half Year Review

Author: Mike Morley-Fletcher Sponsor: Jane MacLeod Meeting date: 28 September 2016

Executive Summary

Context

At the half year the RCC conducts a full review of the Top Risks (descriptions and evaluations) and associated Key Further Actions.

Questions this paper addresses

1. How was the Half Year Review conducted?
2. What changes have been suggested?
3. What is the impact on the Top Risks?
4. What are the key "risks of the moment" from the CEO's perspective?

Conclusion

1. The Central Risk Team has interviewed all the GE Risk owners and their Risk Champions to assist them in completing a half year refresh of their Top Risks (descriptions and evaluations) and update of their Key Further Actions. On 8th September the RCC approved the updated Group Risk Profile (see appendix 1, tab 1) and Key Further Actions (see appendix 1, tab 2a for a summary, 2b for details). These are now presented to the ARC for review. Movements since last quarter have been shown by black solid arrows, and white "target" dotted arrows have been removed as the detail is contained in the chart.

2. Full details of proposed changes are provided overleaf. Suggested changes, for the ARC to consider, have been marked up on the GRP in red font and include the following:

    - 6 changes to risk titles and descriptions
    - 0 new risks or risks removed
    - 7 risks with increases in their net evaluation (most significantly Pension Costs and Government Funding)
    - 4 risks with decreases in their net evaluation (most significantly Industrial Relations).

    GE risk owners were asked to consider the effect of Brexit on their risks and this was most apparent for 1) Pension Costs, 2) Government Funding, 12) Market Developments/ Competition (non-FS) and 12) Market Developments/ Competition (FS).

POL00400101

3. Overall the total number of risks remains at 27, however the number of Top (i.e. red risks) has increased from 15 to 18, as Brexit uncertainty and trading pressure have accentuated our concerns for achieving our targets. Key Further Actions have been captured for all Top Risks.

4. Key risks of the moment are reported to the Board by the CEO in the CEO's Report. They are summarised here for the information of the ARC. Note: due to advance production of the ARC papers, there may be some differences with the risk disclosed in the Board papers. These risks were as at 22nd Sept 2016. They include:

    - Pensions (GRP 1, Neil H) – the Pensions Trustees meet next week to consider our proposal to close the defined benefit pension scheme to future accrual. We hope that they will be in a position to reach a decision which would allow us to provide certainty to colleagues.
    - Industrial Relations (GRP 7, Neil H) – talks with the unions continued at ACAS on 21st September, but without resolution. Further industrial action is anticipated.

Input Sought

The Committee is asked to consider the proposed changes, suggest any further changes as appropriate and approve the 2016/17 Half Year Group Risk Profile.

POL00400101

2016/ 17 Half Year Group Risk Profile Review - Summary

5. For the Half Year Group Risk Profile Review GE members (and their Risk Champions) have been interviewed by the Central Risk team to refresh their Top Risks (descriptions and evaluations) and update their Key Further Actions. Suggested changes have been marked up on the GRP (see appendix 1) in red font and include the following:

a) Changes to risk titles and descriptions (6)

- 2) Government Funding, addition of "Headroom" to title and description in recognition that our balance sheet headroom requirements need to be built into strategy and 5 Year Plan development.
- 5) IT Availability/ Ability to Trade, addition of "Ability to Trade" to risk title to clarify the concern of the severity that could occur from IT unavailability and the addition of reference to "supplier/ partner failure" as a cause in the risk description.
- 14) Change Portfolio Delivery, change from "Transformation IT Delivery" in recognition that this should now cover the whole Change portfolio, not just IT programmes.
- 15) FS Regulatory Supervision, included reference to "Fit & Proper staff vetting, agency contracts/ conflicts of interest" as possible additional compliance breaches that could trigger supervision and regulatory requirements.
- 17) Information Security/ Data Protection Breach, addition of "Data Protection" to risk title.
- 22) Commercial Sustainability, change from "Cost Reduction", in recognition that the risk needs to focus on how we use cost reductions and growth developments to steer PO to break even and then commercial sustainability.

b) New risks (1)/ removed risks (0)

- A new risks or risks removed.

c) Increases in net evaluation (6)

Increase to the evaluations of the following risks have been proposed:

- Pension Costs (4/3 to 5/4), due to further deterioration in rates accelerating the reduction of the DB scheme surplus.
- Government Funding (5/2 to 5/3), due to the increased level of uncertainty caused by Brexit, both from a funding availability and a stakeholder perspective, at a key stage in negotiations.
- 5) IT Availability/ Ability to Trade (4/3 to 4/4), due to increasing concerns over the age of some applications, flipover issues, vulnerabilities and lack of testing.
- 6) Transformation Benefits Realisation (3/4 to 4/4), due to benefits originally identified in the business case being eroded by delay in delivery and complexities integrating a POL and Third Party plans (mainly relates to IT change activities).
- 17) Information Security/ Data Protection Breach (3/3 to 3/4), due to an increasing threatening external environment and our move to the higher regulated environment of FS.

POL00400101

- 18) Digital Competency (2/4 to 3/4), due to increasing significance of digital channel, especially to FS's growth targets, and need to recruit successor to current Head of.
- 22) Commercial Sustainability (2/3 to 3/3), due to the size of challenge to breakeven/ sustainability, pressure on performance (FS and Telecoms) and high levels of uncertainty from the external market, political situation and our own industrial relations.

d) Decreases in net evaluation (3)

- 7) Industrial Relations (Transformation) (5/4 to 3/5), due to expectation that any industrial action will be shorter and more limited in scope, plus development of contingency plan.
- 8) Network Proposition (5/3 to 4/3), due to pipe line of retailers and success in maintaining buffer over 11,500 limit.
- 9) People Capability (5/3 to 4/3), due to success with work on the TOM/ organisational design, recent successful key hires and the completion of succession planning exercise.
- 13) Transformation Strategic Alignment (3/5 to 3/4), due to significant work aligning all projects to the strategy direction and mechanisms put in place to monitor this.

6. Overall the total number of risks remains at 27, however the number of Top (i.e. red risks) has increased from 15 to 18, as Brexit uncertainty and trading pressure have accentuated our concerns for achieving our targets. Key Further Actions have been captured for all Top Risks.

POL00400101

Appendix 1 – updated 2016/ 17 Half Year Group Risk Profile

POL00400101

POST OFFICE

GROUP RISK PROFILE - Sept 2016

Version: Updated 21st September 2016

Appendix 1

See overleaf (appendix 2) for Key Further Actions,
(appendix 3) for Harm Table and
(appendix 4) for full list of risk descriptions

Strategic Objectives

Our core business strategy – our path to profitability - is:

- To be the Number One letters and parcels retailer
- To grow financial services
- To be a trusted distributor for our own products and those of others

And, in so doing

- To protect and deepen our social purpose by providing access to these essential services for all communities in the UK.

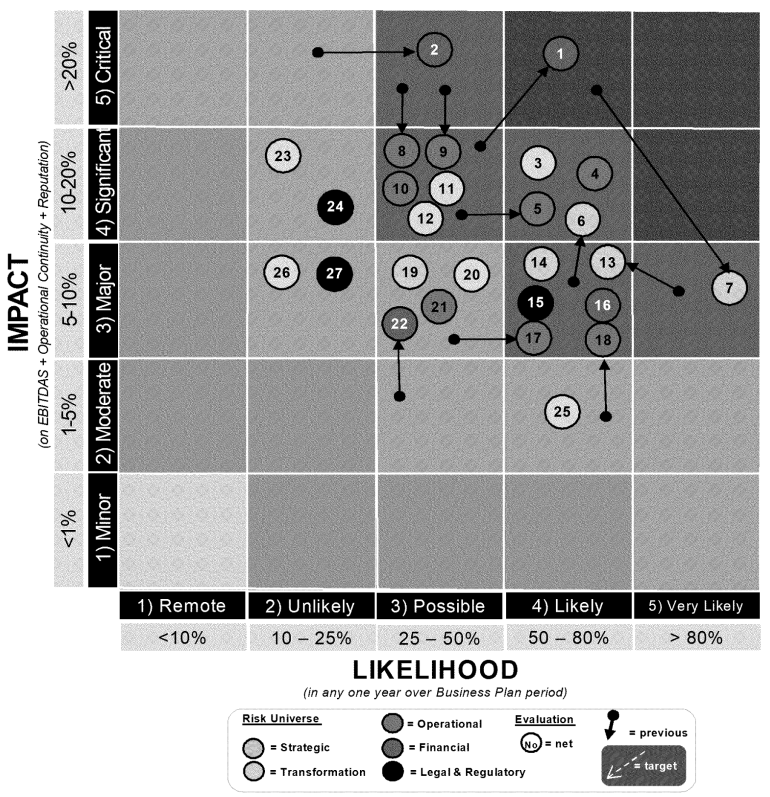
Targets

Achieve EDITDAS breakeven by 2017/18

KEY RISKS

Ref	Title	Owner	Risk Cat	Original (Sep '15)	Change Previous	Previous (Mar '16)	Change This Qu	Net (I/L)	Target (I/ L)
RED RISKS - *for actioning to bring the net evaluation to the target*									
1	**Pension Cost**	Neil H	Fin	3 - 3	Up	4 - 3	Up	5 - 4	5 - 2
2	**Government Funding** and Headroom	Al C	Fin	5 - 2	-	5 - 2	Up	5 - 3	4 - 2
3	**Market Developments/ Competition (non-FS)**	Martin G	Strat	4 - 4	-	4 - 4	-	4 - 4	2 - 3
4	**Third Party Relationship Management**	Jane McL	Oper	4 - 4	-	4 - 4	-	4 - 4	2 - 2
5	**IT Availability**/ Ability to Trade	Al C	Oper	4 - 3	-	4 - 3	Up	4 - 4	4 - 2
6	**Transformation Benefit Realisation**	David H	Trans	4 - 3	-	3 - 4	Up	4 - 4	3 - 3
7	**Industrial Relations (Transformation)**	Neil H	Trans	5 - 4	-	5 - 4	Down	3 - 5	3 - 3
8	**Network Proposition**	Kevin G	Oper	5 - 3	-	5 - 3	Down	4 - 3	4 - 2
9	**People Capability**	Neil H	Oper	5 - 3	-	5 - 3	Down	4 - 3	2 - 3
10	**Customer Experience**	Martin G	Oper	4 - 3	-	4 - 3	-	4 - 3	3 - 2
11	**Royal Mail Alignment**	Martin G	Strat	4 - 3	-	4 - 3	-	4 - 3	4 - 2
12	**Market Developments/ Competition (FS)**	Nick K	Strat	3 - 3	Up	4 - 3	-	4 - 3	3 - 2
13	**Transformation Strategic Alignment**	David H	Trans	3 - 5	-	3 - 5	Down	3 - 4	3 - 3
14	Change Portfolio Delivery	David H	Trans	4 - 3	-	3 - 4	-	3 - 4	3 - 3
15	**FS Regulatory Supervision**	Nick K	Leg & Reg	3 - 4	-	3 - 4	-	3 - 4	3 - 2
16	**Financial Reporting and Controls**	Al C	Fin	3 - 4	-	3 - 4	-	3 - 4	2 - 2
17	**Information Security**/ Data Protection **Breach**	Jane McL	Oper	3 - 3	-	3 - 3	Up	3 - 4	3 - 1
18	**Digital Competency**	Martin G	Oper	2 - 4	-	2 - 4	Up	3 - 4	3 - 2
AMBER RISKS - *for monitoring to alert if turning Red*									
19	**Transformation Resources**	David H	Trans		-		-		
20	**Investments Decisions**	Al C	Strat		-		-		
21	**FS Sales Capability**	Kevin G	Oper		-		-		
22	Commercial Sustainability	Al C	Fin	-	New		Up		
23	**Corporate Reputation**	Neil H	Strat		-		-		
24	**Regulatory Compliance Breach**	Jane McL	Leg & Reg		-		-		
25	**Government Alignment**	Neil H	Strat		-		-		
26	**NFSP Alignment**	Neil H	Strat		-		-		
27	**Health & Safety**	Neil H	Leg & Reg	-	New		-		

NET RISK PROFILE (including change from previous/ Mar '16)



Note:
- *Objectives and Targets are from Business Plan 15/16 - 17/18. Used as illustrative example until updated for Business Plan 16/17 - 18/19.*
- *A risk's "net" evaluation is after consideration of the effect of current controls; it's "target" evaluation is the estimate of where the risk will be in 12 months after the effect of planned Key Further Actions (see overleaf for details of Key Further Actions).*
- *For ARC/ governance purposes, Red Risks are for actioning and have Key Further Actions designed to bring the net evaluation to the target; Amber Risks are for monitoring, to alert if the risk is turning Red. Risk owners may well have Key Further Actions for amber risk, but they are not reported to the ARC.*
- *Further details of current controls and further actions are held by risk owners in their business area Risk Registers.*

POL00400101

POST OFFICE

SUMMARY OF KEY FURTHER ACTIONS (RED RISKS ONLY) - Updated Sept 2016

Appendix 2a

Blue text is new for Sept 2016

Version: Updated 21st September 2016

Details of Risks and Evaluations

Risk Owner	Ref	Title	Description	Update on June 2016 KFAs	New Sept 2016 KFAs	Action Owner	Action Target Date
Neil Hayward	1	**Pension Cost**	the current surplus in the DB scheme reduces to deficit and PO is unable to mainatin funding of the plan.	• Proposal presented to Trustees on 12/07/16	• Awaiting decision from Trustees on proposal	Natasha Wilson	Oct-16
	7	**Industrial Relations (Transformation)**	There is a risk of industrial action/dispute resulting from the implementation of our business plans and strategy	• Information and business cases shared with unions • IA Contingency plan reviewed	• Develop and roll out transformation narrative • Review effectiveness of IA contingency plans	Martin Kirke Martin Kirke	Mar-17 Oct-16
	9	**People Capability**	there is no clear prioritisation of capabilities required to deliver the business strategy	• Process and Organisational Design support team recruited	• Top level Org Design approved by CEO • Define detailed operating model • Implement strategic hiring and retention plans	Jonathan Cormack Jonathan Cormack Jonathan Cormack	Nov-16 Apr-17 Oct-17
Martin George	3	**Market Developments/ Competition (non-FS)**	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	• Developed Mails implementation plan • Used Customer Strategy to inform product strategies • Developed Government Services implementation plan	• Develop new product proposals (e.g. POCA+) • Submit business case for fibre broadband	Chris Doutney Geoff Smyth	Jan-17 Jan-17
	10	**Customer Experience**	our customer experience, propositions and channel strategy fail to deliver what customers want	• Product strategies informed and implementation plans developed	• Review product journeys and identify generic capabilities needed to improve customer journeys • End to end review of customer complaints	Glyn Williams/ Martin George Martin George	Dec-16 Oct-16
	11	**Royal Mail Alignment**	misalignment of objectives and unsuccessful renegotiation of MDA or renegotiation on disadvantageous terms	• RMG negotiations commenced	• Continue joint strategy project with RMG	Gordon Rose/ Mark Siviter	Jan-17
	18	**Digital Competency**	lack of digital competency to spot and implement quickly enough (e.g. new products, customer journey, back office)	• New red risk, so no previous KFAs recorded	• Define roadmap for each product grouping	Glyn Williams	Oct-16
Kevin Gilliland	8	**Network Proposition**	POL is 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	• Branch Proposition and Network Strategy developed • Cost implications of new models validated	• Develop win/win proposition for agents to improve bottom line • Communicate true value of proposition to existing/ potential agents to drive demand	Kevin Seller Kevin Seller	Dec 16 Dec 16
Nick Kennett	12	**Market Developments/ Competition (FS)**	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 - includes BoI is not aligned (strategically or financially) to assist POL's growth plans	• FS Strategy approved by POL Board	• Negotiations underway with BoI • Implementing 100 Day Roadmap and present plan to POL Board	Jonathan Hill Jonathan Hill	Oct-16 Oct-16
	15	**FS Regulatory Supervision**	growth, transformation and/ or compliance breaches (e.g. FS mis-selling risk, non-compliant product distribution, design or marketing, Fit & Proper staff vetting, agency contracts/ conflicts of interest) trigger supervision and regulatory requirements	• Conflicts of Interest working party established	• Complete network conduct risk remediations • Agree approach to resolve network regulatory conflicts of interest issues • Respond and implement required improvements to vetting process following Mortgage Specialist Reviews • Operationalise new Vetting policy	Owen Woodley/ Jonathan Hill Nick Kennett/ Owen Woodley Joe Connor Jonathan Cormack/ Joe Connor	Dec-16 Sept-16 Oct-16 Jan-17
David Hussey	6	**Transformation Benefit Realisation**	Business Transformation programme is unable to deliver projects within timescale, costs and agreed business case leading to erosion of confirmed benefits	• Benefits Tracking Framework /Governance implemented. • TDG reviews tracking of Programmes, including costs and benefits	• Prioritise and schedule review of the agreed change portfolio to ensure strategic alignment • Complete due diligence of contracte to understand obligations	Nick Sambridge/ Alison Japp Martyn Lewis/ Neil Wilkinson/ Ben Cooke	Oct-16 Oct-16
	13	**Transformation Strategic Alignment**	PO strategy is still evolving and will result in changes to the existing operating model. Current Transformation activities will not fully achieve POLs future plans, strategy and direction and replan may be required to ensure it continues to support commercial sustainability	• Reviewed Transformation programmes against emerging TOM	• Develop TOM, identify conflicts with Strategies • Conduct Prioritisation exercise and agree sequencing of activities	Alison Jaap/ Martin Edwards Martin Edwards/ Alison Jaap	Nov-16 Oct-16
	14	**Change Portfolio Delivery**	Change Portfolio Delivery model (IT and non-IT) is unable to manage the size and impact of Change (either due to internal POL and Third Party issue)	• Review of change process completed	• Identify actions from Change process review • Develop plan for prioritisation and scheduling of Change Portfolio	David Hussey / Rob Houghton David Hussey / Rob Houghton	Oct-16 Nov-16
Al Cameron	2	**Government Funding and Headroom**	funding beyond 2017/18 is insufficient to support the investment and transformation programme and we breach our headroom requirements	• New red risk, so no previous KFAs recorded	• Progress the Strategy to Plan initiatives • Build headroom requirements into strategy and five year plan	Martin Edwards Nick Sambridge/ Martin Edwards	Oct-16 Oct-16
	5	**IT Availability/ Ability to Trade**	failure of infrastructure or application environments, either due to internal issues, supplier/ partner failure or cyber attack, leads to lack of IT availability and/ or inability to trade	• BC/DR plan drafted • Completed EUC separation	• Identify and agree remediations to BC/DR plan • Operationalise BC/DR testing programme • Reshape BOTT project and progress per revised schedule	Sharon Gilkes Sharon Gilkes Ben Cooke	Oct-16 Post Oct-16 Sept-17
	16	**Financial Reporting and Controls**	inadequate financial controls to prevent financial misstatement and lack of compliance with accounting and governance standards	• Completed financial controls mapping • Completed executive declaration trial	• Complete financial controls remediation • Continue trialing CSA	Paul Hemsley Paul Hemsley/ Mike Morley-Fletcher	Mar-17 Mar-17
Jane MacLeod	4	**Third Party Relationship Management**	fail to select, contract, measure, monitor and exit key in-source or out-source relationships/ contracts successfully and/ or unintentional breach of contractual terms by PO	• Contract Management framework developed	• Review CAF process • Upload contracts (top 20) into Bravo and CM training • Annual attestation of compliance with policy/ guidelines	Heads of Legal and CoSec Heads of Legal Heads of Legal/ Compliance Team	Oct-16 Dec-16 Mar-17
	17	**Information Security / Data Protection Breach**	fail to adequately deploy and effectively manage information assurance and cyber security policies, standards and controls within the business and our partners/ suppliers, results in a breach of company data (colleague/ customer)	• Cyber Security & Information Assurance Policy Document Set	• Establish a Security Operations Centre • Deploy Security Incident Event Management • Deploy Data Loss Prevention tool	Sharon Gilkes Rob Houghton Julie George	Jun-17 Mar-17 Mar-17

POL00400101

POST OFFICE

Appendix 2b

DETAILS OF KEY FURTHER ACTIONS (RED RISKS ONLY) - Updated Sept 2016

Version: Updated 21st September 2016

Details of Risks and Evaluations				Key Further Actions (updated till end of August 2016)		
Risk Owner	**Ref**	**Title**	**Description**	**Update on Key Further Actions at March 2016,** June 2016 plus Sept 2016	**Action Owner**	**Action Completion**
Neil Hayward	1	**Pension Cost**	the current surplus in the DB scheme reduces to deficit and PO is unable to maintain funding of the plan	• **Consultation concluded and Consultation Report finalised, including all feedback from members and representatives** • **Recommendation papers presented to GE and Board with de-risking plans** • Present proposal to Trustees on 12/07/16 • Awaiting decision from Trustees (27 Sept or 6 Oct)	**Natasha Wilson** **Natasha Wilson** Natasha Wilson Natasha Wilson	**Completed** **Completed** Sept-16 Octt-16
	7	**Industrial Relations (Transformation)**	There is a risk of industrial action/dispute resulting from the implementation of our business plans and strategy	• **Escalation to CWU General Secretary completed** • Continue to argue case with unions sharing information, including business cases, presented by GE members, supported by professional specialist Industrial Relations and HR team • Continue to review IA Contingency Plans (GE/ CEO) • Continue development of the transformation narrative and roll out • Review effectiveness of Industrial Action Contingency Plans	Martin Kirke Martin Kirke Martin Kirke Martin Kirke Martin Kirke	**Completed** Sept-16 Sept-16 Mar-17 Oct-16
	9	**People Capability**	there is no clear prioritisation of capabilities required to deliver the business strategy	• **Top level organisation design developed** • Approve of top level organisation design by CEO • Recruited Process and Organisational Design support team • Define detailed operating model • Implement strategic hiring • Review sales operating model with Owen Woodley • Implement retention plans	**Jonathan Cormack** Jonathan Cormack Jonathan Cormack Jonathan Cormack Jonathan Cormack Jonathan Cormack Jonathan Cormack	**Completed** Nov-16 Jul-16 Apr-17 Oct-17 Nov-16 Oct-16
Martin George	3	**Market Developments/ Competition (non-FS)**	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	• **Secured approval of Mails strategy, agreeing to seek revised commercial agreement with RMG.** Developed Mails implementation plan • **Concluded Customer Strategy project (markets, customers, channels).** Used Customer Strategy to inform product strategies • **Developed Government Services strategy, focusing on identity, leveraging current capabilities and increasing profitability of current contracts.** Developed Government Services implementation plan • Develop POCA+ proposal; develop branch based ID verification process for wider customer base • Develop and submit business case for fibre broadband • Explore options for expanding Telecoms customer base	Mark Siviter Martin George Chris Doutney Chris Doutney Geoff Smyth Geoff Smyth	Completed Completed Completed Jan-17 Jan-17 Jan-17
	10	**Customer Experience**	our customer experience, propositions and channel strategy fail to deliver what customers want	• **Concluded Customer Strategy and Channel Strategy.** Used to inform product strategies and develop implementation plans • Review product journeys with Bank of Ireland and develop actions plans to implement improvements • Identify generic capabilities (digital and other) needed to improve customer journey over all products • Perform end to end review of customer complaints to improve collection and analysis of complaints	Martin George Glyn Williams Martin George Martin George	Completed Dec-16 Dec-16 Oct-16
	11	**Royal Mail Alignment**	misalignment of objectives and unsuccessful renegotiation of MDA or renegotiation on disadvantageous terms	• **Agreed Terms of Reference for RMG negotiations.** Commence RMG negotiations, using direction/ insights from Mails strategy and Board discussions • Continue joint strategy project with RMG: complete analysis of shared data and agree joint view of market direction	Gordon Rose/ Mark Siviter Gordon Rose/ Mark Siviter	Sept-16 Jan-17
	18	**Digital Competency**	lack of digital competency to spot and implement quickly enough (e.g. new products, customer journey, back office)	• Define digital, multi-channel and omni-channel roadmap for each product grouping as part of Strategy to Plan work	Glyn Williams	Oct-16
Kevin Gilliland	8	**Network Proposition**	POL is 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	• Developed Branch Proposition/ Network Strategy Implementation Plan for new models across existing network • Validated cost implications of new models, then technical solutions chosen, for both POL and agents, and include in proposals to retail partners • Continue to investigate process simplification and cost efficiencies via STRN project • Develop win/win proposition for agents to improve bottom line • Communicate true value of proposition to existing/ potential agents to drive demand	Kevin Seller Kevin Seller Kevin Seller Kevin Seller Kevin Seller	Completed Completed Dec-16 Dec-16 Dec-16
Nick Kennett	12	**Market Developments/ Competition (FS)**	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 - includes BoI is not aligned (strategically or financially) to assist POL's growth plans	• **FS strategy (customer centric/ growth) approved by GE/ POL Board.** Implement 100 Day Roadmap and present fuller FS Implementation Plan to Board (Oct) • **Tactical and longer term negotations with BOI underway to enhance PO position (digital and wider).** Present update to Board (Oct)	Jonathan Hill Jonathan Hill	Oct-16 Oct-16
	15	**FS Regulatory Supervision**	growth, transformation and/ or compliance breaches (e.g. FS mis-selling risk, non-compliant product distribution, design or marketing, Fit & Proper staff vetting, agency contracts/ conflicts of interest) trigger supervision and regulatory requirements	• **Progressing key actions in the network Conduct Risk review.** Complete network conduct risk remediations • **Conflict of interest working party established.** Agree approach to resolving network regulatory conflict of interest issues (e.g. partner retailers with own FS products).Network to provide ongoing compliance • Respond and implement required improvements to vetting process following Mortgage Specialist Reviews • Operationalise new Vetting policy	Owen Woodley/ Jonathan Hill Nick Kennett/ Owen Woodley Joe Connor Jonathan Cormack/ Joe Connor	Dec-16 Sept-16 Oct-16 Jan-17
David Hussey	6	**Transformation Benefit Realisation**	Business Transformation programme is unable to deliver projects within timescale, costs and agreed business case leading to erosion of confirmed benefits	• **Reviewed and implemented revised Benefits Tracking Framework/ Governance** • **Reviewed and revised Business Cases to ensure they provide more detailed analysis of costs and identified benefits** • **TDG review of Transformation Costs and Benefits Tracking of Programmes (every other fortnight)** • **Monthly Deep dives at Programme level are in place to review progress on cost, benefit, resource and plans** • **Developed benefits mapping standard and guidance on how projects should estimate benefits** • Create a phased benefits log (currrently held at an annual level) • Conduct a full prioritisation review of whole change portfolio (current and emerging) to ensure we have absolute strategic alignment and meet the financials • Programmes to complete ongoing due diligence of contracts and plans to ensure obligations are understood and reflected in business case sensitivities and costs	**Nick Sambridge** **Nick Sambridge** **Nick Sambridge** **Nick Sambridge** **Nick Sambridge** Nick Sambridge Nick Sambridge/ Alison Japp Martyn Lewis/ Neil Wilkinson/ Ben Cooke	**Completed** **Completed** **Ongoing** **Ongoing** **Completed** Sep-16 Sep-16 Oct-16
	13	**Transformation Strategic Alignment**	PO strategy is still evolving and will result in changes to the existing operating model. Current Transformation activities will not fully achieve POLs future plans, strategy and direction and replan may be required to ensure it continues to support commercial sustainability	Pre Strategy and TOM Agreement • All parts of the business to understand the impacts of the new strategies across their parts of the business and within Transformation (through Strategy and TOM Working Group) • Develop Target Operating Model and identify conflicts between TOM and Strategies being developed • Strategy to Plan activities to closely align with Transformation Design team and transformation activities • **Collate a list of activities that need to take place to deliver Transformation portfolio and strategies** • Conduct Prioritisation exercise and agreed sequencing of activities • Updated the Digital Roadmap Strategy (for chosen option 1) and aligned with underpinning IT architecture to support it • **Review of of existing funded Transformation programmes against emerging TOM through Bootcamp process and agree stop, start and continue** Post Strategy and TOM Agreement • Implement assurance framework for design approach to ensure Transformation objectives are not compromised and conflicts are identified and remediated	Alison Jaap/ Martin Edwards Alison Jaap/ Martin Edwards Alison Jaap/ Martin Edwards **Alison Jaap** Martin Edwards,/ Alison Jaap Gynn Williams / Rob Houghton **Alison Jaap** Alison Jaap	Ongoing Sept-16 Ongoing **Complete** Oct-16 Completed **Completed** Oct-16
	14	Change Portfolio Delivery	Change Portfolio Delivery model (IT and non-IT) is unable to manage the size and impact of Change (either due to internal POL and Third Party issue)	• Agree appropriate scheduling of Change Portfolio prioritisation activities • **Completed a formal end to end review of change process including supplier.** Redesign change process • Implement tactical quick wins • Improved IT Supplier relationships through heightened governance, with greater involvement of business and by engaging with partners to identify what is needed for change (e.g. obligations, testing etc.) by detailed planning covering all stages from initiation to project delivery • Ensured IT work is scheduled in line with agreed business priorities and with contribution from business SMEs • Continued to mobilise a robust IT Service Model based on Industry Standards and ensure its effectiveness	David Hussey / Rob Houghton David Hussey / Rob Houghton David Hussey / Rob Houghton Neil Wilkinson Neil Wilkinson Neil Wilkinson	Nov-16 Oct-16 Oct-16 Completed Completed Completed
Al Cameron	2	**Government Funding** and Headroom	funding beyond 2017/18 is insufficient to support the investment and transformation programme and we breach our headroom requirements	• Progress the 'Strategy to Plan' initiatives, update project prioritisation list and incorporate into consolidated 5 year plan by October Board (with draft in September) • Ensure headroom requirements are built into development of the strategy and 5 Year Plan, and identify possible contingency plans	Martin Edwards Nick Sambridge/ Martin Edwards	Oct-16 Oct-16
	5	**IT Availability/** Ability to Trade	failure of infrastructure or application environments, either due to internal issues, supplier/ partner failure or cyber attack, leads to lack of IT availability and/ or inability to trade	• **BC/DR plan drafted.** Remediations to BC/DR plan being identified and agreed • **BC/DR testing programme included in draft plan.** BC/DR testing programme will be operationalised after remediation of BC/DR plan • **Completed logical separation of EUC services from RMG by March and physical separation by June** • **Back Office Migration project (BOTT) re-scheduled due to complexity of project and issues with previous and current vendors.** Reshape BOTT project and progress per revised schedule	Sharon Gilkes Sharon Gilkes **Sharon Gilkes** Ben Coake	Oct-16 Post Oct-16 **Completed** Sept-17
	16	**Financial Reporting and Controls**	inadequate financial controls to prevent financial misstatement and lack of compliance with accounting and governance standards	• **Financial controls mapping completed.** Remediation and resource allocation in progress • **Executive Declaration trial completed.** Control Self-Assessment trial commenced. Continue trialling CSA • **Income reconciliation completed**	Paul Hemsley Paul Hemsley/ Mike Morley-Fletcher **Paul Hemsley**	Mar-17 Mar-17 **Completed**
Jane MacLeod	4	**Third Party Relationship Management**	fail to select, contract, measure, monitor and exit key in-source or out-source relationships/ contracts successfully and/ or unintentional breach of contractual terms by PO	• **Contract Management framework developed by Procurement and contracts being uploaded onto Bravo; training commenced.** Complete uploading of (top 20) contracts to Bravo and CM training • **CAF process being reviewed.** Complete review to confirm if CAF process is working as planned • **Developing process for annual attestation of compliance with procurement policy/ guidelines.** Conduct annual attestation of compliance with procurement policy/ guidelines for year end 2016/17	Heads of Legal Heads of Legal and CoSec Heads of Legal/ Compliance Team	Dec-16 Oct-16 Mar-17
	17	**Information Security/** Data Protection **Breach**	fail to adequately deploy and effectively manage information assurance and cyber security policies, standards and controls within the business and our partners/ suppliers, results in a breach of company data (colleague/ customer)	• Establish a Security Operations Centre • Deploy Security Incident Event Management • Deploy a Data Loss Prevention tool • Certification activity with regards to PCI-DSS & ISO27001 • Review of Cyber Security & Information Assurance Policy Document Set	Sharon Gilkes Rob Houghton Julie George Julie George Julie George	Jun-17 Mar-17 Mar-17 Oct-16 Oct 16

POL00400101

POST OFFICE

Appendix 3

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%

*Note: * any one year over Business Plan time horizon*
*** generally use financial measure first, then enhance if an additional operational or reputational impact applies too*

Our risk evaluation can be on a basis of:	
GROSS risk	= the risk evaluation ***before*** taking into account the effectiveness of controls currently in place. Sometimes referred to as "inherent" risk.
NET risk	= the risk evaluation ***after*** taking into account the effectiveness of controls currently in place. Sometimes referred to as "residual" risk.
TARGET risk	= the risk evaluation ***if*** further actions were taken to manage the risk to an acceptable level (i.e. ultimately to meet the desired risk appetite).

POL00400101

POST OFFICE

Appendix 4

RISK DESCRIPTIONS - Updated Sept 2016

Version: Updated 16th September 2016

Details of Risks and Evaluations

Ref	Risk Owner	RU Category	Title	Description	Original (Sep '15)	Change Previous	Previous (Mar '16)	Change This Qu	NET Impact	NET Lik'hood	NET Score	TARGET Impact	TARGET Lik'hood	TARGET Score	Difference
RED RISKS - *for actioning to bring the net evaluation to the target*															
1	Neil Hayward	Financial	Pension Cost	the current surplus in the DB scheme reduces to deficit and PO is unable to maintain funding of the plan	3 - 3	Up	4 - 3	Up	4	3	12	4	2	8	-4
2	Al Cameron	Financial	Government Funding and Headroom	funding beyond 2017/18 is insufficient to support the investment and transformation programme and we breach our headroom requirements	5 - 2	-	5 - 2	Up	5	2	10	4	2	8	-2
3	Martin George	Strategic	Market Developments/ Competition (non-FS)	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	4 - 4	-	4 - 4	-	4	4	16	2	3	6	-10
4	Jane MacLeod	Operational	Third Party Relationship Management	fail to select, contract, measure, monitor and exit key in-source or out-source relationships/ contracts successfully and/ or unintentional breach of contractual terms by PO	4 - 4	-	4 - 4	-	4	4	16	2	2	4	-12
5	Al Cameron	Operational	IT Availability/ Ability to Trade	failure of infrastructure or application environments, either due to internal issues, supplier/ partner failure or cyber attack, leads to lack of IT availability and/ or inability to trade	4 - 3	-	4 - 3	Up	4	3	12	4	2	8	-4
6	David Hussey	Transformation	Transformation Benefit Realisation	Business Transformation programme is unable to deliver projects within timescale, costs and agreed business case leading to erosion of confirmed benefits	4 - 3	-	3 - 4	Up	4	4	16	3	3	9	-7
7	Neil Hayward	Transformation	Industrial Relations (Transformation)	Unions don't support change and undermine transformation through prolonged business-wide industrial action.	5 - 4	-	5 - 4	Down	3	5	15	4	4	16	1
8	Kevin Gilliland	Operational	Network Proposition	POL is 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	5 - 3	-	5 - 3	Down	4	3	12	4	2	8	-4
9	Neil Hayward	Operational	People Capability	there is no clear prioritisation of capabilities required to deliver the business strategy	5 - 3	-	5 - 3	Down	4	3	12	4	2	8	-4
10	Martin George	Operational	Customer Experience	our customer experience, propositions and channel strategy fail to deliver what customers want	4 - 3	-	4 - 3	-	4	3	12	3	2	6	-6
11	Martin George	Strategic	Royal Mail Alignment	misalignment of objectives and unsuccessful renegotiation of MDA or renegotiation on disadvantageous terms	4 - 3	-	4 - 3	-	4	3	12	4	2	8	-4
12	Nick Kennett	Strategic	Market Developments/ Competition (FS)	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 - includes BoI is not aligned (strategically or financially) to assist POL's growth plans	3 - 3	Up	4 - 3	-	4	3	12	3	2	6	-6
13	David Hussey	Transformation	Transformation Strategic Alignment	PO strategy is still evolving and will result in changes to the existing operating model. Current Transformation activities will not fully achieve POLs future plans, strategy and direction and replan may be required to ensure it continues to support commercial sustainability	-	New	3 - 5	Down	3	4	12	3	3	9	-3
14	David Hussey	Transformation	Change Portfolio Delivery	Change Portfolio Delivery model (IT and non-IT) is unable to manage the size and impact of Change (either due to internal POL and Third Party issue)	4 - 3	-	3 - 4	-	3	4	12	3	3	9	-3
15	Nick Kennett	Legal & Regulatory	FS Regulatory Supervision	growth, transformation and/ or compliance breaches (e.g. FS mis-selling risk, non-compliant product distribution, design or marketing, Fit & Proper staff vetting, agency contracts/ conflicts of interest) trigger supervision and regulatory requirements	3 - 4	-	3 - 4	-	3	4	12	3	2	6	-6
16	Al Cameron	Financial	Financial Reporting and Controls	inadequate financial controls to prevent financial misstatement and lack of compliance with accounting and governance standards	3 - 4	-	3 - 4	-	3	4	12	2	2	4	-8
17	Jane MacLeod	Operational	Information Security/ Data Protection Breach	fail to adequately deploy and effectively manage information assurance and cyber security policies, standards and controls within the business and our partners/ suppliers, results in a breach of company data (colleague/ customer)	3 - 3	-	3 - 3	Up	3	4	12	3	1	3	-9
18	Martin George	Operational	Digital Competency	lack of digital competency to spot and implement quickly enough (e.g. new products, customer journey, back office)	2 - 4	-	2 - 4	Up	3	4	12	3	2	6	-6
AMBER RISKS - *for monitoring to alert if turning Red*															
19	David Hussey	Transformation	Transformation Resources	fail to access the right people (their capacity and capability) to deliver the transformation portfolio	3 - 3	-	3 - 3	-	3	3	9	3	2	6	-3
20	Al Cameron	Strategic	Investments Decisions	sub-optimal investment decisions for strategic initiatives (including selection, assessment, pricing and management) made due to weakness in subject expertise, quality financial data and evaluation processes and clear accountabilities	3 - 3	-	3 - 3	-	3	3	9	2	2	4	-5
21	Kevin Gilliland	Operational	FS Sales Capability	FS sales capability unable to deliver FS growth targets, either through design or execution	3 - 3	-	3 - 3	-	3	3	9	2	2	4	-5
22	Al Cameron	Financial	Commercial Sustainability	growth developments and cost reductions fail to steer PO to break even and then commercial sustainability	-	New	2 - 3	Up	3	3	9	1	2	2	-7
23	Neil Hayward	Strategic	Corporate Reputation	threat to PO Brand Reputation (with Government, public, customers, colleagues and retail partners) from issues that are seen to compromise our social purpose (e.g. Transformation, Sparrow)	4 - 2	-	4 - 2	-	4	2	8	4	1	4	-4
24	Jane MacLeod	Legal & Regulatory	Regulatory Compliance Breach	fail to comply with key laws or regulations (in particular Competition, Money Laundering, Bribery & Corruption, Data Privacy) causing fines, sanctions or suspension of business activity	4 - 2	-	4 - 2	-	4	2	8	2	2	4	-4
25	Neil Hayward	Strategic	Government Alignment	misalignment of objectives and lack of Government support for our strategy (e.g. 25-40% cost savings reduce services)	2 - 4	-	2 - 4	-	2	4	8	1	2	2	-6
26	Neil Hayward	Strategic	NFSP Alignment	relationship with NFSP does not progress in line with the aims of the Grant Agreeement, due to the behaviour of the NFSP or changes to the agent proposition which the NFSP believe are unacceptable	3 - 2	-	3 - 2	-	3	2	6	3	1	3	-3
27	Neil Hayward	Legal & Regulatory	Health & Safety	fail to comply with laws or regulations and deploy adequate safeguards for the safety and wellbeing of our people and customers, which is inconsistent wth our values and duty of care	-	New	3 - 2	-	3	2	6	3	1	3	-3

POL00400101

6) Internal Audit Report

Author: Mike Morley-Fletcher Sponsor: Jane MacLeod Meeting date: 28 September 2016

Executive Summary

Context

The purpose of this paper is to update the Committee on the PO Internal Audit (IA) and Business Transformation Assurance (BTA) activity and key outcomes. This includes details of the work completed since the last Audit, Risk and Compliance Committee (ARC) in May and progress on the 2016/17 Internal Audit Plan.

Questions this paper addresses

1. What progress has been made since the May meeting?
2. Is the Internal Audit Plan on track?
3. Do we have the resources we need to deliver the plan and actions arising?
4. Have any significant issues arisen that the committee should be aware of?

Conclusion

1. During the period since the May ARC, 6 reviews have been completed and cleared with GE sponsor, with actions agreed with management: 2 Internal Audit (SISD Delivery, Common Digital Platform) and 4 Business Transformation Assurance (Communications & Stakeholder Management, Digital Programme Mobilisation, Planning Boot Camps, Cyber Review). 7 other reviews are nearing completion: 4 IA (Data Protection, DC Pension, FS Sales Training and Competence Schemes, IT Disaster Recovery) and 3 BTA (Separation PIR, Winning with Retailers PIR, Target Operating Model). Support for scoping and resourcing 3 POMS audits via PwC has progressed with Terms of Reference agreed. Work has continued on mapping the General Controls Framework and developing a Self-Assessment capability for it and the Finance Reporting Project – due to be trail run at the half year (October).

2. We have suffered slippage since the last ARC in our plan during the holiday season, both with audit managers being away, but also finding it difficult to progress reviews with auditees who are away or involved in business critical activities. The 2015/16 plan is completed except for the DP review; the 2016/17 plan is a bit behind, but we will push on in Q3.

3. The IT audit manager we have recruited to provide maternity cover has been inducted and is working on two audits; this means we now have our full complement of 3 Internal Audit managers. Following a review of our structure in June we have been recruiting for a Senior Manager for Internal Audit, rather than the previous Head of role, which was only temporary. The Head of Risk and Assurance assumes

POL00400101

the Head of role. We have been unsuccessful in finding the right quality candidate through our own research and so now will invest the savings we have made to recruit. All these actions are within our budgeted costs.

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

Input Sought

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

POL00400101

The Report

Internal Audit Reviews - Completed

5. The **Service Integrator and Service Desk** (SISD) review was completed earlier in the year, but was then re-cleared with the new CIO, at the CFO's request. This version incorporates the new CIO's thoughts and agreed actions. The report covers an assessment of the Towers Governance Model as envisaged in 2014, which was not successfully implemented and as a result our operational model has had to be adapted in order to maintain control. The findings related to the governance aspects of accountability, roles and responsibilities and processes design. The resultant overall audit rating is Red. To remediate the highlighted issues, IT management has defined actions and included them in the new IT Strategy. The Executive Summary is included in Appendix 3.

6. The **Common Digital Platform** (CPD) review has been completed, report findings agreed by management from Commercial, Business Transformation and IT, and has been finalised with the GE sponsor. Our review found that: changes in the business' key deliverables for CDP were not reviewed, which has resulted in the current wider value of CDP not being clearly understood; benefits from CDP realised to date have not been articulated; and ultimately, the CDP technology alone cannot deliver the original vision. The changes (outputs of the Digital Strategy) in the business' key deliverables for CDP are now being reviewed and will be modelled to understand what is next for CDP. In addition, the Digital team is establishing collectively with IT, how CDP can be used as the strategic digital channel platform going forward. The resultant overall audit rating is Amber. Actions have been agreed with management from Commercial, Business Transformation and IT. The Executive Summary is included in Appendix 3.

Internal Audit Reviews – In Progress

7. The **Data Protection** (DP) review focuses on current state compliance with UK Data protection Act (1998) and was rescheduled in order to combine with the start of a project to ascertain our readiness for the new General Data Protection Regulation (GDPR) requirements, due May 2018 – SME provided by PwC. A workshop was held on 26th August, branch visits and follow up interviews have now been completed. The report on the DP review is expected at the end of September, for presentation to the November RCC/ ARC.

8. In addition to our plan for 2016/ 17, we were requested by the CFO to review issues with deductions relating to the **DC Pensions Scheme**. The report is currently going through final management clearance before going to the GE sponsor (Al C). In summary, the actions taken by the business have addressed the issue of incorrect contributions being made on a monthly basis. The necessary declarations were made promptly to the Regulator and the small number of members suffering detriment were rectified immediately. The actions to address the issues identified and prevent

POL00400101

further occurrence are being formalised and agreed as part of the report clearance process.

9. Fieldwork for the **FS Training and Competence Schemes** review is still on going as we have experience delays in arranging all the site visits over the holiday season. These site visits have now been completed and the report is being drafted. Reporting is now rescheduled to November RCC/ ARC.

10. Fieldwork and initial report drafting for the **IT Disaster Recovery and Resilience** review has completed. Discussion with the CIO and IT Disaster Recovery and Resilience SMEs is scheduled for early September. The report is scheduled for November RCC/ ARC.

11. A full summary of Audit Plan Status is included in Appendix 1.

Updates on Internal Audit Overdue Actions

12. We have continued to operate the Overdue Actions monitoring process providing summaries to GE Sponsors and their SMEs. There were a total of 6 Overdue Actions brought forward, of which 2 Financial Crime (Jane M) have been cleared. For the balance (4) there are action plans in place to push for completion:
    - Treasury (Al C, 1) – recruitment of a replacement Treasurer has proved challenging, with a preferred candidate withdrawing at the closing stages. External adverts plus a specialist recruiter are expected to secure an appointment by end Q3 2016/17. An interim or secondee will be appointed before then.
    - Critical Metrics (Al C, 1) – following a change in Financial Controller, implementation of formalisation of roles and responsibilities for providing scorecard metrics will now progress.
    - Contract Management (Jane M, 1) – obligations mapping is continuing.
    - Financial Crime (Jane M, 1) – Financial Crime policy has been approved (July) and lodged on Sharepoint. Communications to follow in October.

Updates on Self-Assessment Assurance work

13. Our aim is to provide management and the ARC with enhanced, systematic assurance information for year end March 2017, with trial runs at the half year. In preparation for the half year the following work has been completed/ is planned:

    - **General Control Framework:** the current state assessment (except for IT as they are not ready for current state assessment) for all General Controls has been completed and will be shared with SME owners ahead of the half year dry run assessment. Work will be completed in October for presentation to November RCC/ ARC.
    - **Executive Declaration:** our Executive Declaration is being reviewed (particularly considering the materiality of each item) and expanded,

POL00400101

incorporating in particular the lessons learnt from the initial dry run, BCV fraud and contract obligation exposures, for re-running at the half year. Work will be completed in October for presentation to November RCC/ ARC.

- **Control Self-Assessment, Financial Reporting:** subject to the receipt of all controls data from Finance, Control Self-Assessment will be performed in a phased role out for all financial reporting processes from October through to January. Finance colleagues will receive guidance and training in how to use the tool (TrAction) and attest correctly, closely supported by the Assurance Senior Manager on their first return. Implementation will be tracked via a Monthly Steering Group chaired by Alisdair Cameron. Internal Audit are developing an approach to provide an independent review over the process and check self-certifications on a sample basis. An update will be provided to November RCC/ ARC.

Business Assistance – Property

14. A recent update:
    - Residential: the electrical tests have now all been completed and a mitigation plan is in place for all the risks identified.
    - Crown branches: all statutory compliance tests have been performed and remedial works have been rolled out. Risk assessments have been completed on all the properties with the highest risk profile will receive additional focus from management in the form of a programme of regular audit visits.
    - Environmental issue: legal advice have been obtained that environmental assessments are only legally required in limited circumstances. However management is considering adopting a "best practice" approach to use environmental assessments to support significant business decisions. Relevant environmental trainings have been set up and a Compliance Focus Group has been set-up to focus on Post Office future approach on environmental issues.
    - Property Compliance and Health and Safety training programme: has been rolled out to all the PiCs (Person in Control) responsible for branches.
    - Property Compliance Forum: a good collaborative way of working have been developed across the Property, Health and Safety and Network Operating teams to support the PiCs (Person in Control) at the branch to manage their fire risk assessment. Continued support from all parties concerned will still be required to embed a strong compliance culture.

15. Given the recent improvements in monitoring and mitigating compliance issues more effectively and the provision of regular updates by the Property Team to RCC and ARC, IA will reduce its involvement and no longer report separately on Property Compliance. The Head of Property has provided a separate, noting paper to this ARC.

POL00400101

Business Assistance – Fraud/ BCV

16. The team have contributed in a business assistance capacity to the collective response to the recent product frauds. We have performed a wider lessons learnt, which has informed the recent improvements to processes made in the escalation of and response to material frauds. An action plan has been developed which will build further on the progress already made by the business. Continued business assistance will be given throughout the period of implementation. Further details are provided in the separate paper to the ARC.

Resourcing

17. Following a recent restructuring to replace Heads of with Senior Managers, we have the following structure/ headcount:
    - For Internal Audit reviews we have a headcount of 3 managers and an Internal Audit senior manager (currently vacant), supplemented by approximately 150 days of co-sourced resource from PwC for specialised audit work. In addition we have co-source support from Deloitte for our Business Transformation Assurance work. Both contracts run till March 2017.
    - For developing other assurance mechanisms ("Control Self-Assessment") for management and subsequently the RCC/ ARC we have 1 Assurance senior manager.
    - Both teams are supported by a Risk & Assurance analyst.

18. However our capacity has suffered:
    - The contractor we have secured to provide maternity cover for our IT Audit Manager has taken time to induct, but is now operational.
    - Another team member left earlier in the year following extended sick leave and has been replaced by a manager who was "acting up" as our Head of.
    - An IA manager has been providing support to POMS in scoping and resourcing POMS audits for PwC delivery, as part of our approach to FS assurance. We expect to recover some of our costs, but have lost some capacity. For next year, we will consider the best way to balance our resources.
    - We are still recruiting for a Senior Manager for Internal Audit. We have been unsuccessful in finding the right quality candidate through our own research and so now will invest the savings we have made to use a recruitment agency. These actions are not expected to exceed our annual budgeted costs.
    - In consequence, we have lost resource capacity earlier in the year, which has delayed some reviews, but we are now up to our full complement of 3 Internal Audit managers and aim to catch up. Timely recruitment of the Internal Audit Senior Manager will be of great assistance to this.

POL00400101

Business Transformation Assurance Reviews

19. During the period the Business Transformation Assurance team have completed and cleared with GE sponsor, with actions agreed with management 4 reviews (Communications & Stakeholder Management, Digital Programme Mobilisation, Planning Boot Camps, Cyber Review) - the Executive Summaries are included in Appendix 4. 3 more are in progress with 1 due to finalise shortly (Separation PIR, Winning with Retailers PIR). These reviews are generating recommendations for programmes going forward and aim to create more effective and efficient processes within Transformation and across Post Office as a whole.

20. In the first 12 months, BTA have completed 12 reviews across the transformation. They have been aligned with transformation's progress and planned activity. As such many of the reviews to date have focused on the design effectiveness of the central controls and governance, as well as technology projects. 99 individual issues have been identified, of which 64 (65%) have been remediated by management.

21. As a consequence of the Boot Camps a replanning of the Transformation Assurance work has had to be undertaken. This was completed with the involvement of the Post Office Internal Audit, Central Risk and Transformation Risk teams. 18 focus areas have been identified, from which reviews can be selected and approved by Transformation Risk and Assurance Group. These areas reflect a change in focus from reviews of controls and process design at portfolio level to reviews of operating effectiveness and embeddedness of controls at programme level.

22. A full summary of BTA Progress to Plan status is included in Appendix 2.

POL00400101

Appendix 1a 2015/16 Audit Plan Status – @ Sept 2016 Page 8

Activity				Actions			Reporting		
Audit	GE	Status	Report Rating	High	Medium	Low	RCC	ARC	Comments
Completed Reviews									
Contract Management	Al C	Issued		4	11	1	Sep 15	Sep 15	Closed out
Financial Crime	Jane M	Issued		18	20	2	Sep 15	Sep 15	Closed out
FS Conduct Risk	Nick K	Issued		13	-	-	Oct 15	Nov 15	Closed out
Drop and Go	Martin G	Issued		2	3	-	Oct 15	Nov 15	Closed out
Wave	Martin G	Issued		1	13	8	Oct 15	Nov 15	Closed out
Fujitsu Exit	Al C	Issued		-	2	5	Jan 16	Jan 16	Subsequently superseded by the re-engagement of Fujitsu on the Front Office Project
Critical Metric Management	Al C	Issued		3	1	1	May 16	May 16	Closed out
SISD Delivery	Al C	Issued		7	2	-	May 16	Sept 16	Closed out
Social Media	Martin G	Issued		-	5	-	May 16	May 16	Closed out
Treasury Operational Risk	Al C	Issued		6	8	-	May 16	May 16	Closed out
POMS Governance Follow up	Nick K	Issued		N/A	N/A	N/A	May 16	May 16	Closed out
Common Digital Platform	Martin G	Issued		4	9	-	Sep 16	Sep16	Closed out
Data Protection	Jane M	Finalising					Nov 16	Nov 16	Rescheduled to accommodate GDPR project, now In progress, expected Nov ARC
Agent Remuneration	Kevin G	Superceded	N/A	N/A	N/A	N/A	N/A	N/A	Superseded by business developments

POST OFFICE®

POL00400101

Appendix 1b 2016/17 Audit Plan Status – @ Sept 2016 Page 9

Activity				Reporting		
Audit	GE Owner	Timing	Status	Due RCC	Due ARC	Comments
Reviews in progress						
00) DC Pensions Issue*	Neil H/ Al C	Q2	Fieldwork	Sept 16	Sept 16	At Management clearance
01) FS Sales Training and Competence Schemes	Nick K/ Kevin G	Q1 & Q2	Fieldwork	Sept 16	Sept 16	Fieldwork delayed by auditee holidays, in initial drafting, expected Nov ARC
02) IT Disaster Recovery and Resilience	Al C	Q2	Fieldwork	Nov 16	Nov 16	Fieldwork completed, in initial drafting, taking to Management
03) Identity and Access Management (Joiners, Movers, Leavers)	Al C/ Neil H	Q2	Scoping	Nov 16	Nov 16	In scoping, planning to start fieldwork in September, slightly delayed due to induction of maternity cover IT Audit Manager
04) Branch Audit	Kevin G	Q2	Scoping	Jan 17	Jan 17	In scoping, planning to start fieldwork in September, slightly delayed due to additional DC Pensions review
05) Financial Controls Framework – Independent Testing	Al C	Q3				
06) FS Sales Compliance	Nick K	Q3				
07) NBSC Handling of Agents Complaints and Queries	Kevin G	Q3				
08) Business Continuity and Crisis Management	Al C	Q3				
09) IT Operations Governance and IT Risk Management	Al C	Q3				
10) Procurement Process	Al C	Q4				
11) IT Third Party Management	Al C	Q4				
12) FS Sales Operations First Line of Defence	Nick K	Q4				

POST OFFICE®

* Additional review at CFO request, in consequence we will consider removing one of the audits from Q3 or Q4.

POL00400101

Appendix 2a BTA Plan Status – @ Sept 2016 Page 10

Activity				Actions			Reporting		
Assurance	Timing	Status	Report Rating	High	Medium	Low	Due to RCC	Due to ARC	Comments
Completed Reviews									
End to end financial management of Transformation	Q4 15/16	Final Report	Average	1	8	**5**	May 16	May 16	Final Report Issued
Portfolio management OE #1	Q4 15/16	Final Report	Satisfactory	-	1	**2**	May 16	May 16	Final Report Issued
Communications & Stakeholder management	Q1 16/17	Final Report	Satisfactory	-	2	**1**	July 16	Sept 16	Final Report Issued (to July RCC)
Digital Programme Mobilisation	Q1 16/17	Final Report	Adverse	6	1	**-**	July 16	Sept 16	Final Report Issued (to July RCC)
Planning Boot Camps #2	Q1 16/17	Highlight Report	Satisfactory	-	-	**-**	July 16	Sept 16	Highlight Report to TRAG
Cyber Review (ARC Request)	Q2 16/17	Final Report	Adverse	8	7	**2**	Sept 16	Sept 16	Final Report Issued

POST OFFICE®

POL00400101

Appendix 2b BTA Plan Status – @ Sept 2016 Page 11

Activity			Reporting		
Assurance	Timing	Status	Due to RCC	Due to ARC	Comments
Review in Progress / Planned					
Separation PIR	Q2 16/17	Final Report	Sept 16	Sept 16	At GE Clearance
Winning with Retailers PIR	Q1 16/17	Draft Report	Sept 16	Sept 16	Draft Report at GE Clearance (outstanding meeting with ex -employee arranged for 22nd Sept – possible verbal update)
Target Operating Model	Q2 16/17	Fieldwork	Nov 16	Nov 16	Fieldwork in progress (management timings have been pushed back - TOM paper now due to November Board)
Support Services Transformation	Q3 16/17	Scoping			Timings subject to confirmation with TRAG
Back Office Tower Transition	Q3 16/17	Scoping			Timings subject to confirmation with TRAG
POCA	Q3 16/17	Scoping			Timings subject to confirmation with TRAG
Data Management and Quality	Q3 16/17	Scoping			Timings subject to confirmation with TRAG
3rd Party Vendor Management	Q3 16/17	Scoping			Timings subject to confirmation with TRAG

POST OFFICE®

POL00400101

A) Completed Internal Audit Reports – Executive Summaries

IA 01) SISD Governance Review

1. Executive Summary

As part of the Atos contract, an SISD (Service Integrator and Service Desk) governance model (Schedule 8.1) was defined in 2014. The governance model, structured on 3 layers of meetings: operational, management and strategic, was designed to enable Atos to manage five towers/main IT suppliers (front office, back office, end user computing, network and data centre) on behalf of PO. Over the last 2 years the IT strategy has evolved and two of the original towers (e.g. data centre and front office) have been dropped. This leaves PO and Atos operating in a hybrid service integrator mode, with an extended number of incumbents (approximatively 90 IT suppliers when there were originally only supposed to be 4) still supplying the different levels of IT services and with only one tower in its final stage of implementation (end user computing). It is to be noted that the SISD model covers two dimensions: 1) system integration which deals with the change management process and 2) service integration which deals with all the IT supply management processes.

ATOS have taken a pragmatic view in their approach to the situation which has enabled the relationship to continue despite the lack of a formally signed off agreement. It is only now that the Front Office supplier situation has been formalised that a more fit for purpose model can be explored. Whilst this is being worked through there will be inevitably be issues with definition of governance and challenges with the application of governance. With this in mind the following major issues have been identified during the review:

1. The **SISD governance structure** as originally designed **is neither effective nor fit for purpose for managing the current IT supply chain**. The existing contractual agreements between PO, Atos and incumbents were never designed for the current situation. This means that there is considerable challenge when attempting to ensure adequate management of the incumbents, with the result that some are not being managed by either ATOS or PO (see finding No 4 in the detailed report).

2. Although **the SISD governance framework** has been deployed, and the intended meetings run since May 2014, the model **has never been formally approved by either PO or Atos**. The detailed SISD framework operational model is an Atos contractual requirement which has not been formally adopted because it is impossible to make it work in the current situation. Whilst discussions are being undertaken to adapt to the new landscape this situation will continue (see finding No. 5 in the detailed report).

3. It is **unclear which roles are responsible for approving documents and their changes, within both organisations**. An authority matrix had to be defined as part of the Atos contract agreement and this document now exists in draft. It has not been formally approved by either party and will necessarily remain that way until the new model has been decided upon and agreed (see finding No 6 in the detailed report).

POL00400101

4. The **SISD governance framework does not clearly define the information required and the processes PO IT and ISAG need to manage** to ensure the right decisions are taken in a timely fashion (see finding No. 7&8 in the detailed report).

5. **The effectiveness of the SISD governance is limited by the lack of a formal agreement and joint approval of the *Operational manual*,** a set of documents that defines Atos operational services. Although not approved, a draft version of the Operations manual is currently in usage (see finding No.9 in the detailed report). This will be addressed by the new model once defined and agreed.

The **main root causes** of the above issues are the following:

1. ***Accountability:*** Lack of clear roles, responsibilities and accountability matrix, between PO (IT, ISAG), Atos and the IT supply chain.

2. ***Knowledge - SISD expertise:*** There is not enough SIAM model knowledge and expertise within the PO IT team to ensure the risks on PO side are adequately managed and to ensure that important decisions are not outsourced to suppliers without PO being informed/involved in the process.

3. ***Resources***: High turnover and changes within the PO IT organisation over the last 2 years combined with limited knowledge transfer and a lack of accountability and clear delegation of authority led to decisions not been taken or being delayed.

The success of an effective SISD/SIAM depends on its governance structure, processes and controls, therefore we think the following urgent actions are required to address the root causes:

1. ***Direct/Accountability/Responsibilities:*** the roles and responsibilities of everyone involved in the SISD governance structure (PO IT and ISAG, Atos, tower suppliers and other incumbents) must be clearly defined and formally agreed between all parties. These should define the level of SISD (Atos) autonomy, where it acts as an agent on behalf of PO. Furthermore the governance ownership should be assigned to a nominated role within PO, ensuring accountability for directing the SISD is clear.
2. ***Knowledge - SISD expertise*:** An effective governance structure requires a good understanding of the current IT strategy, the IT supply chain model and its risks, and the service providers' commercial obligations and limitations. We acknowledge that work is being done to design a model that the businesses can evolve to. This will ensure that the risks of operating with a large number of disparate suppliers are adequately managed. This recommendation is closely linked to the one below which requires an adequate set of skills within the PO IT organisation.

3. ***Resources:*** PO IT organisation needs to be adequately resourced (in terms of FTE and expertise) to ensure PO obligations of ownership, accountabilities and responsibilities over the SISD governance model are met. We understand that the structure and composition of the PO IT team is being reviewed to better address these issues and to make decision making more efficient.

POL00400101

As the basic governance aspects: accountability, roles and responsibilities and processes design have been raised as major issues the overall audit is rated Red (high risk).

Our overall assessment:

Report rating	Actions		
Red	High (7)	Medium (2)	Low (-)

2. Overall management response

IT Management acknowledges the risks and issues raised by this audit report. More granular actions are already in progress to address some of the self-identified issues.

The report covers an assessment of the Towers Governance Model as envisaged in 2014 versus the actual situation in 2016. In 2014 it was anticipated that by now POL would have migrated to 4 key IT suppliers, whereas we still have of most of the original 90 suppliers still in play. As a result, the operational model has had to be adapted in order to maintain control.

To remediate highlighted issues, IT management has defined the following high level activities that will be in line with new IT Strategy:

- Management will review the SIAM Operating Model with external help to assess and propose a target operating model and implementation approach. The first deliverable will be a proposed new SIAM operating model which will reflect the existing situation and experience of the last two operating years:
  - Status: in progress
  - Deliverable: Proposal of SIAM Operating Model
  - Due date: end August
- Management is in process of establishing a new IT governance and reporting model. This will be operational and will run for a quarter before being judged effective.
  - Status: in progress
  - Deliverable: Documented governance and reporting model; Governance and Reporting operational.
  - Due date: end of October - effective
- Management will revise and publish IT policies and procedures to ensure effective end-to-end processes are documented and governance controls are implemented. The accountability will be reviewed and redefined as part of process and controls review. The policies will be created and published, an assessment of gaps to the policy will then be assessed and remediation plans developed; finally the policy will be judged to be operating effectively. The GAP Assessment will also include identification and evaluation of control points for all processes, any required activities will be included into the remediation plan. The dates for remediation and operational effectiveness will be dependent on the gap assessment
  - Status: initiated

POL00400101

  - Deliverable: IT Policies and Procedures documented; Gap Assessment and Remediation Plan.
  - Due date: end of November (policy and procedures agreed); end January (Gap Assessment and outline remediation plan)
- An organisation structure has been proposed and is planned to be implemented through 2016. Recruitment is required, which takes time, and is intended to be fully staffed by the end of the year;
  - Status: in progress
  - Deliverable: effective IT team, clearly defined accountability structure and published authority matrix.
  - Due date: end of 2016.

POL00400101

IA 01) Common Digital Platform

Background:

The Common Digital Platform (CDP) was designed to be a single point for migrating sales processes and integrating the Front Office (or customer facing activities) with the Online Contact Centre and Social Media channels. During separation from Royal Mail Group, CDP was built by Accenture for PO. The annual cost for CDP is £3.5m, plus any change costs. Approximately, £12 million was spent on set up (sunk costs).

The Talk Talk security breach which resulted in customer records being accessed highlighted the need for the business to ensure it was protected. By way of design, CDP (at the time) contained unencrypted data, including non-financial personal details. In response to PO being reportedly targeted by a series of DDOS attacks in 2015 (Accenture) the business took the decision to urgently address unencrypted data at rest in CDP applications, in the effort to reduce our exposure to further attacks (albeit retrospectively) through archiving, encrypting and secure storage of customer data. Data sent to third parties remains unencrypted. The business has implemented a DDOS solution (Verizon) in parallel.

Our overall assessment:

Report rating	**Actions**		
Amber	**High (4)**	**Medium (9)**	**Low (-)**

The original vision (IT led) was to have CDP as our single strategic digital channel. However the business has been more focused on other individual technology solutions with less of an eye to transforming the business. The value of CDP will only be understood when the business is clear on its purpose and deliverables. This means going beyond just saying we want to digitalise or become omni-channel.

The underuse of CDP relates back to our business fundamentals, rather than the technology itself. Essentially, solutions for various business problems have been implemented and culturally each individual project has been allowed to optimise a solution for their own needs, rather than follow a mandated imperative to utilise or leverage the platform. This has led to underuse of the platform and high cost of ownership for the very few solutions that are on the platform.

Our review found that:

1. Changes in the business' key deliverables for CDP were not reviewed, which has resulted in the current wider value of CDP not being clearly understood.
2. Benefits from CDP realised to date have not been articulated.
3. Ultimately, technology (in this case CDP) alone could not delivered the original vision.

Whilst Post Office can now positively state that it does encrypt customer data and have a DDOS solution, additional work will be required to understand our wider exposures outside of CDP.

Other issues:

- No strategic imperative to use CDP as a default option.
- CDP has developed organically, rather than strategically.
- Roles, responsibilities and interactions for managing, assessing and exploiting CDP are not formalised.
- Insights gained on the benefits and limitations of CDP during the Rod Fishing Licence (RFL) showcase have not been reviewed and leveraged.

POL00400101

Priority actions:

- Changes (outputs of the Digital Strategy) in the business' key deliverables for CDP should be reviewed and modelled to understand what is next for CDP.
- Establish what is required for CDP to be used as the strategic digital channel platform (i.e. everything that is digital or Omni-channel goes through it).
- Technical debt that needs to be resolved (i.e. getting CDP software versions of CDP components up-to-date and refactor / optimise the internal architecture of CDP).

All actions have been agreed by Management.

POL00400101

B) Completed Business Transformation Assurance Reports – Executive Summaries

BTA 01) Communication and Stakeholder Engagement Review – Rated Satisfactory

Executive summary

This review focused upon the 'transformation' level communication and stakeholder engagement, and overall our review identified that approaches and plans are in place and are being executed effectively by the programmes tested. Transformation communication is not managed as a separate entity, and all communication activity is embedded within the corporate communications framework and structure. For a transformation of this size we would expect the activity at the programme level to be supported, and at times controlled, by a centralised portfolio communication and stakeholder engagement function. If transformation is viewed within isolation, gaps can be identified in the transformation communication and stakeholder engagement. However, these are mitigated by the fact that all activity is embedded within corporate communications, which is carrying out these activities. Some elements at this 'transformation' level were incomplete or absent and therefore, a number of risks have been identified. However, the corporate level communications team carries out a number of the functions absent at the 'transformation' level which mitigate the overall risk to the organisation, such as detailed central stakeholder and change impact analysis, which incorporates both BAU and transformational impacts. A number of the findings identified relate to the fact that the Head of Transformation and People Communication had only recently started in role at the time of this review, and as such was still in the process of creating a central strategy and framework. Communication is now managed as a separate stream within the Transformation High-Level plan, with key communication events detailed as milestones and we understand this will remain in place for the rest of Transformation.

In total, there were 3 findings; 2 moderate and 1 minor. The moderate findings are below:

- **Incomplete communication and engagement strategy.** The portfolio strategy for transformation communication and stakeholder engagement is incomplete. There is a Transformation strategic plan, which outlines objectives and team approach; however, there is no formal summary of the transformation stakeholders, change impact, or communication development process that is clear and consistent across all programmes. Although, the elements listed above are not present within the transformation strategy, it is noted that some of these elements do exist at the corporate level which does mitigate this issue.
- **Lack of documented central communication distribution controls.** Although there is no formally defined process for the approval of external communications, it is understood by communication team members that there is a requirement to gain approval from appropriate senior management before releasing communications. This is done via email, where communications are drafted, before being signed off by an appropriate manager / director, and then released.

POL00400101

This review has identified weakness in processes and controls at the portfolio level. The Head of Transformation and People Communication has developed a central strategy and framework, and has drafted a Communication Covenant, which sets out the principles of how communication will work in Transformation (there is now a clear set of expectations for the communication team, where previously there was not). However, detailed analysis of stakeholders and change impacts is occurring at the corporate level, and transformation communication and stakeholder engagement is being carried out at the programme level. Stakeholder analysis is effective, programme communication plans exist, and stakeholder feedback is being actioned.

Although, the review did not formally look at communication and stakeholder engagement at the corporate level, it is clear through discussions with the Communications and Corporate Affairs Director, and through review of available documentation, that risks at the transformation level are mitigated through the work being carried out.

Based on the work performed, as stated in the scope and methodology sections, we have given our review of the transformation communication and stakeholder engagement within POL an satisfactory (with exceptions) average risk rating. A satisfactory report rating is defined as:

Overall control environment is sound in almost every operational aspect. However, a low level number of minor non-compliance with internal and external requirements, and weaknesses in records, systems and controls were identified. Examples may include: only minor or process improvement findings.

POL00400101

BTA 02) Digital Projects Review – Rated Adverse

Executive summary

The Head of Digital (supported by the Head of Portfolio and the appointed Programme Manager) is responsible for the delivery of Digital initiatives projects at Post Office, which includes projects and initiatives within the digital space. At the time of this report exploiting digital opportunities was a core component of the Post Office Strategy. A business wide Digital Strategy is due to be developed, after which a Digital programme will be fully mobilised within Commercial to coordinate and align the associated initiatives. Overall, our review identified a number of weaknesses in how the digital programme was managed in particular these include:

- monitoring of project financials (ability to measure successful delivery versus approved funding)
- tracking of the benefits management plan
- recording of resource utilisation across the business case initiatives.

We acknowledge that the Digital Programme Team faced various challenges (particularly in the earlier stages) relating to capacity issues, which was driven by a lack of business as usual (BAU) resource, Head of Digital leaving the business, unplanned urgency to address issues with the Common Digital Platform (CDP) and wider business prioritisation of trade to meet revenue targets.

Interviews with stakeholders established that challenges (highlighted above) resulted in Programme resource being diverted to prioritise BAU activity. As a consequence this resulted in a "blurring the lines" between BAU and Programme resource / scope deliverables. This ambiguity could be viewed as contributing to a number of the issues identified within this report.

A number of recommendations have been made within this report which, whilst remediated should be applied to future projects and programmes as appropriate. In total there were seven findings; six major and one moderate. The major findings are summarised below:

- **Inadequate scope and change management process.** Delivery items were de-scoped or added to the business cases without re-approval. This was partly due to the tolerance perimeters for scope change requests (CRs) not being clear at the early stages of the programme. After the implementation of the Transformation Delivery Group (TDG), proposed CRs were submitted for approval, however these did not pass through an initial Steerco review/approval (as the Steerco had been disbanded).
- **Cost / Budget breakdown.** There was an absence of granular time recording which reduces the ability to transparently report on resource utilisation across project and BAU activity. This issue is particularly evident due to the fact that many resources were assigned to both project and BAU work activities. The absence of granular reporting potentially impacts the accuracy to which financial spend versus budget can be reported per project / initiative.
- **Benefits tracking and ownership.** The benefits management plan (as outlined in the initiating business cases) was not monitored, tracked or reported to the relevant benefit owners until December 2015 (later stage of the project by). This was reportedly due to the lack of resource to perform this activity until this time. The absence of benefits

POL00400101

tracking and accountability to benefit owners, impacts the accuracy and ability to measure the return on investment that has been authorised within each business case.

- **Project / initiative closedown.** There was no formal project / initiative close-out procedure, including handover to BAU. Work is still ongoing for projects / initiatives which should be complete as per the approved business case plans. Again this was due in part to the lack of formality between project and BAU activity. The lack of a formal close down process includes:
  - Lack of formal transition and acceptance to BAU;
  - Undocumented measurement against success criteria; and
  - Absence of formal acceptance from business sponsor and benefit owner.

- **Lack of formal transition of sponsor.** The original Programme Sponsor (Head of Digital) left the organisation and as such the role of Programme Sponsor was transitioned to the Director for Commercial and Chief Marketing Officer. However, this role was not formalised. As such this could have created a lack of clarity elsewhere in the organisation on who was accountable for this programme.
- **Lack of project steering committee.** There was a breakdown in programme governance processes, evident in the fact that the programme Steering Committee for 'Fix the Funnell' was disbanded in the initial stages of the programme (May 2015) and was not formally reinstated. We understand that the Director for Commercial and Chief Marketing Officer continued to have oversight through 1-2-1 meetings (whilst informal), although the meetings would not have had the range of stakeholder input as the Steering Committee.

Based on the work performed, as stated in the Scope and methodology sections, we have given our review of the benefits framework management within POL an adverse risk rating. An adverse report rating is defined as:

Inadequate internal control environment. A high number of non-compliance with internal and external guidelines and weaknesses in records, systems and controls were identified. Examples may include: reputational damage or inappropriate use of company assets.

POL00400101

BTA 03) Transformation Boot Camps #2

Executive Summary

BTA has continued to conduct assurance over the transformation portfolio. BTA attended the Transformation Planning Boot Camps, where individual programme plans were discussed between key stakeholders in order to re-baseline an integrated transformation plan. This also involved discussing risks / issues and identifying key obligations and dependencies between programmes.

Overall Summary

- BTA endorse the very positive approach taken throughout the boot camps to conduct 'bottom up' portfolio planning to identify schedule, resource dependencies, risks, issues etc.

Key highlights

- There was strong engagement from across the various teams, including 3rd Party Suppliers where appropriate. There was good, robust challenge from key stakeholders from across the business e.g. ISAG reps.
- A number of risks, issues and dependencies were identified that will result in follow up actions assigned to individuals, and an Action Log created centrally.
- The structure and content of the sessions were all conducted with an appropriate level of detail and were consistently well attended, including by senior leadership
- All plans are now using standard templates and the processes and gateways within One Best Way are being consistently adhered to.
- BTA would recommend that these boot camps are conducted on a periodic basis (biannually), or when there is significant change.

BTA is approximately half way through the engagement; with the first half focussing on design of governance, process and controls. Following issues raised by BTA, new governance frameworks and controls have been designed and implemented. Looking forward BTA intends to focus more on implementation of these governance controls and processes through thematic reviews and detailed reviews of programmes.

POL00400101

BTA 04) Information Security (Cyber) – Rated Adverse

Executive Summary

As with many organisations, Post Office has been facing substantial challenges around its information security landscape, but particularly as it attempts to implement its 2020 strategy. Developing revenue from delivering financial products means increasing and extensive regulation regarding cyber. Transformation will result in progressively capable digital platforms on new potentially untested digital technology which is provided by a large number of suppliers. Services increasingly accessible around the clock will require more resilient operations. As a key partner to government for the delivery of official services, the impact of any breach would be significant to the Post Office's reputation. As such the Post Office is exposed to significant cyber security risks, which will continue to grow over the coming years.

The information security operational model Post Office has been using was designed for an anticipated Towers supplier model. In consequence ISAG was set-up to act as an overseeing governance body to manage information security risk based on this blueprint of having services delivered through a range of third parties, with an overarching Systems Integrator to manage this as well as performing a variety of security operations. However this operating model has not proved possible to implement and has since been changed. As such many security operation activities have fallen to an assurance group not staffed, tooled or accountable to do this. In addition, changes to the CIO in recent times has naturally disrupted progress in addressing IS issues. In response to these changing circumstances, mitigations have been put in place and risks have been raised to the governance committees. It should be noted that during this time no material data losses have been recorded. In addition, Post Office has obtained and maintained compliance certification for PCI-DSS and ISO27001 for various systems.

Notwithstanding this, from our review of controls, we have identified several interrelated findings which indicate that these risks are not being managed appropriately and that controls are behind in maturity to where we would expect them to be. Three critical findings (i.e. fundamental to the Post Office) and five significant ones (i.e. for the attention of senior management) were raised in this review. Many of the findings have been raised in previous reports (external and internal) and have not been fully addressed.

Moving forward we support management in reviewing and addressing important cyber security operational controls both those operated by the Post Office and its technology suppliers. Elements of this have been included as part of the revised IT Strategy. As a priority this should include remote access, network monitoring, completion of penetration tests and incident reporting along with the processes associated with access to critical systems and applications. In addition, accountabilities/ responsibilities around cyber security should be reviewed. This should include those regarding third parties, which is currently unclear, as well as considering the balance between assurance and operational security activities. Deciding on the most appropriate reporting line for ISAG and ensuring a fit for purpose system is in place for managing security risks with the transformation programmes will also be important.

POL00400101

Key Findings

- Remote access controls (including usage of Office365 and single sign-on for access to multiple systems) are not configured in line with good practice. Leavers are not being removed in a timely manner and no data leakage technology is implemented. All of which increases the risk of the loss of sensitive data.
- Penetration tests of some critical infrastructure has not been completed or remediated in line with policy.
- The responsibilities of the ISAG have increased significantly over recent years to support the 2020 change strategy and increasing cyber security risk. However, ISAG remain under resourced and consequently are unable to fully deliver their current remit.
- Supplier contracts typically define some requirements for security operations. However, suppliers are not reporting security incidents to Post Office staff in a timely or consistent manner.
- Information security engagement into business transformation projects is ad-hoc and reliant on the security awareness of the relevant project management.
- Security policies have been re-written and restructured into a comprehensive set of policies, frameworks and standards (including how data is classified). However, they are yet to be fully adopted and embedded into the business and appropriately assured.
- Lack of timely action in response to findings raised in a 2013 review of Information Security, of which many have been included in this review.

Conclusion

Overall, we identified several material findings in this review, but we also noted that the Post Office have agreed action plans related to each of these findings. Many of these are based on the updated agreed IT Strategy. Plans include budgets for the implementation of a range of technologies and associated processes to manage security operations; completion of outstanding penetration tests; updating security assurance processes and reviewing accountabilities for all aspects of information security. Successful, timely implementation of these is fundamental to ensuring cyber risk is managed appropriately and controls are of sufficient maturity for an organisation such as the Post Office, with the 2020 strategic ambition. Action will be required by all senior business leaders as well as IT and ISAG.

Critical to the success of any Information Security strategy is building a resilient culture of cyber awareness and behaviour throughout its business structures and operational practices. The Post Office has started this journey, but we feel that further focus is needed in this area. Cyber security is a business risk and requires action by all staff as well as ownership and leadership by business management in addition to IT and assurance.

Based on the work performed, as stated in the Scope and methodology sections, we have given our review of the benefits framework management within POL an adverse risk rating. An adverse report rating is defined as:

Inadequate internal control environment. A high number of non-compliance with internal and external guidelines and weaknesses in records, systems and controls were identified. Examples may include: reputational damage or inappropriate use of company assets.

POL00400101

Horizon Outage Lessons Learnt

Author: Rob Houghton Sponsor: Al Cameron Meeting date: 28 September 2016

Context

On Monday 9 May, the Horizon branch trading system failed. A high percentage of branches were unable to transact for 60-90 minutes. The outage took place as the system was returned to its primary server after a week successfully testing the operation of its secondary back-up server.

Memory utilisation levels on the primary database had become irregular following the failback. This caused severe degradation of service which could only be addressed by applying a memory control parameter and a systems reboot.

This resolution started to be effective after 15 minutes and was completely effective after a further 15 minutes. However, we identified a number of failings in our wider incident management process:

- Monitoring: Our monitoring was inadequate. Fujitsu misunderstood the first, clear warning sign on the Monday, worsening the outage. As a result, the seriousness of the issue was only identified because branches were unable to trade.
- Incident management: our internal management process was slow to be activated.
- Communication: We did not communicate with internal and external stakeholders as proactively as we would expect to. Our communication with branches was limited and messages were not heard.

There was limited customer and postmaster impact from incomplete or disputed transactions and these were dealt with through BAU procedures.

Questions

1. What caused the outage and what IT changes have been implemented?
2. Can we rely on the secondary systems and revert between primary and secondary?
3. What changes have we made to communications and incident management?

Conclusions

Cause and IT changes

4. Fujitsu and Oracle are unable to explain the root cause: Oracle considers this a unique incident, not experienced anywhere else in its worldwide estate. The same failover/failback exercise was replicated in the test environment but the symptoms could not be reproduced, preventing further analysis. The root cause therefore remains and is expected to remain inconclusive.

POL00400101

5. To mitigate a repeat of the incident, the memory control parameter is permanently applied to all databases.

6. Fujitsu monitoring systems did raise an alert. However, the monitoring threshold levels were too high which caused delay. Additional low level monitoring has been introduced into live production to provide an earlier alert of memory irregularities. The script is live and triggers an alert if a 1% change (previously 5%) occurs in a 10 second window. Post Office IT has real time access to the Fujitsu transaction processing monitoring tool which provides a service dashboard

Reliance on secondary servers

7. In a planned and tested exercise, approved by the Group Executive and supported by ATOS, Fujitsu and Oracle, on Saturday 3rd September the primary branch database was failed over to the back-up server. Horizon ran on the secondary server for a week and on the following weekend, the system was failed back to its primary server. No issues were experienced with either exercise and trading was not affected at any stage. Branches and the NFSP were briefed throughout.

Changes to communications and incident management

8. The incident management response has been revised and clarified with all participants. Fujitsu now directly alerts Post Office IT when it commences a technical investigation process. Clear information flow and joint working has been established with ATOS. The POL incident management team has been re-defined with clear roles and responsibilities defined and agreed.

9. A "Social" policy is now in place (developed with Marketing) for incident management that outlines what, who, when and under what circumstances. This has three levels of incident severity and what will happen under each scenario.

10. The Communications team has established representation on the incident management team. Team contacts are circulated each weekend with identified members of the team available to lead on issues arising.

11. A "standalone" (i.e. not reliant on Horizon) Network Status webpage has been developed to advise customers and agents of any network issues (current and future) (www.onepostoffice.co.uk/status).

Input Sought

12. The ARC is asked to review and comment on the lessons learnt.

POL00400101

Business Continuity & Crisis Management Project update

Author: Jonathan Waples Sponsor: Jane MacLeod Meeting date: 28th September

Executive Summary

Context

The Business Continuity Project Manager has been asked to review, revise and develop plans, materials, processes and infrastructure to draw our Business Continuity (BC) & Crisis Management (CM) disciplines in line with best practice guidelines, as defined by the Business Continuity Institute, and measured against ISO22301:2012 Societal Security – Business Continuity Management Systems (BCMS).

It is recognised that whilst the organisation is historically successful in reacting to business interruptions and critical incidents, the GE and the Board would gain significant confidence if the approach were formalised. It is expected that adopting such a formal response will improve resilience, reduce time taken to recover, and allow for more cost effective use of resources upon invocation.

The project started in late November 2015 and is divided into three phases:

- Phase 1: Gap analysis; policy creation; CM review; pilot BC activity
- Phase 2: Expanded BC activity; BCMS Framework delivery
- Phase 3: Improve BCMS awareness; BCMS integration to BAU.

In addition, the Business Continuity Project Manager's role involves providing significant assistance to the business with its ongoing BC and CM support needs, including assisting with planning for the potential of industrial action across the Network.

Questions this paper addresses

1. How have we progressed our plan?
2. How is this bringing us in line with ISO 22301?
3. What testing requirements are yet to be met?
4. What are the recommendations for continued BC best practice, post project?

Conclusion

1. How have we progressed our plan?
    a. The plan has been devised and shared with management and the sponsor; Phase one milestones have delivered a revised and improved Business Continuity policy (ARC approval, May) and Crisis Management

POL00400101

processes (end of April 2016), BPT workshop (June 2016) and cyber-breach exercise (July 2016).

b. Following greater engagement from BPT membership, Business Impact Assessments for multiple business areas are in progress which will enable the passage of BC plan development into BAU (as per Phase Two & Three) ahead of schedule. In consequence Phase 1 is complete and Phases 2 & 3 are well underway. See Appendix 1 for details.
c. Activity on BIAs was also hampered by the summer holidays, as well as the potential for industrial action. However, focus has been maintained on BIAs for Financial Services (a wrap-up meeting for the Savings Team BIA took place on Monday 12th September), Contact Centres and for Information Technology – see appendix 2. The focus on Contact Centres has enabled us to clearly identify requirements for our Work Area Recovery (WAR) contract with SunGard; develop the desktop (PC) for the WAR location; begin assessment of the optimal location for a recovery site to support Future Walk. Additionally, the re-utilisation of existing contracted services for WAR positions now provides for a minimal cover of 10 seats for use in London in support of Finsbury Dials.

2. How is this bringing us in line with ISO 22301?
    a. Planned progress was for 75% of achievement to conformity to ISO 22301 at this stage, which has been exceeded (82%), but most documentation requires testing and approvals.
    b. The delivery of Business Impact Analysis results - along with the development of resulting continuity plans - will progress from now until the end of the project.

3. What testing requirements are yet to be met?
    a. A testing schedule is in development, providing planning capability for BC, BPT and Crisis Management exercises through-out the calendar year. The schedule will be contained within, and supported by, the Business Continuity Exercising & Testing Schedule document, which also forms part of the BC Framework under ISO 22301:2012.
    b. Testing, for the purposes of project delivery, should include:
        i. BPT Invocation Testing – test time to invocation/ team response
        ii. Major Incident Response (MIR) Procedures Testing – to test process suitability and understanding of roles & responsibilities
        iii. Table top testing of individual business unit plans – fit for purpose tests
        iv. Scenario testing of specific response plans (staff abstraction/ industrial action/ building compromise) – fit for purpose tests

POL00400101

v. Work Area Recovery (WAR) provision testing (use of alternate premises) – end to end technology test; fit for purpose tests; process suitability and understanding of roles and responsibilities.

c. BPT & MIR testing has been conducted.
d. Table top testing will be scheduled to coincide with delivery of business unit plans through September.
e. Incorporation of MIR processes to industrial action response planning, and live deployment of these plans over the strike period superseded scenario testing of abstraction plans for present. The implementation of these plans for the IA Gold Team response was a great success, and enabled the management of the day's activities in line with the existing Major Incident Response processes.
f. Discussions underway with Computacenter, Atos and SunGard on update requirements for Work Area Recovery sites, in light of technology and location changes.

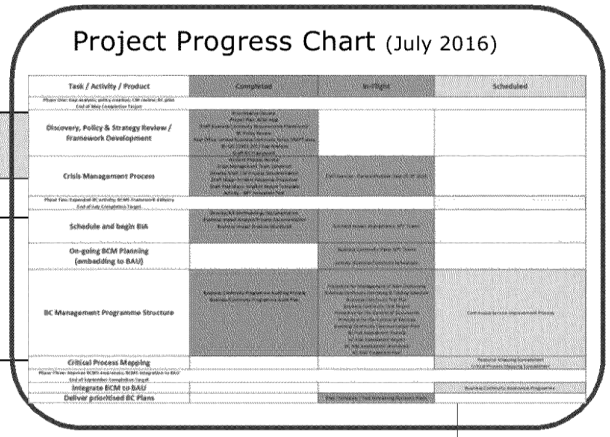
4. What are the recommendations for continued BC best practice, post project?
    a. The continued development of the BC Framework, specifically:
        i. Appointment of a permanent Business Continuity Manager, of appropriate experience, to ensure BC Framework is maintained, expanded and adhered to.
        ii. Incorporation of identified resource/ skills requirements & gaps into a skills matrix.
        iii. Review of externally provided BC services (SunGard Work Area Recovery sites), and their continued suitability.
        iv. Review of BC input during procurement process, with particular regard to on-going audit requirements.

Input Sought

The Committee is requested to review this report and highlight any input or suggestions it has on the project's goals or progress.

POL00400101

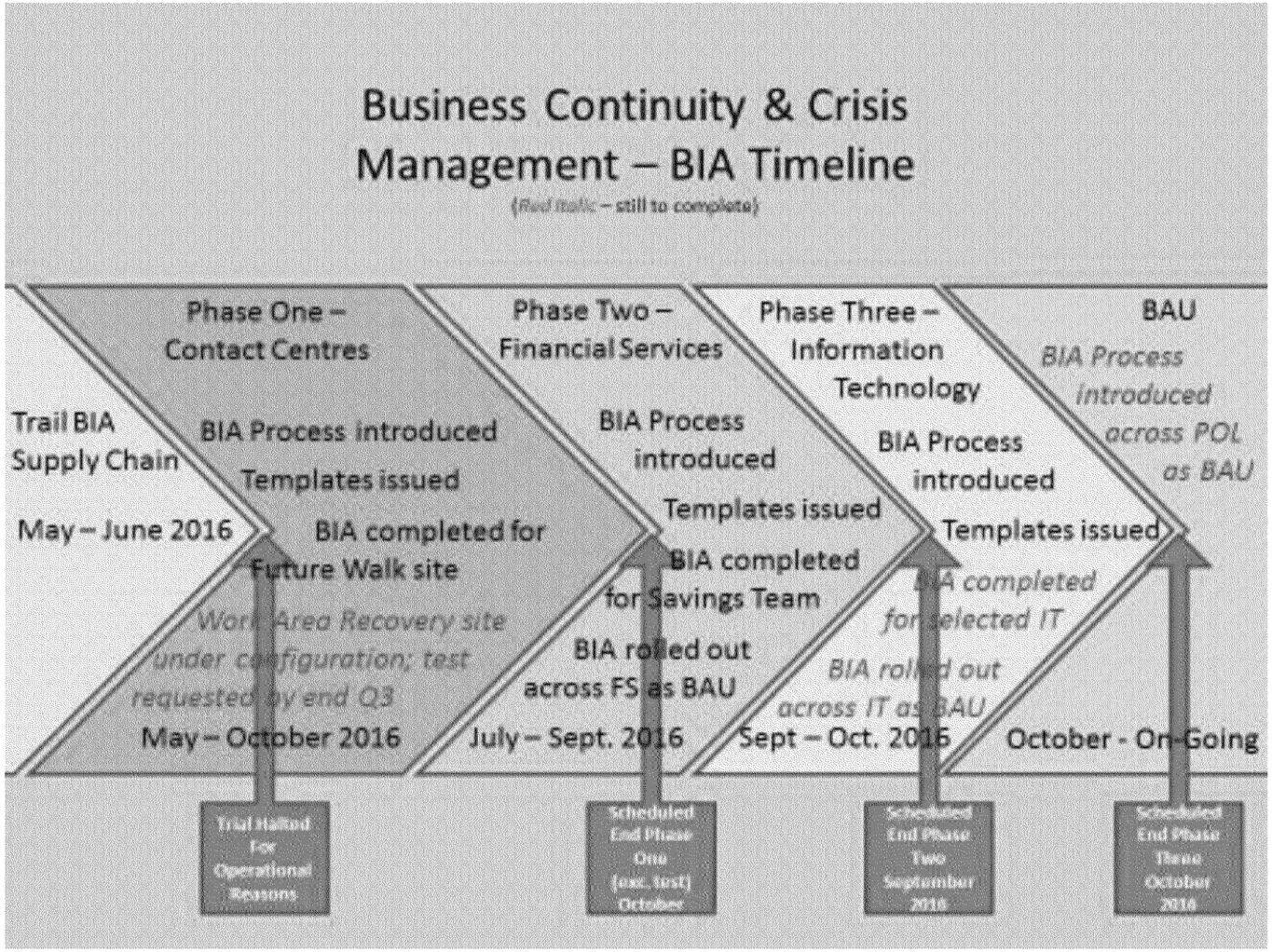
Appendix 1: Project Progress Chart (August 2016)



Task / Activity / Product	Completed	In-Flight	Scheduled
Phase One: Gap analysis; policy creation; CM review; BC pilot **End of May Completion Target**			
Discovery, Policy & Strategy Review / Framework Development	Prioritisation Review Project Plan: BCM.mpp Draft Business Continuity Requirements Framework BC Policy Review Post Office Limited Business Continuity Policy DRAFT.docx BS ISO 22301:2012 Gap Analysis Draft BC Framework		
Crisis Management Process	Incident Process Review Crisis Management Team Construct Develop Draft CM Process Documentation Draft Major Incident Response Procedure Draft Post Major Incident Report Template CMT Exercise - Earliest Possible Date Activity - BPT Invocation Test		
Phase Two: Expanded BC activity; BCMS Framework delivery **End of July Completion Target**			
Schedule and begin BIA	Develop BIA Methodology Documentation Business Impact Analysis Process Documentation Business Impact Analysis Workbook	Business Impact Assessments: BPT Teams	
On-going BCM Planning (embedding to BAU)		Business Continuity Plans: BPT Teams Activity: Business Continuity Rehearsals	
BC Management Programme Structure	Procedure for Management of Non-Conformity Business Continuity Programme Auditing Process Business Continuity Programme Audit Plan Skills and Training Needs Assessment Skills Development Survey Response Analysis Skills Development Survey Business Continuity Exercising & Testing Schedule BC Risk Assessment Process BC Risk Assessment Process BC Risk Assessment Report BC Risk Assessment Workbook BC Risk Treatment Plan Business Continuity Communication Plan	Business Continuity Test Plan Business Continuity Test Report Procedure for the Control of Documents Procedure for the Control of Records	Continuous Service Improvement Process
Critical Process Mapping			Resource Mapping Spreadsheet Critical Process Mapping Spreadsheet
Phase Three: Improve BCMS awareness; BCMS integration to BAU **End of September Completion Target**			
Integrate BCM to BAU			Business Continuity Awareness Programme
Deliver prioritised BC Plans		Plan / Schedule / Test Remaining Recovery Plans	

POL00400101

Appendix 2: Business Impact Assessment Timeline (August 2016)



POL00400101

AUDIT RISK AND COMPLIANCE COMMITTEE

AML and CTF Risk Update

Author: Sally Smith Sponsor: Jane MacLeod Meeting date: 28th September 2016

Executive Summary

Context

This paper updates the Audit Risk & 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 to progress the recommendations set out in the Promontory Report.

Questions this paper addresses

1. What is the current position on the HMRC Audit?
2. What is the current position on progress with the Promontory Report recommendations?

Conclusion

1. At this stage it is too early to tell what the findings will be from the HMRC audit, however we expect to receive HMRC's response by end October 2016 and we will provide the ARC with a full update including at the next ARC meeting in November.
2. The initial findings from the Thistle review (which are summarised in paragraph 16 below) indicate a number of findings which overlap with lessons learned and findings from the BCV fraud and contract management audit. Actions to address certain of these are being considered and, where appropriate, implemented.
3. Following receipt of the finalised risk assessment at end September, we will prepare a full response together with management actions and this, together with the status of the actions to address concerns, will be shared at the ARC in November.

Recommendation

4. The ARC is requested to note the status of the HMRC audit and the initial draft findings of the Risk Assessment work.

POL00400101

Update

HMRC Audit

5. HMRC have now confirmed that their audit approach will be confined to data analysis of Travel Money activity in the branch network. They have supplied a list of 1,111 branches for which they have requested 12 months transactional data relating to buy and sell on demand and branch pre-orders, including customer information, where this has been captured. The data was supplied to HMRC week commencing 19th September 2016.

6. HMRC advise that they may need to visit a few agency branches to validate their findings from the data analysis exercise. They are still expecting to get their report completed and issued by the end of October 2016.

7. HMRC have advised that their Policy Team have reviewed the cash processing that is undertaken by Supply Chain for MSB clients and they believe these may be within scope of 'Money Transmission' business and therefore within the regulations. Their interpretation would bring into scope all Supply Chain cash processing clients and we have requested Legal advice from Stephenson Harwood in this regard. HMRC have advised that they do not intend to bring these clients within scope of the audit as all relationships have been advised of termination of contract and will be exited by 5th November 2016.

Branch Premises Registration

8. All premises registrations are up to date and the new data extracts, reports and processes are now running as business as usual. We are reviewing accountability for the supply of this information to HMRC as current processes are cumbersome.

9. We are still awaiting a response from HMRC in relation to potential penalties and/or interest with respect to premises registration errors. A paper has been submitted setting out the reasons for the historic branch premises registration errors, we understand that the HMRC Registrations Team are seeking advice from the HMRC Policy Team.

AML/CTF training

10. Completion levels of AML/CTF compliance training delivered between March and May is as follows:

    - Back/Head Office Training – As of 15th August 2016, 96.5% completion. There are a number of colleagues who are leaving the business, and this has affected the take up of training.
    - Crown Office Training – 100% completion
    - Agency branches - 87% completion as of 24th August 2016 (being chased by Network)

Promontory Report Recommendations

11. One of the key recommendations of the Promontory report was that Post Office should undertake a risk assessment. To this end Post Office has engaged Thistle Initiatives to undertake a Post Office wide (including POMS) Financial Crime Risk Assessment.

12. The objectives of this risk assessment are to:

POL00400101

- Fulfil Post Office's regulatory requirement to conduct an annual financial crime (and in particular, AML/CTF) risk assessment;
- Conduct a review of POL's current AML framework including its human resources, products and services, channels, technology, policies, processes and procedures to work through risk exposure and any gaps or challenges taking into account the Promontory report and any findings from the HMRC audit; and
- Provide recommendations and solutions to enhance existing controls, design and implement the target state outcomes in line with the findings within the Promontory report and the results of the risk assessment.

13. Thistle's initial focus was on high risk priorities and consideration of the impact of current controls in relation to these risks. The methodology being used is to:

- assess the residual risk based on the assumption that the controls identified via the documents provided are working as planned
- estimate the likelihood of such controls working in terms of known incidents and outcomes of interviews conducted
- combine this information to provide an estimate of likely current residual risk

14. As at 15 September, Thistle had:

- Interviewed c. 17 individuals across all product areas;
- Visited the Grapevine helpdesk in Bradford, the Financial Crime operational team in Chesterfield and had an overview of Horizon functions in the Model Office;
- Been provided with c.300 documents for review (after allowing for duplication);
- Undertaken an initial review of available contracts (excluding BOI contracts); and
- Developed a comprehensive risk matrix to record and quantify inherent financial crime risks within Post Office products and services as well as enabling Thistle to record and quantify the residual risk that remains once all of the existing controls have been fully assessed.

15. Next key actions and delivery dates:

- Conclude the document review
- Complete interviews with GE members (currently scheduled to complete by 4th October 2016); and
- Deliver final draft residual risk report before 30 September 2016

16. Thistle's initial high level findings (which remain to be validated) include:

- Reputational risk is the single biggest risk to the PO brand. Focus on financial crime by regulators is increasing and may signal greater enforcement in this area. HMRC do not publish their penalties, but recent FCA fines of between £0.5m and £72m have largely related to failures by businesses to:
    - have robust policies and procedures;
    - adequately assess and acknowledge the risks to which the business was exposed;
    - establish and record an adequate commercial rationale for its products and services; and
    - have adequate oversight and handling of financial crime risks by senior

POL00400101

management.

- PO approach to managing and controlling financial crime risk is reactive and responsive in the main and there is insufficient resource internally to adopt a significant proactive approach commensurate with the risk.
- Retention and management of key contractual documentation is inconsistent; and provision of final executed copies of documents has been erratic. It is therefore not possible to establish whether the versions provided are the final execution copies.
- Current resourcing levels in the Financial Crime team impact the ability to monitor the effectiveness of, and maintain, controls at a level commensurate with Post Office's risk appetite.
- Access to appropriate and timely MI is dependent on third parties or is subject to the limitations of existing Post Office infrastructure.
- Recognition of the level of financial crime risk inherent in the Post Office business model is inconsistent across products and services and the supporting supply chains.
- Post Office is unable to demonstrate through appropriate evidence that it has had a robust governance and decision making framework in relation to financial crime.
- Provision of risk based training to all staff to ensure a relevant level of knowledge and understanding of the financial crime risks affecting the business and more specifically their role, is not fully operational.
- Risk and controls within Post Office do not appear to have been designed to operate at a granular product/service level that considers the inherent risks within the particular product/service.
- Financial crime MI is not at a granular product level to aid decision making therefore there is a risk that decision making may be skewed by considerations such as commercial and community support.

17. The next project phase is to verify the effectiveness of existing controls to determine the true residual risk and identify where on the path to desired residual risk each product sits. The project will then be able to make recommendations to address gaps where controls do not appear to exist and actions to ensure that existing controls work effectively. The final draft residual risk report is due before the end of September 2016. If these recommendations are received before the ARC on 28 September, a verbal update will be provided at that meeting.

18. As the risk assessment is a pre-requirement to closing a number of the Promontory recommendations, there have been no further Promontory Report recommendations closed since the last ARC update as summarised below. Subject to receiving the risk assessment, we expect that most of the outstanding Promontory actions will be closed by the end of November:

	Status			
Area	**Complete**	**In Progress**	**Not Started**	**Deferred**
Governance and Culture	1	2	0	0
Risk Assessment	4	7	0	0

POL00400101

Policies & Procedures	2	8	0	4
Monitoring Arrangements	0	4	0	0
Operation of Relevant Systems and Processes	0	0	4	0
Training, Awareness and Testing	1	5	0	0
Suspicion Reporting	4	2	0	0
MSB	4	0	0	3
Resourcing	0	3	1	0
TOTAL	**16**	**31**	**5**	**7**

POL00400101

BCV Fraud - Lessons Learnt

Author: Paul Hemsley/Angela Van-Den-Bogerd Sponsor: Al Cameron Meeting date: 28 September 2016

Executive Summary

Context

Between January 2015 and June 2016, we suffered repeated fraudulent batch control voucher ('BCV') losses, totalling £840k, net of £150k of recovered payments.

The BCV issue was identified by an existing FSC reconciliation process in early 2015. It was escalated to the internal security team and through them to the police. A number of amendments were made to internal processes which appeared to stop the fraud, only for it to recur with minor variations.

In the absence of a formal process, the existence of such a material fraud was not escalated to the CEO, CFO, RCC, ARC or the external auditors. When flagged by the Financial Controller, the 2016/17 ARA sign-off was delayed and additional costs of £80k incurred to enable EY to complete its work.

At the ARC on 25 July, we set out the detailed background to the fraud and the steps that would be taken to strengthen the processes and controls around the BCV process. The ARC requested that we report back on lessons learned and progress.

Questions

1. When will the BCV process be automated, preventing repetition of this particular fraud?
2. In the meantime, what has been done to manage the current BCV fraud risk?
3. Are the accountabilities for fraud management now clearly established?
4. What changes have been made to ensure that details of fraud will be formally captured and escalated in future? How does this become an established part of our culture?
5. What other changes need to be made to the management of fraud?
6. Is there evidence that frauds are now being escalated appropriately – and what further fraudulent activity has been identified?

Conclusions

Work is underway with the banks to automate the BCV process. Subject to any delays in third party arrangements, this is expected to be concluded by end December 2016. In the meantime, additional manual controls are in place and no further losses have been incurred.

The overall accountability for the management of fraud, together with responsibility for the Security Operations Team, will transfer to the Director of Support Services from 1 October. She is establishing a Financial Crime Forum with representatives from across the business. Accountability for policy and assurance remains within Corporate Services.

POL00400101

Responsibilities to report suspicions of fraud have been communicated across the leadership team and the FSC in Support Services. A formal fraud alert for material risks (over £50k exposure) has been implemented. Monthly reporting will be made to the Group Executive and summarised for the RCC and the ARC.

Other changes underway or in planning include removing backlogs in the FSC reconciliation processes, developing a formal Fraud Response Plan, reviewing accountability for losses caused by fraud and optimising recovery from culpable agents.

Suspicions of fraud are now escalated rapidly and openly. Four further frauds, smaller in value, have been identified, with details set out later in the report. These are under investigation and the losses, which may fall on Sub-Postmasters (SPMs) have not been finally quantified.

Input Sought

The ARC is asked to note and comment on the lessons learnt and the progress made.

The Report

Process automation

7. As flagged on 25 July, we are working with the banks to fully automate the BCV process, removing the manual forms and establishing a direct transaction interface from Horizon to the banks without the need for a third party intermediary. These changes are on track for completion by end December 2016 subject to final bank agreement.

Interim management of BCV

8. In the meantime we have enhanced manual controls, with additional resources in our FSC undertaking overnight reconciliations to identify suspicious transactions. Since the last ARC, two further frauds have been attempted. In both cases the attempt was identified quickly and the money recovered before it could be removed. No further losses have therefore been incurred, although this type of defence cannot be considered watertight.

9. Communications have been issued to the Network reminding them that BCVs must not be shared. Evidence including CCTV images has been shared with the Police team investigating. Communications have also been issued to staff advising that all fraud or suspected fraudulent activity must be reported to the Grapevine hotline, for onward transmission to, and investigation by Security Operations.

POL00400101

Accountabilities

10. While the Security team within Corporate Services has taken on fraud risk management activities, no function, team or individual had been formally delegated to act on behalf of the Group Executive to ensure the business has appropriate arrangements to: *prevent, detect and respond to fraud*.

11. From 1 October, the overall, operational responsibility and accountability will sit with the Director of Support Services, reporting to the CFO. Responsibility for policy and assurance will remain with Corporate Services, led by Sally Smith of the Financial Crime Unit. Job descriptions are being finalised.

12. The Head of Support Services is establishing a fraud forum with support from the Network and product teams and Corporate Services and is working with colleagues to agree a Fraud Response Plan. This will be shared with the ARC in November.

13. One area under review is the optimal allocation of losses from frauds. These are currently managed centrally, within Support Services, together with other debt and product losses. We are considering whether allocating losses to the product managers and network, depending on the nature of the fraud, would sharpen ownership and accountability. The fraud forum will also consider the policies around the recovery of fraudulent losses from culpable agents.

Escalation

14. Communications have been issued to the POL leadership team and colleagues in the FSC that any identified or suspected fraud should be reported formally via the Grapevine tool, managed by Security Operations.

15. A 'Fraud Alert' is now issued immediately by Security Operations where fraud losses are: over £50k, either single or systemic/ multiples, plus those which could attract media attention or Network wide impact. At a minimum this is sent to the CFO, General Counsel, Head of Support Services, the GE member(s) impacted and relevant Product Managers.

16. Additional monthly reporting of fraud, agents' debt and other losses is in development for the Group Executive. A summary of fraudulent activity will be shared with the RCC and the ARC on a quarterly basis.

17. Any "material" fraud should also be captured within the bi-annual Executive Declaration. The results of this declaration are shared with the ARC every six months and support the annual financial statements.

POL00400101

Other changes

18. The BCV fraud was detected by the existing FSC reconciliation process but outside the timescale in which the loss could be prevented: FSC reconciliations have not been produced to a specific SLA. The FSC has undertaken a review across its reconciliation processes and identified outstanding and aged work as follows:

Enquiries Open Items	Aged	2 Periods Old	1 Period Old	Current Period	Totals	Current %	1 Period Old %	2 Periods Old %	Aged %
Santander	12	213	276	685	1,186	57.76	23.27	17.96	1.01
Moneygram	19,564	2,383	4,922	3,635	30,504	11.92	16.14	7.81	64.14
Personal Banking	39	148	481	6,505	7,173	90.69	6.71	2.06	0.54
ATM Retracts	1,885	1,392	2,516	2,669	8,462	31.54	29.73	16.45	22.28
ATM	17	58	823	2,770	3,668	75.52	22.44	1.58	0.46
Travellers' Cheques	290	20	33	283	626	45.21	5.27	3.19	46.33
Lottery	1,640	2,511	32,839	149,320	186,310	80.15	17.63	1.35	0.88
Debit Cards	242	216	1,669	108,572	110,699	98.08	1.51	0.2	0.22
Missing Cheques	124	27	111	154	416	37.02	26.68	6.49	29.81
Unpaid Cheques	126	55	39	102	322	31.68	12.11	17.08	39.13
Bulk Cheques	96	674	2,032	14,153	16,955	83.47	11.98	3.98	0.57
Bureau	0	52	352	12,104	12,508	96.77	2.81	0.42	0
Cash	1	59	437	11,643	12,140	95.91	3.6	0.49	0.01
Totals	24,036	7,808	46,530	312,595	390,969	79.95	11.9	2	6.15

19. Temporary resource has been recruited to clear the immediate backlog, which is expected to reduce significantly by end October. A report on outstanding activity is reported to the GE monthly and the Fraud Forum will ensure that product managers agree SLAs with Support Services which will be met and reported against.

20. Planning is underway for Security Operations and Financial Crime teams to provide targeted anti-fraud training to the relevant teams within Support Services. The requirement to report any suspicion of fraud will be covered within induction training for both employees and contractors.

Other fraudulent activity

21. The emphasis on reporting appears to have been effective with the following additional fraudulent activity identified and reported on a timely basis:

- MoneyGram, IRRELEVANT Suspicions were reported in August by the FSC regarding transactions from one branch repeatedly reversed but not cancelled with MoneyGram. 46 fraudulent transactions were processed totalling c£160k. The transactions were carried out by an individual employed by the SPM on a casual basis, who was not registered with HR and who was paid cash in hand. Delay in identification – the fraud took place in March - was a result of MoneyGram not identifying this activity under their transaction monitoring and the FSC reconciliation backlog.

POL00400101

It has been confirmed that this is an isolated incident for MoneyGram, with additional checks underway on equivalent products. A manual process to review a reversals report is being trialled by the Fraud Analysis Team. The SPM is contractually liable for the loss but is disputing this with the support of the NFSP. Communications for SPMs reminding them of their accountabilities are planned for October. In addition to better and more rapid monitoring, the business is considering the structure of the reversals process and an investment to strengthen unique user IDs on Horizon.

- Santander cash withdrawal (2 incidents) – business cheques. Under the Santander contract, business and corporate customers can use Post Office to make an emergency withdrawal using a cheque. The Santander cash cheque authorisation process is independent of Horizon. The sort code and drawer name are not captured which makes monitoring for potential non-conformance very difficult. There have been two incidents where branches have failed to follow the Santander emergency withdrawal by cheque process which have resulted in fraud.

  In one case, identified by the Fraud Analysis team in July, the SPM is claiming that the transactions, totalling £170k, had been authorised by Santander, which the bank cannot confirm. An investigation is underway. In the other, worth £150k, the issue was identified by Santander, the SPM has accepted that he processed the cheques without the right authorisation and has agreed a repayment plan which is now active.

- Transcash with Santander. Suspicions were reported by Santander following cheques being accepted for 15 'SAN 20' transcash payments between August and September at nine branches, totalling £126,000. The cheques credited three different Santander accounts. The only acceptable method of processing SAN20 transcash payments is by either cash or debit card, unless the payment is being made to a registered charity where an exception is made. Santander treated these transactions as cash payments and therefore they immediately credited the customer's accounts. All transactions were just below the threshold limit - £10K. Contractually, the branches are liable for the losses under non-conformance.

  The bank accounts where the deposits have been credited are now blocked and we have managed to freeze c£49,100. A memoview and national text blast was been issued to the Network on 16th September reminding branches of the SAN20 transaction process (i.e. not to accept cheques). The Fraud Analysis team are reviewing transcash payments relating to this period and CCTV from the affected branches has been requested. A response team has been established (with business owner Martin Kersley leading) to urgently review processes including dishonoured cheque process, potential mitigations and establishing whether there have been any other historical instances.

POL00400101

POST OFFICE
AUDIT, RISK AND COMPLIANCE COMMITTEE

8) Policy Framework Project – Update & Policy Approvals

Author: Mike Morley-Fletcher Reviewer: Jane MacLeod Meeting date: 28th September 2016

Executive Summary

Context

The purpose of the Policy Framework Project ("PFP") is to ensure that we know what our key policies are and that they are up to date, implemented and that we can demonstrate this to the Board and third parties. The project has developed a benchmarked Key Policy Framework comprising of a suite of 23 key policies. Policies have been reviewed to determine which need re-drafting or developing. Once drafted, a gap analysis has been performed and any further remediations or compliance activities identified and costed. In addition, further actions may be needed to communicate awareness of the policies, provide training and ensure compliance.

Questions?

POLICY DRAFTING

1) What is the status of drafting or redrafting key policies?
2) What implementation issues does the Gap Analyses highlight?
3) What are the next steps?

SUPPORTING POLICY FRAMEWORK PROCEDURES

4) What key supporting processes are required and what is their status?

Conclusion

POLICY DRAFTING:

1) Of the 23 key polices, 11 were identified as needing drafting or redrafting and this has been completed: 2 have been approved previously (May RCC/ ARC), 5 have been approved by the RCC (July & Sept) and are presented for approval to this ARC. The final 4 will be presented for approval in the near future. See appendix 1 Governance Approvals Calendar for further details. This has been created to ensure that all key polices are reviewed by the policy Owner/ Sponsor on (at least) an annual basis and their assessment reported to the RCC and ARC.

2) For the 5 policies presented, gap analyses, with costings, have been completed to highlight what is needed to operationalise the policy and enable compliance.

   There are expected to be additional costs for the financial crime policies (Financial Crime, Anti-Bribery & Corruption, Anti-Money Laundering), dependent on the outcome of risk assessments currently being conducted and consideration of POL's risk appetite and regulatory obligations. In summary:

   - Budgeted costs: the risk assessments have already been budgeted for. The training, communication and awareness, and enhancing internal procedures should not create additional cost and should be managed within existing budgets and resource – refreshed ABC training has been developed recently and is running currently.
   - Additional costs: depending on the outcome of the risk assessments and Success Factors' functionality, additional legal costs, resources and systems enhancements would be needed. These will be assessed in parallel with the development of remediation plans to ensure that responses are proportionate.

   For the other 2 policies, the gap analyses have not identified significant further actions, except for consideration of communication and training needs.

POL00400101

3) The remaining 4 policies are being progressed and the intention is to present them for approval as soon as possible:
    - Conflict of Interest and Business Change Management are going through final policy owner sign off - expected to be ready for November RCC/ ARC.
    - Vulnerable Customer is awaiting appointment of a new policy Implementor who will conduct a gap analysis. The intention is to enhance procedures over time, but ensure that minimum legal standards are in place currently. The policy Sponsor will report progress to RCC/ ARC on an annual basis, per the Governance Approvals Calendar – the next report will be March 2017.
    - Treasury Risk Management has been drafted and reviewed by relevant stakeholders but is being held back for review from the new Treasurer - expected to be presented for November RCC/ ARC.

SUPPORTING POLICY FRAMEWORK PROCEDURES:

4) We have identified several procedures that will help ensure the efficient and effective approval, maintenance, communication, training and review of our key policies and drafting is progressing. In particular:
    - a new intranet page has been set up on SharePoint under "Help to do your job". It is quite basic at present, but the Communications team is helping to make it more informative. Once approved, policies will loaded and Corporate Services will promote the site in October.
    - also, Corporate Services will be producing an Annual Calendar of Communications to co-ordinate messages to colleagues, which will include communications on policies.

Input Sought

ARC is asked to review this paper and invited to provide feedback and comments. In particular to ratify:

1) the progress to date
2) the 6 key policies submitted for approval
3) the supporting framework policy procedures identified and the progress to date.

Appendices

Appendix 1: (23) Key Policies - Governance Approvals Calendar
Appendix 2: Draft of Policy for Approval – Financial Crime
Appendix 3: Draft of Policy for Approval – Anti-Bribery & Corruption (incl. Gifts & Hospitality)
Appendix 4: Draft of Policy for Approval – Anti-Money Laundering (incl. Counter Terrorism, Sanctions)
Appendix 5: Draft of Policy for Approval – Investigations
Appendix 6: Draft of Policy for Approval – Physical Security

POL00400101

Appendix 1: (23) Key Policies - Governance Approvals Calendar – sorted by month order

The Policy Manager (in the Central Risk Team) will brief Policy owners/ implementors on details are required for the cyclical review.

Key to colouring: Blue = policy exists and is approved, Green = for approval/ noting at this ARC, Yellow = policy being redrafted/ still to be approved

Policy Update	Owner	Jan	Mar	May	Sept	Nov	To Board?
1) Board Constitution	Jane MacLeod	As required	As required	As required	As required	As required	Yes
6) Investigations	Jane MacLeod	RCC					
11) Financial Crime	Jane MacLeod	RCC & ARC					
12) Anti-Bribery and Corruption (incl. Gifts & Hospitality Policy)	Jane MacLeod	RCC & ARC & BOARD					Yes
13) Anti-Money Laundering (incl. Counter Terrorism, Sanctions)	Jane MacLeod	RCC & ARC & BOARD					Yes
14) Prosecution (England and Wales)	Jane MacLeod	BOARD					Yes
15) Physical Security	Jane MacLeod	RCC & ARC					
23) Health & Safety	Neil Hayward	ARC & BOARD					Yes
2) Conflicts of Interest	Jane MacLeod		RCC & BOARD				Yes
3) Enterprise Risk	Jane MacLeod		RCC & ARC				
4) Internal Audit (IA Charter)	Jane MacLeod		ARC				
5) Whistleblowing	Jane MacLeod		ARC & BOARD				Yes
17) Code of Business Standards	Neil Hayward		Board				Yes
18) Customer Treatment/ Vulnerable Customers	Martin George		RCC & ARC				
20) Business Change Management	David Hussey		RCC & ARC				
21) Accounting and Reporting (reviewed annually as part of accounting policies year end procedures)	Alisdair Cameron			ARC			
22) Treasury Risk Management	Alisdair Cameron			ARC			
7) Cyber & Information Security	Jane MacLeod				RCC & ARC		
8) IS - Acceptable Use	Jane MacLeod				RCC		
9) Business Information Systems	Jane MacLeod				RCC		
10) Information Assurance (incl. Data Protection)	Jane MacLeod				RCC		
16) Business Continuity	Jane MacLeod				RCC & ARC		
19) Social Purpose - Distribution Network Coverage	Kevin Gilliland	As required	As required	As required	As required	As required	Yes

Note: May and November kept as free as possible for interims and year end

POL00400101

Appendix 2: Draft of Policy for Approval – Financial Crime

Appendix 3: Draft of Policy for Approval – Anti-Bribery & Corruption (incl. Gifts & Hospitality)

Appendix 4: Draft of Policy for Approval – Anti-Money Laundering (incl. Counter Terrorism, Sanctions)

Appendix 5: Draft of Policy for Approval – Investigations

Appendix 6: Draft of Policy for Approval – Physical Security

POL00400101

Post Office Group

Financial Crime Policy

POL00400101

Contents Page

POL00400101

Document Control Sheet

SUMMARY			
GE Policy Sponsor	**Policy Owner**	**Policy Implementor**	**Policy Approver(s)**
General Counsel **Jane MacLeod**	Head of Security and Financial Crime (MLRO) **John Scott**	Senior Security Manager, Financial Crime **Sally Smith**	Post Office **RCC and ARC Committees**
Version and Status:	**Policy Review Period**	**Effective From :**	**Policy location:**
Final V0.7	Annually from policy effective date	[To be confirmed]	Z:\NEW COMPLIANCE\New Policy Framework 2015\Refreshed Policies 2016

DOCUMENT REVISION HISTORY			
Version	**Date**	**Author**	**Reason For Change**
Draft v0.5	25th April 2016	Mark Rodgers	Re-aligned to become the Financial Crime Policy & Owners review
Final v0.6	27th April 2016	Jane Macleod	Sponsor/ Exec Owner sign off
Final v0.7	13th June 2016	Sally Smith/Susan John	Amendments following controls 'gap' check

POLICY APPROVAL		
Role/Forum	**Name**	**Date**
Executive Owner and Sponsor	General Counsel (Jane MacLeod)	30 March 2016
Executive Committee	Post Office Risk and Compliance Committee (RCC)	[To be confirmed]
Board Committee	Post Office Audit, Risk and Compliance Committee (ARC)	[To be Confirmed

DOCUMENT DISTRIBUTION STATUS			
Distribution (Mark x as appropriate)		Document Sensitivity (Mark x as appropriate)	
Internal Only	X	Non-sensitive	
External Only		Sensitive	X

QUALITY STATEMENT	
Quality Control	Next review date
This document is periodically reviewed and at least once each year starting from the last effective date. This policy has been reviewed against the latest Post Office policy standards.	[To be confirmed]

POL00400101

Section A. Introduction

Chief Executive's Note

The Post Office Group ('Post Office') is committed to doing things correctly. Our Business Standards are our code of behaviours that represent the conduct we expect. This policy supports the code to help us ensure the highest standards of financial crime prevention, detection and management are maintained.

This policy sets out what is and is not acceptable but if you have any doubts or questions, these should be referred in the first instance to the policy owner, The Head of Security and Financial Crime ("MLRO") (see section E for the definition of "MLRO"), who oversees compliance with this policy. It is essential that all employees read this policy.

Introduction by the Group Executive Policy Owner: General Counsel

As Post Office's General Counsel and the Group Executive Policy Owner I have overall accountability for the management of financial crime to the Board of Directors. Post Office's Audit, Risk and Compliance Committee considers financial crime as an agenda item and the Post Office Board is updated as necessary.

POL00400101

Section B. Context

About this Policy

The purpose of this policy is to provide a framework to enable the effective management of financial crime risks to which Post Office may be exposed.

The policy defines the minimum standards to which Post Office shall operate to minimise the likelihood of financial loss, customer impact, regulatory breaches and reputational damage in line with Post Office's financial risk appetite.

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

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

In this policy employees refer to permanent staff, temporary including agency staff, contractors and consultants.

Financial crime risks are reviewed by the Financial Crime on a regular basis. This policy's effective date will be determined by the date on which final approval is given by the appropriate governance forum.

What is financial crime?

Post Office is exposed to several risks arising from the threat of behaviour leading to financial crime, both internal and external. Failure to manage financial crime risks and incidents appropriately could result in financial loss to Post Office, customer impact, regulatory breach, and/ or damage to the Post Office's reputation. These risks include, but are not limited to, the following:

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

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

POL00400101

Internal Financial Crime

The risk of internal events arises because of acts of a type intended to defraud, steal or misappropriate assets/property, or which seek to circumvent regulations or the law applicable to Post Office or Post Office policy which involves at least one internal party. Examples would include:

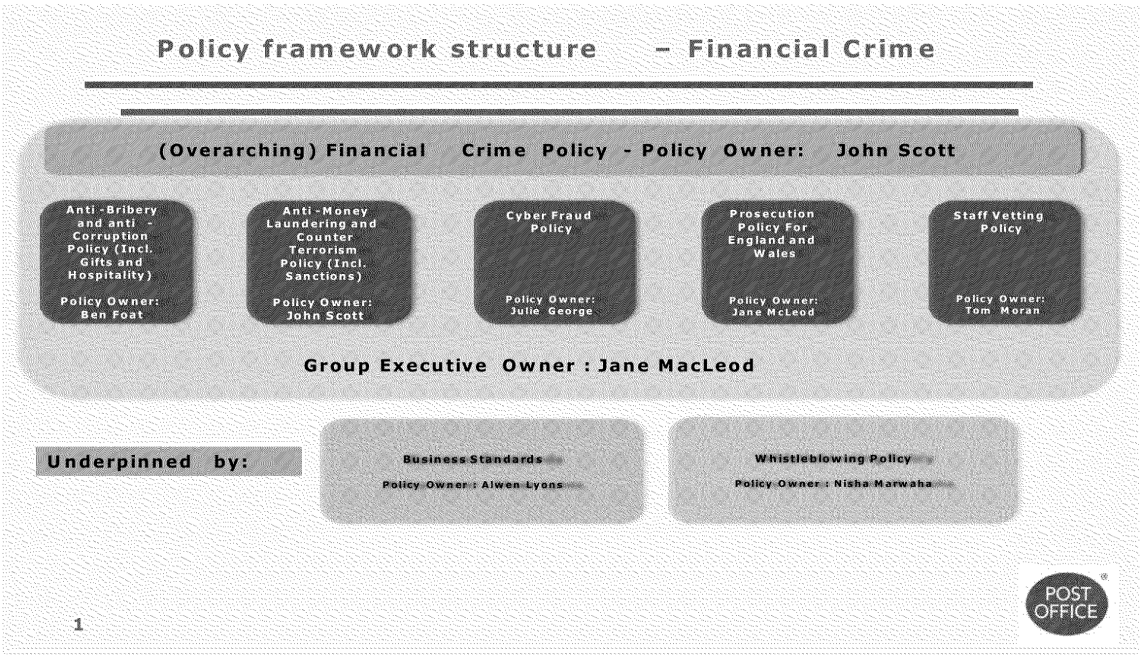
- Any dishonest or fraudulent act,
- Profiteering as a result of insider knowledge of Post Office activities,
- Theft of assets from Post Office or its customers,
- Manipulation of transactional data at Point of Sale,
- False expense or payroll claims,
- Manipulation of Post Office accounts or financial statements, and
- Breach of internal processes or controls for personal gain.

Risk Appetite

The Post Office's risk appetite is intolerant of non-compliance with law and regulations or deviation from its business conduct standards. Post Office has a risk-based tolerance to financial crime. This policy reflects this appetite and sets out controls to reduce and/or mitigate any such risks.

How we manage financial crime

This policy is Post Office's overarching key financial crime policy forming a broad suite of related policies. It overarches the financial crime policy framework as shown below, and each policy should be considered and read in conjunction with each other policy where relevant.



POL00400101

Who is responsible

Post Office's Board of Directors have overall responsibility for ensuring that Post Office has a framework to ensure compliance with legal and regulatory requirements. The Board is kept abreast of relevant matters relating to the management of financial crime by reports from its committees including its Risk & Compliance Committee and ARC Committee. The key individuals and their specific responsibilities in relation to this policy are:

ROLE	RESPONSIBILITY
Policy Owner	The policy owner will review this Policy on an annual basis or upon change in relevant legislation.
General Counsel	The General Counsel who is a member of the Post Office Executive is the Executive Owner and Sponsor of the Financial Crime policy. The General Counsel is accountable to the CEO and to the Post Office Board overall.
Head of Security and Financial Crime (MLRO)	The Head of Security and Financial Crime (MLRO) is the Owner of the Financial Crime Overarching Policy and is responsible for the day to day implementation and compliance with this Policy. The Head of Security and Financial Crime (MLRO) is accountable to the General Counsel.
Senior Security Manager, Financial Crime and AML	The Senior Security Manager, Financial Crime and AML is the policy implementer and is accountable to the Policy owner. The Senior Security Manager, Financial Crime and AML, may delegate duties to an appointed person. The Senior Security Manager, Financial Crime and AML, (and/or the appointed person) has responsibilities which include, but are not limited to: • Acting as the focal point for financial crime issues • Promoting the compliance culture by communicating the financial crime controls and standards which drives ownership and accountability throughout Post Office • Overseeing financial crime activities ensuring processes, procedures and controls are compliant with the Policy and/ or local laws • Ensuring effective governance arrangements are in place within Post

POL00400101

	Office to effectively monitor and manage financial crime risks • Ensuring there are effective mechanisms in place to identify and investigate potential non-compliance with this Policy including adequate risk assessment and conformance activities • Providing regular updates to the MLRO
Senior Management / The Head of each Business Unit	Senior Management / The Head of each Business Unit has ultimate responsibility for ensuring that their respective business areas establish systems and controls to comply with this Policy, whether they are performed by the business or outsourced to third parties. These responsibilities include but are not limited to: • Taking a full account of this Policy when entering into new products or sales channels, implementing new systems or expanding the business operations including branch network design • Ensuring that any reliance on third parties or service providers for compliance with this Policy meet the requirements of this Policy • Ensuring all relevant employees receive appropriate training with the support of the MLRO and Financial Crime Team • Ensuring all relevant employees understand their obligation to prevent the use of the Post Office for the purpose of financial crime in general • Ensuring immediate reporting of any breach or suspected breach of this Policy to the MLRO and Financial Crime Team
Employees (Staff and Agents)	All Staff and Agents are responsible for ensuring they comply with the terms of this Policy and complete financial crime training as required

Who must comply and how

Compliance with this policy is mandatory for all Post Office employees, officers, contractors, casual workers and agency workers. This policy applies wherever in the world Post Office's business is undertaken. All third parties who do business with Post Office, including consultants, suppliers and business and franchise partners, will be asked to agree contractually to this policy or to comply with their own equivalent policy.

It is important that all Post Office employees read, understand and comply with this policy. Failure to comply with financial crime requirements may result in personal liability such as fines and imprisonment. Employees who fail to comply with this Policy may be subject to disciplinary action up to and including dismissal.

POL00400101

If an employee has reasonable grounds to believe or suspect that a breach of this policy has occurred or may occur, he/she must notify his/her line manager in the first instance, as soon as possible.

Employees may request a policy exception or waiver to this policy, but you must follow the Post Office's exceptions and waivers procedures which can be obtained from the Head of Security and Financial Crime (MLRO).

If non-compliance is identified the matter must be referred to the Policy Owner, the Head of Security and Financial Crime. Any investigations should be carried out in accordance with Investigations Policy. If the cause is found to be due to wilful disregard or negligence, it will be treated as a disciplinary offence.

POL00400101

Section C. Policy Details

Information

Post Office complies with relevant UK legal and regulatory requirements including:

- The Fraud Act 2006 (excluding Scotland),
- The Theft Act 1968 (excluding Scotland),
- Common Law Offences of Fraud in Scotland,
- The Proceeds of Crime Act 2002,
- The Terrorism Act 2000,
- The Money Laundering Regulations 2007,
- JMLSG: Prevention of Money Laundering/Combating Terrorist Financing,(2014 Revised Version),
- HMRC - Anti-money laundering guidance for money service businesses,
- Computer Misuse Act 1990,
- Forgery and counterfeiting Act 1981, and
- Identity Documents Act 2010.

Our Controls

These minimum standards provide the requirements under which Post Office shall manage its financial crime risks. Business Units (see Section E for definition) must identify, assess and manage their internal and external financial crime risks as follows:

Financial Crime Risk Assessment

- New products and services and changes to existing products and services that are delivered or serviced through Post Office branches, call centres or Internet sites must be risk assessed and assured by the Financial Crime Team.
- Whenever risks are identified, each risk must be assessed and where appropriate mitigating controls must be put in place.
- The head of each Business Unit has ultimate responsibility for ensuring that a formal risk assessment is undertaken and that adequate controls are in place.
- Business Units must consider both internal and external risks together with any relevant market developments and/ or trends, when implementing or revising a process, system, product, service or channel and engage with relevant stakeholders.

Incident Management

- Business Units must assess and investigate where appropriate, all alleged or actual incidents and if internal or external financial crime is suspected, irrespective of whether these have resulted in loss to the Post Office or its customers, it must be reported to Grapevine by telephone on GRO
- Each Business Unit must have processes in place for reporting both internal and external financial crime incidents to Grapevine by telephone on GRO

POL00400101

- Post Office will seek to recover, where it is cost effective to do so, all assets of which Post Office or its customers have been stolen, defrauded or otherwise loss as a result of financial crime, and where appropriate, pursue legal remedies to effect such recoveries.

Risk Controls

The Post Office takes a risk based approach to managing financial crime and will take reasonable measures to prevent, deter and detect financial crime activity against it, whether arising from the actions of internal or external parties. It will conduct:

- Pre-Employment Screening for all employees,
- Due Diligence for third parties as required, and
- Monitoring for financial crime activity against the Post Office.

Business Units must test the adequacy and effectiveness of key controls and key risk indicators should be in place to highlight any potential control issues.

Business Units must identify, monitor and report any financial crime losses to the Post Office Financial Crime Team and Risk & Compliance Commitee. Details of losses and the cause of the loss will be reported regularly to the Post Office ARC by the General Counsel.

POL00400101

Section D. Governance

How do we monitor compliance

The Head of Security and Financial Crime (MLRO) will ensure that this policy is implemented, reviewed and remains effective. Post Office internal systems of risk control ensure that financial crime controls in this policy are regularly independently assessed for effectiveness, suitability and adequacy. Post Office Internal Audit retains independent third line oversight with regard to this policy.

The Head of Security and Financial Crime (MLRO) assisted by the Senior Security Manager assess compliance with this policy on a regular basis and regular reports will be issued to Post Office's RCC and to the ARC Committee.

Post Office requires third parties who do business with them to have at least equivalent arrangements, systems and controls to this policy.

How to raise a concern

Any Post Office employee who reasonably suspects dishonest or fraudulent activity has a duty to:

- discuss the matter fully with their Line Manager; or,
- report any breach, crime or suspicions by telephoning Grapevine on GRO GRO ; or,
- Bring it to the Post Office's attention independently of management, via the Speak Up Line (see Section E for more information).

Contact us and more information

- **If you need further information about this policy or wish to report an issue in relation to this policy , please contact** John Scott – Head of Security and Financial Crime (MLRO) on GRO or by email at **john.m.scott** GRO

POL00400101

Section E Key Terms and References

Key Terms

Term or Acronym	Description
MLRO	Money Laundering Reporting Officer
Business Unit	A specific business function or area within Post Office (currently: Financial Services, Commercial, Network, Finance, People & Engagement, Transformation, Corporate Services)
Post Office Group ('Post Office')	Post Office Limited and all subsidiaries and entities within the Post Office Group which includes Post Office Management Services ("POMS")

References	Description
Whistle-Blowing Policy	In case of concerns staff may contact their line manager, a senior member of the HR Team, or if either or both are not available staff may contact Post Office's General Counsel, Jane MacLeod 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

POL00400101

Post Office Group

Anti-Bribery and Anti-Corruption ("ABC") Policy

(Incorporating Post Office Gifts and Hospitality Policy)

POL00400101

Contents Page

POL00400101

Document Control Sheet

POLICY SUMMARY			
GE Policy Sponsor	Policy Owner	Policy Implementor	Policy Approver(s)
General Counsel **Jane MacLeod**	Head of Legal – Financial Services **Ben Foat**	Head of Risk and Assurance **Mike Morley-Fletcher**	Post Office **RCC and ARC Committees**
Version and Status:	Policy Review Period	Policy - effective date :	Policy location:
Current : Draft V1.6	Annually from policy effective date	To be confirmed	Z:\NEW COMPLIANCE\New Policy Framework 2015\Refreshed Policies 2016

DOCUMENT REVISION HISTORY			
Version	**Date**	**Author**	**Reason For Change**
Draft v1.0	4th March 16	**Ben Foat**	1st draft for new policy framework
Draft v1.1	10th March 16	**Mark Rodgers**	Standards and review of v1.0 draft
Draft v1.2	18th March 16	**Mark Rodgers**	Updating feedback from key business role holders
Draft v1.3	21st March 16	**Mike Morley Fletcher**	Head of Risk sign – off readiness Review
Draft v1.4	30th March 16	**Jane MacLeod**	Sponsor review and policy sign – off
Draft v1.5	30th March 16	**Ben Foat**	Owner review and incorporate changes requested
Draft v1.6	21st June 16	**Mike Morley-Fletcher and Mark Rodgers**	Feedback following controls gap analysis with Policy Owner and feedback from POMS

POLICY APPROVAL		
Role/Forum	**Name**	**Date**
Executive Owner and Sponsor	General Counsel (Jane MacLeod)	30 March 2016
Executive Committee	Post Office Risk and Compliance Committee (RCC)	[To be confirmed
Board Committee	Post Office Audit, Risk and Compliance Committee (ARC)	[to be confirmed]

DOCUMENT DISTRIBUTION STATUS			
Distribution (Mark x as appropriate)		Document Sensitivity (Mark x as appropriate)	
Internal Only	x	Non-sensitive	
External Only		Sensitive	x

QUALITY STATEMENT	
Quality Control	Next review date
This document is periodically reviewed and at least once in each 12 month period starting from the last policy sign off date. This policy has been reviewed against the latest Post Office policy standards.	[to be confirmed]

POL00400101

Section A. Introduction

Chief Executive's Note

The Post Office Group ('Post Office') is committed to doing things correctly. Our Business Standards are our code of behaviours that represent the conduct we expect. This policy supports the code to help us ensure the highest standards are maintained, including a zero tolerance to bribery and corruption. This policy sets out what is and is not acceptable but if you have any doubts or questions, these should be referred in the first instance to the policy Owner, the Head of Legal – Financial Services who oversees compliance with this policy. It is essential that you read this policy.

Introduction by the Group Executive Policy Owner: General Counsel

As Post Office's General Counsel and the Group Executive Policy Owner and Sponsor I have overall accountability to the Group Executive and the Board for ensuring that Post Office has appropriate controls in place to meet its Anti-Bribery and Anti-Corruption ("ABC") obligations. Post Office's Audit, Risk and Compliance Committee ("ARC") considers ABC risks as an agenda item and the Post Office Board is updated as required.

POL00400101

Section B. Context

About this Policy

The purpose of this policy is to manage Post Office's bribery and corruption risks. Post Office is committed to ensuring that its activities are free from any form of bribery and corruption.

This policy sets out what we must all do to prevent and manage the risks associated with bribery and corruption in the context of our risk appetite and seeks to support the wider national fight against financial crime.

Bribery and corruption risks are reviewed with relevant individuals (see "Who is responsible") on a regular basis and at least half yearly.

This policy enables us to comply with our obligations under applicable legislation and with regulatory requirements. It also protects Post Office's brand and reputation.

This policy's effective date will be determined by the date on which final approval is given by the appropriate governance forum.

Note: it includes our Gifts and Hospitality Policy in Appendix 1.

What is Bribery and Corruption?

Post Office is subject to the UK Bribery Act 2010 (Bribery Act) and could become criminally liable as a result of an act of bribery or corruption by its employees or Associated Parties (see Section E for definition of this term).

Under the Bribery Act, it is an offence to:

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

The Bribery Act has extra-territorial effect which means that the actions of an Associated Party (see section E) outside of the UK may fall within the scope of the Act. In the context of Post Office, this could apply where a Post Office contractor resides outside the UK.

Moreover, under the corporate offence, Post Office may be held liable for failing to prevent bribery by its employees or Associated Parties unless it can demonstrate that it had in place "adequate procedures" designed to prevent this type of misconduct. The controls outlined in this Policy, including appendices, assist Post Office in

POL00400101

preventing and detecting corrupt conduct and form an essential component of Post Office's adequate procedures.

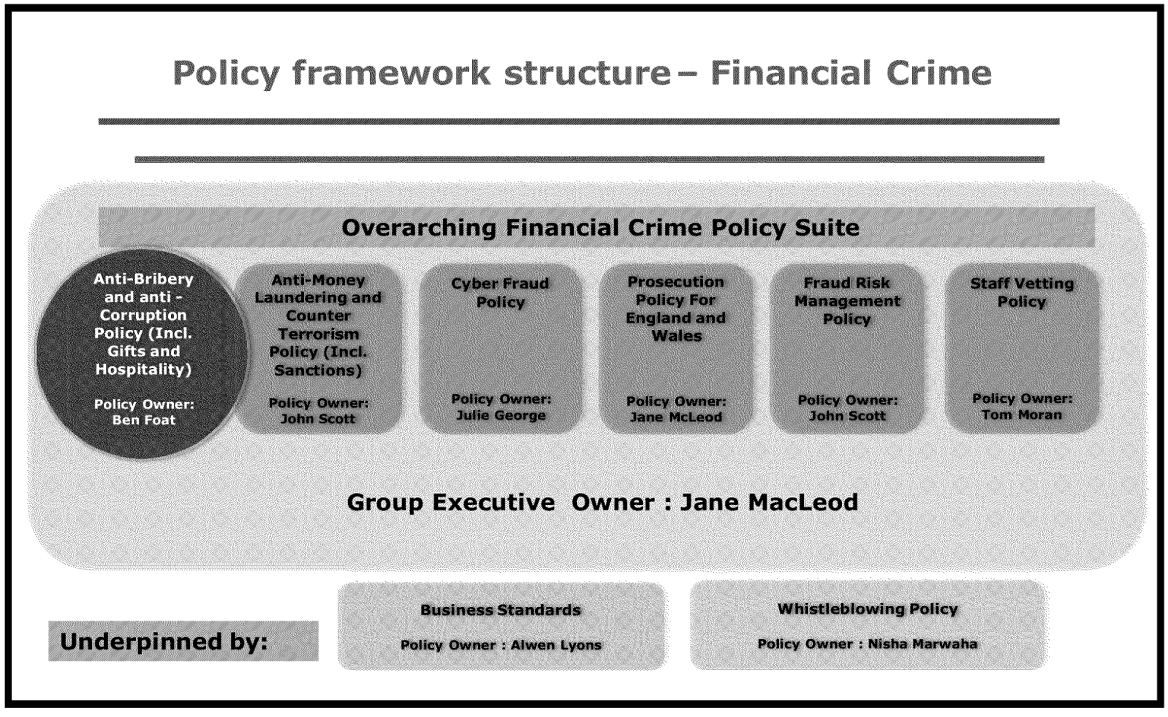
Post Office Ltd must also comply with particular regulatory obligations arising through contracts with directly regulated companies or directly through its subsidiary, Post Office Management Services (POMS). As an Appointed Representative of each of the Bank of Ireland and POMS, Post Office Ltd is contractually obliged to comply with certain regulatory obligations including ensuring adequate systems and controls to mitigate against Financial Crime risks are in place. POMS is directly exposed to regulatory fines and censure if the FCA determine that the systems and controls associated with this Policy are not effectively implemented. This Policy contributes to Post Office's compliance with these regulatory obligations.

Risk Appetite

The Post Office risk appetite is intolerant for non-compliance with law and regulations or deviation from its business conduct standards. Post Office has a zero tolerance to bribery and corruption risks. This policy reflects this appetite and sets out controls to reduce and/ or mitigate any such risks.

How we organise ABC risk management

This policy sits within a broader Financial Crime family policy structure. It is one within a suite of policies and each should be read in conjunction with the others. Our Financial crime policy structure is shown below highlighting the ABC Policy.



(See Section E for policy descriptions)

POL00400101

Who is responsible

Post Office has a framework to ensure compliance with legal and regulatory requirements. The Board is kept abreast of relevant matters relating to the management of ABC risks by reports from its committees including the ARC Committee. The key individuals and their specific responsibilities in relation to this policy are:

- The General Counsel who is a member of the Post Office Executive team is the policy Executive Owner and policy Sponsor, accountable to the Post Office Board overall.
- The Head of Legal – Financial Services and POMS is the policy Owner who is responsible for the general management of this policy and its coordination across the Post Office. This person is accountable to the General Counsel.
- The Head of Risk and Assurance is the policy Implementor who is responsible for the day to day oversight and management of ABC issues within the Post Office as described in this Policy.

Within the Business:

- The Post Office Commercial Director is responsible for managing all ABC risks within the Commercial business
- The Post Office Network Director is responsible for managing all ABC risks within and across the Branch Network, including Crown branches, agency branches and sub-postmasters, and the property team
- The Chief Financial Officer is responsible for managing all ABC risks within business areas known as Supply Chain, Support Services, IT and Procurement.
- The Managing Director of Financial Services is responsible for managing all ABC risks within Financial Services and the provision of training in respect of ABC issues.
- The POMS Head of Risk and Compliance is responsible for managing all ABC risks in respect of POMS and for the provision of any specific ABC training to POMS.
- The Post Office Internal Audit Team provides the 3rd line of defence in respect of ABC issues across the Post Office.

Who must comply and how

Compliance with this policy is mandatory for all Post Office employees, officers, contractors, casual workers and agency workers. This policy applies wherever in the world Post Office's business is undertaken. All third parties who do business with Post Office, including consultants, suppliers and business and franchise partners, will be asked to agree contractually to this policy or to comply with their own equivalent policy.

POL00400101

It is important that you read, understand and comply with this policy. Your actions, behaviour and conduct to apply the provisions of this policy are your responsibility.

You must adhere to all parts of this policy. You should avoid any activity which may lead to a breach of this policy. We may request your confirmation of agreement to this policy. You must notify your line manager, in the first instance, as soon as possible if you have reasonable grounds to believe or suspect that a breach of this policy has occurred or may occur.

You may request a policy exception or waiver to this policy, but you must follow the Post Office's exceptions and waivers procedures which can be obtained from the Policy Owner, the Head of Legal – Financial Services.

If non-compliance is identified the matter must be referred to the General Counsel. Any investigations should be carried out in accordance with Investigations Policy. If the cause is found to be due to wilful disregard or negligence, it will be treated as a disciplinary offence.

Section C. Policy Details

Information

Legislative and Regulatory Background

Post Office complies with relevant UK legal and regulatory requirements including the:

- UK Bribery Act 2010; and
- Financial Conduct Authority (FCA) Rules and Guidance, which are in the FCA Handbook as directly applicable to POMS and indirectly to Post Office as an Appointed Representative.

In line with the Bribery Act, Post Office categorises bribery and corruption as either to:

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

Post Office could be exposed to ABC risks from two potential areas:

- Employees, including permanent employees and contractors;
- Third parties/Associated Parties, which include persons or entities that perform services for or on behalf of Post Office.

POL00400101

Prohibition of Bribery and Corruption

Under this Policy, Post Office employees are **prohibited** from offering, promising, requesting or receiving anything of value to or from any person or entity for the purpose of:

- Improperly obtaining or retaining business or securing an advantage; and/ or
- Inducing the recipient to perform his or her role in breach of an expectation of good faith, impartiality or trust.

Such conduct constitutes bribery and corruption for the purpose of this Policy and is **strictly prohibited**.

Anything of value would include (but is not limited to) the following:

- Cash;
- Preferential Treatment;
- Gifts and Entertainment;
- Offers of Employment;
- Political Donations;
- Charitable Donations.

The ABC risk is heightened when dealing with a **Public Official**. Merely offering something of value with the intention of influencing the official in their role in order to improperly obtain a benefit is illegal. Individuals and companies involved in these activities are at risk of criminal prosecution which could result in imprisonment or significant financial penalties as well as profound reputational damage.

Types of ABC Risks at Post Office

ABC risks can be classified as follows:

1. **Payment Risks** – arising from, for example, facilitation payments, gifts & hospitality, client training programmes, charitable or political donations, ex-gratia payments/ legal settlements.
2. **Third Party/ Associated Party Risks** – arising from third parties who provide services on behalf of Post Office engaging in bribery or corruption while performing such services. The scope of this could include agency operators within the Post Office network and suppliers procured through the business or through the Procurement Team. Examples of Associated Parties include agents, consultants, suppliers, introducers, and intermediaries.
3. **Employment Risks** – arising from Post Office employees requesting or receiving something of value from a third party in exchange for providing employment or work opportunities at the Post Office or offering or providing work opportunities, paid or unpaid, to Connected Individuals (see definition), or otherwise using employee connections to improperly obtain business or secure an advantage for Post Office. Employment opportunities (including work experience, secondments, etc.) have a value to the recipient and/ or their close family members and may be considered to be bribes if used to improperly obtain or retain business or secure an advantage for Post Office.

POL00400101

Our Controls

Control framework

Post Office has a legal and regulatory obligation to implement systems and controls to prevent financial crime, including bribery and corruption.

The design of these controls are to:

- Reasonably identify, deter, prevent and combat bribery and corruption;
- Respond to the risks of bribery and corruption in a comprehensive and proportionate manner reflecting the nature and scale of the relevant activities of the various areas of the business; and
- Align to this policy and related Financial Crime policies.

Business area systems and controls

Description of specific ABC Controls
A) ABC-related Processes and Procedures designed to ensure compliance with this Policy
Each business area is required, with support from the Central Risk teams, to ensure that they have in place adequate systems and controls to comply with this policy and manage bribery and corruption risks. Records of incidents, suspected or actual, should be kept locally and forwarded to the Central Risk team.
1. **Payment Risks –** types of payments for the business area and employees to consider: • **Facilitation payments** are unofficial payments made to public officials to secure or expedite the performance of their duties. These are **strictly prohibited** under UK law and this Policy. Employees who receive a request should follow the control requirements set out in this Policy and report it to their line manager at first instance. • **Gifts and Hospitality (G&H):** as these are part of corporate life, it is important that such G&H are **neither excessive nor lavish** or provided with any intention to improperly obtain or secure an advantage. Employees are expected to comply with the control requirements set out in this Policy including the G&H Policy annexed to this Policy. • **Client training programmes:** employees should ensure that the provision of training neither creates an inducement nor creates the appearance of an inducement for the purpose of improperly obtaining or retaining business or securing an advantage for Post Office. Like G&H, the training provided should **not be excessive or lavish**. • **Charitable donations:** Post Office is proud of its public purpose and its involvement in the community. However, it is important that donations are made free from any suspicion of bribery or corruption. Where a supplier or third party requests that Post Office makes a charitable donation, Post Office and its employees should ensure that the donation is **not linked to any business or services** provided to or by that supplier or third party.

POL00400101

There must be no perceived inducement for the purpose of improperly obtaining or retaining business or securing an advantage for Post Office.

- **Political donations:** as Post Office's shareholder is the UK Government Department for Business Innovation and Skills, it is particularly important that employees do **not purport to make or solicit** any political donations on behalf of Post Office. Post Office is an apolitical organisation and does not make donations to any political parties.
- **Ex-gratia payments/ legal settlement:** an ex-gratia payment or a legal settlement is a possible basis of resolving a dispute or claim. The business area should assess the liability of making such a payment and ensure that it is **justified and proportionate** having regard to the circumstances of the matter. Such payments should not be made or accepted to obtain any improper advantage or favour.

2. **Third Party/ Associated Party Risks** – before engaging with a Third Party/ Associated Party, the business area and employee should:

   - undertake a **due diligence exercise** (including a risk assessment) on the proposed Associated Party to determine the ABC risk profile of the Associated Party. When undertaking the ABC due diligence/ risk assessment consider whether there are any "red flags" or heightened risks arising from that assessment.
   - relevant **mandatory ABC contract clauses** should be included in the agreement with that party. Please liaise with Legal and Procurement Departments to ensure that all contracts include the appropriate ABC clauses.

3. **Employment Risks** – when involved in recruitment, business areas and employees should consider the possibility for breaching ABC legal and regulatory requirements:

   - Post Office employs a merit based approach in its hiring of staff. Employees should comply with the Post Office HR and Conflicts of Interests policies when wishing to refer to recommend a connected individual for employment or work at Post Office.
   - employees have an ongoing obligation to consider their close connections and should disclose to their line manager as necessary.
   - all business areas must ensure that where there is any risk that the business could be awarded to Post Office because of an employee's connection rather than Post Office's services and products, it manages such risks.

B) Robust Risk Assessments and Due Diligence across relevant business areas

Each business area is required, with support from the Central Risk teams to identify, clarify and review key bribery and corruption risks through thorough assessment and where appropriate due diligence. Particularly heightened risks or "red flags" could include:

- **Payment Risks** – where there is the possibility for facilitation payments, gifts & entertainment, client training programmes, charitable or political donations, ex-gratia payments/ legal settlements.

POL00400101

- **Third Party/ Associated Party Risks** - where the Associated Party may be providing services in a country that is at high risk for bribery and corruption; or engages in transactions that give rise to higher risks for bribery and corruption (for example, transactions involving public officials or the use of sub-contractors); or is themselves a Public Official, Politically Exposed Person (PEP) or is linked to a prominent Public Official or PEP. Specific may include:
    - Remuneration which is not proportionate with the services being rendered or consistent with the market or relevant industry.
    - Excessive large up-front fee structures linked to making "necessary arrangements" or expedite work.
    - Requests for payments to be made to another third party or undisclosed beneficiary.
- **Employment Risks** – where there are work opportunities with high reward packages, or a significant element of judgment in awarding elements of the package, for instance bonuses, expenses, compensation.

C) Training

Each business area should ensure that its employees understand the risks associated with bribery and corruption and their roles and responsibilities to ensure compliance with this Policy. The Post Office Academy will develop risk based ABC training to be delivered at least annually in a variety of formats.

D) Incident reporting, response and recording

Each business area within Post Office should ensure that incidents can be reported through formal channels including line managers within the business or the whistleblowing help line. Incidents are to be recorded by the business area, where applicable, and escalated to the relevant risk team.

The Central Risk team holds a register of incidents and reports significant incidents to the Post Office ARC Committee. This ensures that the bribery and corruption incidents are identified and managed appropriately (including any enhanced controls if necessary) within the various levels of the organisation.

E) Risk Indicators

Each business area is to monitor ABC risks and escalate existing and new bribery and corruption risks to the head of that area who shall, in turn, inform the relevant risk team. The Central Risk team determines the risk indicators and MI required.

F) Self Assessment

Bribery and corruption risks are reviewed with relevant individuals (see "Who is responsible") on a regular basis and at least twice a year. All individuals subject to this policy may be requested to confirmation agreement to this policy.

POL00400101

Section D. Governance

How do we monitor compliance

It is the responsibility of all line mangers to ensure that their direct reports comply with this policy. It is the responsibility of the Head of Legal – Financial Services to review the Policy regularly and ensure it remains effective. Post Office internal systems of risk control ensure that ABC controls in this policy are regularly independently assessed for effectiveness suitability and adequacy. Post Office Internal Audit retains independent third line oversight with regard to this policy.

We will assess compliance with this policy on a timely basis and regular ABC reports will be issued by the Policy Implementor to the Security Group Forum, the Post Office Risk and Compliance Committee and the Post Office ARC.

Annually, the ABC policy Sponsor reports on the effectiveness of ABC risk controls to the Post Office ARC Committee.

We require our subsidiaries and third parties to have at least equivalent arrangements, systems and controls to this policy.

How to raise a concern

A Post Office employee who reasonably suspects or reasonably believes there is a breach of this Policy should report this without any undue delay.

Post Office has established mechanisms for the receipt of confidential feedback to assist individuals to speak up and to ensure that they are confident in doing so.

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

- their line manager,
- a senior member of the HR Team, or
- if either or both are not available, staff can contact the Post Office's General Counsel, currently Jane MacLeod who can be contacted by email at: whistleblowing GRO or by telephone on: GRO.
- Alternatively staff can use the Speak Up service available on GRO
- or via a secure on-line web portal: http://www.intouchfeedback.com/postoffice

Post Office encourages members of the public or people not employed by us who suspect bribery or corruption to write, in confidence, to the **Chief Executive's Office, Finsbury Dials, 20 Finsbury St, London EC2 9AQ.**

If you are unsure whether there is a breach of this policy or have any other general policy concerns these matters should be raised in the first instance with your line manager or if that is not appropriate in the circumstances to Head of Legal – Financial Services on GRO or by email at ben.foat GRO

POL00400101

Contact us and more information

If you need further information about this policy or wish to report an issue in relation to this policy please contact Ben Foat Head of Legal – Financial Services on GRO or by email at ben.foat GRO

Section E. Key Terms and References

In order of occurrence in this document.

Key Terms

Term or Acronym	Description
MI	Post Office Management Information
HR	Post Office Human Resources team

References

References	Description
Business Standards	Post Office rules of behaviour setting out at high level the conduct it expects of its staff in all Post Office undertakings.
Post Office Group	Post Office Limited and all subsidiaries and entities within the Post Office Group which includes Post Office Management Services (POMS).
Public Official	A public official includes: a) any officer, employee or representative of the government including local authorities b) any individual who exercises a legislative, executive or judicial junction irrespective of whether they are elected or appointed c) any political party or official of a political party d) any officer, employee or representative of a public international organisation e) any member of a royal family f) any officer, employee or representative of any government entity
Corruption	the misuse of entrusted power or public office for private gain.
Anti-Bribery and Anti-Corruption Policy (Incorporating Gifts Policies)	Post Office anti-bribery and anti-corruption standards. Including (gifts and hospitality procedures).
Anti-Money Laundering and Counter Terrorism Financing Policy	Combined Post Office Anti-Money Laundering and Counter Terrorism standards and arrangements.
Cyber Fraud Policy	Post Office information security specific fraud policies Including information security forensics

POL00400101

Whistleblowing Policy	Post Office arrangements for individuals to raise concerns for wrongdoings in the organisation. Supported by whistleblowing investigations procedures.
Prosecution Policy for England and Wales	Post Office approach when it is suspected that crime has been committed against its business in England and Wales.
Staffing Vetting Policy	Post Office framework for the vetting of all roles within, and providing services for Post Office Ltd and Post Office Management Services which delivers our legal, regulatory, and contractual obligations
Bribery	The offer, promise, payment, request, agreement to receive anything of value whether directly or indirectly to or from any person or entity in order to induce that person or entity to perform their roles improperly or in the case of a Public Official in order to influence them with the intention of obtaining or retaining business or an advantage in the conduct of business. Examples include an offer or promise to give anything of value to anyone to obtain or retain business for or on behalf of the Post Office or to obtain or fulfil a legal or regulatory requirement in furtherance of PO's business. A bribe can take the form of a "reward" and be paid after the improper performance of the relevant duty or obligation.
Politically Exposed Person (PEP)	A person who has at some point been responsible for a prominent public function and their close family members or close associates.
Ex Gratia Payment	A good will payment made in circumstances where there is no technical legal obligation.
Connected Individuals	Those individuals who are known to have close connections to existing or prospective clients, Public Officials, Politically Exposed Persons (PEPs) or using employees connections to improperly obtain business or secure an advantage for PO.
Associated Party	A person or entity which performs services for or on behalf of Post Office, as determined by the risk-based ABC control requirements set out in this policy. Examples include, but are not limited to, agents, representatives, consultants, or other intermediaries, advisors, and outsourcers engaged by Post Office.
Framework	The Post Office Policy Framework of key policies which form a key controls layer within its General Controls Framework.

POL00400101

Appendix 1 – Post Office Gifts and Hospitality Policy

Gifts and hospitality are part of corporate life. It is important that such G&H are **neither excessive nor lavish** or provided with any **intention to improperly obtain or secure an advantage**.

Gifts - Approvals Procedure and Register

No gift should be offered or accepted if it is intended to induce improper behaviour. In general the giving and receiving of gifts is not permitted, with the exception of low value promotional items costing under £20 each, such as pens, calendars, diaries, notepads and paperweights.

- In a situation where refusal to give or accept a gift would cause embarrassment or offence, the gift must not appear lavish or extravagant and should not cost more than £200.
- Before giving any gift costing more than £20, written approval must be obtained from your line manager and forwarded to the Central Risk team at riskandcompliance@postoffice.co.uk
- If you receive a gift worth more than £20 you must notify your line manager in writing, and forward the details to the Central Risk team at riskandcompliance@GRO

The POL Central Risk team maintains a Register of all POL activity Gifts given and received of over £20. POMS maintains a separate register concerning POMS activities.

Hospitality – Approvals Procedure and Register

This policy allows reasonable and appropriate hospitality or entertainment given to or received from third parties, for the purposes of:

- Establishing and maintaining good business relationships;
- Improving or maintaining our image or reputation; or
- Marketing or presenting our products and/or services effectively,
- 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.

You must beware of accepting any hospitality and entertainment which might compromise your performance of official business, or which might reasonably appear to have improperly influenced a business decision. Any attempt at entrapment, blackmail, or any suggestion that preferential treatment or divulgence of confidential information is expected in return for hospitality and entertainment, must be reported to your line manager and the Central Risk team.

POL00400101

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. The giving and receiving of hospitality and entertainment is subject to the following rules:

- Before accepting or giving hospitality prior written approval must be obtained from your line manager;
- 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 given and accepted, including details of the host business (if not Post Office Limited), the number of people attending and the businesses they represent (if Post Office Limited is the host), with details of the location of the hospitality and the cost per person, along with the written approval from your line manager, to the Central Risk team at riskandcompliance GRO

The Central Risk team maintains a Register of all Hospitality given and received.

End of Policy

POL00400101

Post Office Anti-Money Laundering and Counter Terrorist Financing Policy

POL00400101

Contents Page

POL00400101

Document Control Sheet

SUMMARY			
GE Policy Sponsor	Policy Owner	Policy Implementor	Policy Approver(s)
General Counsel **Jane MacLeod**	Head of Security and Financial Crime (MLRO) **John Scott**	Senior Security Manager, Financial Crime **Sally Smith**	Post Office **RCC and ARC Committees**
Version and Policy Status:	Policy Review Period	Effective from:	Policy location:
Final V2.9	Annual (from effective date)	[To be confirmed]	Z:\NEW COMPLIANCE\New Policy Framework 2015\Refreshed Policies 2016

REVISION HISTORY			
Version	**Date**	**Author**	**Reason For Change**
Draft v2.7	27th April 2016	**Jane MacLeod**	Sponsor/Executive Owner sign – off
Final v2.8	29th April 2016	**Sally Smith/Mark Rodgers**	Final update of Executive Member (N Kennett) feedback
Final v2.9	23rd June 2016	**Sally Smith/Mark Rodgers**	Amendments following controls 'gap' check

POLICY APPROVAL		
Role/Forum	**Name**	**Date**
Executive Owner and Sponsor	**General Counsel (Jane MacLeod)**	30th March 2016
Executive Committee	**Post Office Risk and Compliance Committee (RCC)**	[to be confirmed]
Board Committee	**Post Office Audit, Risk and Compliance Committee (ARC)**	[To be confirmed]

DOCUMENT DISTRIBUTION STATUS			
Distribution (Mark x as appropriate)		Document Sensitivity (Mark x as appropriate)	
Internal Only	X	Non-sensitive	
External Only		Sensitive	X

QUALITY STATEMENT	
Quality Control	Next review date
This document is periodically reviewed and at least once each year starting from the last effective date. This policy has been reviewed against the latest Post Office policy standards.	[To be confirmed

POL00400101

Section A. Introduction

Chief Executive's Note

The Post Office Group ('Post Office') is committed to doing things correctly. Our Business Standards are our code of behaviours that represent the conduct we expect. This policy supports the code to help us ensure the highest standards of fraud prevention, detection and management are maintained, including a zero tolerance to anti-money laundering and counter finance terrorism financing risks. This policy sets out what is and is not acceptable in general terms but if you have any doubts or questions, these should be referred in the first instance to The Head Security and Financial Crime (Money Laundering Reporting Officer) who oversees compliance with this policy. It is essential that you read this policy.

Introduction by the General Executive Policy Owner: General Counsel

As Post Office's General Counsel and the General Executive Policy Owner I have overall accountability for AML and CTF to the Board of Directors. Post Office's Audit, Risk and Compliance Committee ("ARC") considers AML and CTF matters as an agenda item and the Post Office Board is updated as required.

POL00400101

Section B. Context

About this Policy

The purpose of this policy is to ensure that Post Office complies with the requirements and obligations set out in UK legislation, regulations, rules and industry guidance for Anti-Money Laundering and Counter Terrorist Financing ("AML and CTF").

This policy sets out what we must all do to prevent and manage AML and CTF risks and it is a set of standards to minimise the likelihood of regulatory breach.

This policy's effective date will be determined by the date on which final approval is given by the appropriate governance forum.

What is AML and CTF?

In common with many other countries, the United Kingdom has passed legislation designed to prevent money laundering and to combat terrorism financing. This legislation, together with regulations, rules and industry guidance, forms the cornerstone of AML and CTF obligations for Post Office and outlines the offences and penalties for failing to comply.

Post Office is authorised and regulated by Her Majesty's Revenue and Customs (HMRC) for the following business activities, and is directly responsible to HMRC for compliance with AML/CTF requirements in relation to the following regulated activities:

- Money Service Business (MSB) activity,
- Branch bureau on-demand and pre-order sales and on-demand purchase,
- Third Party Cheque encashment (e.g. HMRC cheques), and
- Bill Payments.

In addition, for several regulated products and services Post Office is the Appointed Representative (AR) under agreements with Bank of Ireland (BOI) and Post Office Management Services Limited (POMS) and is an agent for MoneyGram; and has a number of partnerships and strategic distribution alliances with suppliers including Partner Banks, GVS Prepaid Limited and First Rate Exchange Services Limited (FRES). Where stated, each agreement imposes obligations on Post Office to comply with regulatory requirements including those relating to AML/CTF and in particular Know Your Customer requirements ("KYC").

Post Office is responsible for and complies with all directly applicable AML/CTF legislation, together with regulations, rules and industry guidance. Where Post Office is an Appointed Representative ultimate accountability, including KYC, rests with the Principal firm who is our partner.

POL00400101

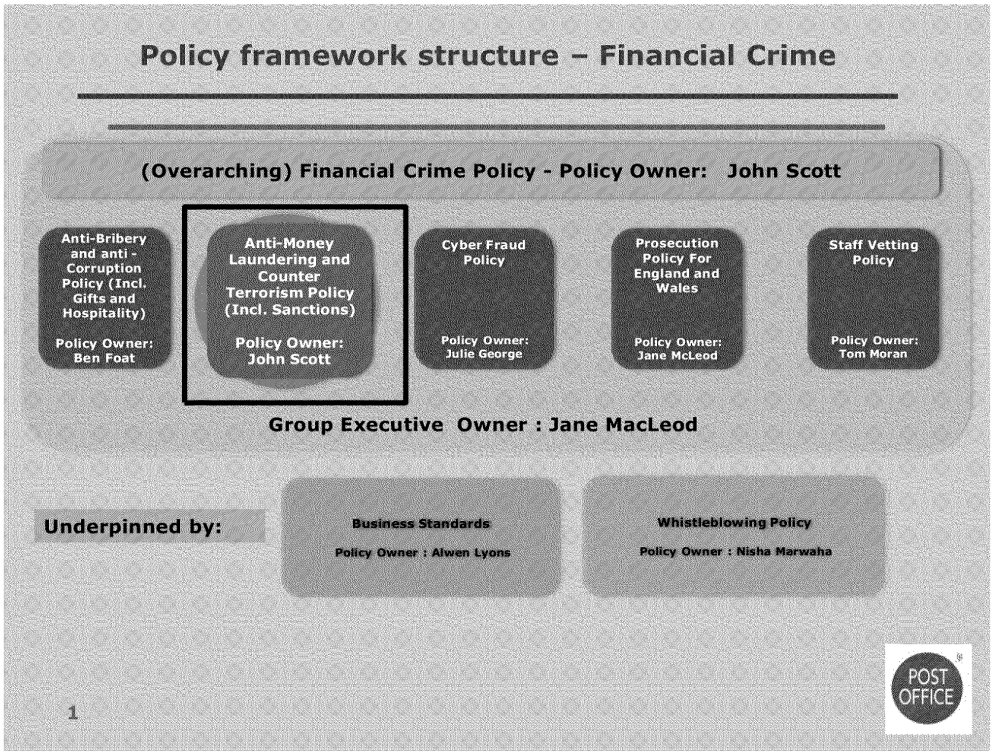
The AML and CTF regulatory and contractual framework requires Post Office to ensure that it is not used as a conduit for money laundering or terrorist financing, report suspicious activity, provide appropriate AML/CTF training for relevant individuals, and maintain adequate transaction records.

Risk Appetite

The Post Office's risk appetite is intolerant for non-compliance with law and regulations or deviation from its business conduct standards. Post Office has a zero tolerance to money laundering and terrorist financing risks. This policy reflects this appetite and sets out controls to reduce and/or mitigate any such risks.

How we organise AML/CTF management

This policy sits within a broader Financial Crime family policy structure. It is one within a suite of policies and each should be read in conjunction with the others. Our Financial Crime Policy structure is shown below.



Who is responsible

Post Office's Board of Directors have overall responsibility for ensuring that Post Office has a framework to ensure compliance with legal and regulatory requirements. The Board will be kept informed of relevant matters relating to the management of AML and CTF through reports to its committees – principally to the Audit, Risk & Compliance Committee ('ARC'). The key individuals and their specific responsibilities:

POL00400101

ROLE	RESPONSIBILITY
Policy Owner	The policy owner will review this Policy on an annual basis or upon change in relevant legislation.
General Counsel	The General Counsel who is a member of the Post Office Executive is the Executive Owner and Sponsor of the AML Policy. The General Counsel is accountable to the CEO and to the Post Office Board overall.
Head of Security and Financial Crime (MLRO)	The Head of Security and Financial crime (MLRO) is the owner of the AML Policy and is responsible for the implementation and compliance with this Policy. The Head of Security and Financial crime (MLRO) is also the Nominated Officer and accountable to the General Counsel.
Senior Security Manager, Financial Crime and AML	The Senior Security Manager, Financial Crime and AML is the policy implementer and is accountable to the Policy owner. The Senior Security Manager, Financial Crime and AML, may delegate duties to an appointed person. The Senior Security Manager, Financial Crime and AML, (and/or the appointed person) has responsibilities which include, but are not limited to: • Acting as the focal point for AML/CTF issues • Promoting the compliance culture by communicating the AML/CTF standards which drives ownership and accountability throughout Post Office • Overseeing AML/CTF activities ensuring processes, procedures and controls are compliant with the Policy and/or local laws • Ensuring effective governance arrangements are in place within Post Office to effectively monitor and manage AML/CTF risks • Ensuring there are effective mechanisms in place to identify and investigate potential non-compliance with this Policy including adequate risk assessment and conformance activities • Providing regular updates to the MLRO
Senior Management/The Head of each Business Unit	Senior Management/The head of each Business Unit has ultimate responsibility for ensuring that

POL00400101

	their respective business areas establish systems and controls to comply with this Policy, whether they are performed by the Business or outsourced to third parties. These responsibilities include but are not limited to: • Taking a full account of this Policy when entering into new products or sales channels, implementing new systems or expanding the business operations including branch network design • Ensuring that any reliance on third parties or service providers for compliance with this Policy meets the requirements of this Policy • Ensuring all relevant employees receive appropriate training with the support of the MLRO and Financial Crime Team • Ensuring all relevant employees understand their obligation to prevent the use of the Post Office for the purpose of money laundering, terrorism financing and financial crime in general • Ensuring immediate reporting of any breach or suspected breach of this Policy to the MLRO and Financial Crime Team
Employees (Staff and Agents)	All Staff and Agents are responsible for ensuring they comply with the terms of this Policy and complete all AML training as required

Who must comply and how

Compliance with this policy is mandatory for all Post Office employees, officers, contractors, casual workers and agency workers. This policy applies wherever in the world Post Office's business is undertaken. All third parties who do business with Post Office, including consultants, suppliers and business and franchise partners, will be asked to agree contractually to this policy or to comply with their own equivalent policy.

It is important that all Post Office employees read, understand and comply with all parts of this policy. Failure to comply with AML requirements can result in personal liability such as fines and imprisonment. Employees who fail to comply with this policy may be subject to disciplinary action up to and including dismissal. Agents or contractors who fail to comply with this Policy may have their contract terminated.

It is a legal requirement that if an employee believes or suspects that a breach of this policy has occurred or may occur, he/she must raise a SAR, as soon as possible. Reporting via SAR protects individuals from personal liability.

POL00400101

Employees may request a policy exception or waiver to this policy, but he/she must follow the Post Office's exceptions and waivers procedures which can be obtained from the Policy Owner, the Head of Security and Financial Crime (MLRO).

Any queries in respect of the policy must be referred to the Policy Owner. If non-compliance is identified the matter must be reported via a SAR. Any investigations should be carried out in accordance with Investigations Policy. If the cause is found to be due to wilful disregard or negligence, it will be treated as a disciplinary offence.

POL00400101

Section C. Policy Details

Information

Post Office complies with relevant UK legal and regulatory requirements including:

- The Proceeds of Crime Act 2002 ('POCA'),
- The Terrorism Act 2000,
- The Money Laundering Regulations 2007 (the Regulations'),
- JMLSG: Prevention of Money Laundering/Combating Terrorist Financing,(2014 Revised Version), and
- HMRC - Anti-money laundering guidance for money service businesses.
- Financial Conduct Authority Handbook

Primary Money Laundering offences include:

- Concealing, disguising, converting, transferring, or removing from the UK (S327 of POCA),
- Entering into or becoming concerned in an arrangement which you know or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person (S328 of POCA), and
- The acquisition, use or possession of criminal property (S329 of POCA).

Secondary Money Laundering offences include:

- Failure to disclose any of the three primary offences; and
- Tipping off.

The Regulations provide that no person shall in the course of carrying out relevant financial business in the UK form a business relationship or carry out a one off transaction where a payment of more than **€15,000** is involved or where several one off transactions are involved and the total value of the linked transactions exceeds **€15,000** with or for another person. Any business relationships of more than €15,000 over a 90 day period must have appropriate due diligence applied (as described below in 'Our Controls' section) and must be approved and authorised by the MLRO.

Failure undertake appropriate due diligence even if no money laundering takes place, is in itself a criminal offence punishable with up to two years in prison and/or an unlimited fine.

POL00400101

Post Office addresses the risk of money laundering and terrorist financing through its anti-money laundering risks and controls which include the following:

- Appointing a Money Laundering Reporting Officer,
- Ensuring AML/CTF compliance training is provided, at a minimum on an annual basis, to all employees including senior management and all agents and that they are made aware of their requirement to report suspicious activity,
- Conducting periodic risk assessments of our money laundering and terrorist financing risk,
- Implementing risk based controls designed to detect, deter and report known or suspected money laundering or terrorist financing and subjecting these controls to independent periodic testing,
- Conducting a risk based identification, verification and due diligence process for all new customers of regulated products where transactions are more than €15,000 over 90 days,
- Where a business relationship is established, screening customers of Post Office and their transactions for potential financial sanctions breaches, and
- Monitoring regulated transactions and assessing compliance with this Policy.

Our Controls

For AML/CTF obligations which Post Office is responsible and/or accountable, its key controls are designed to ensure regulatory compliance and to make sure we appropriately manage money laundering and terrorist financing risk. To do this Post Office will:

- Carry out a risk assessment identifying any products, customers, suppliers, geographic areas or other factors where its business and operations are vulnerable to money laundering and terrorist financing,
- Ensure that it has a relevant policy supported by appropriate procedures to demonstrate how Post Office manages the risks of money laundering and terrorist financing identified in risk assessments,
- Ensure there are sufficient trained people to implement the policy adequately, and systems to help them,
- Monitor effectiveness of the policy and controls and make improvements where required, and
- Appoint a Money Laundering Reporting Officer ("MLRO") of sufficient seniority, who has responsibility for Post Office compliance with relevant legislation, regulations, rules and industry guidance.

Subject to the scope of Post Office AML/CTF obligations stated in the list immediately above, the following regulatory requirements will be met:

- **Registration** – Post Office is registered with HMRC as a Money Service Business providing over the counter foreign exchange services, third party cheque encashment services and bill payment services. An up to date record of every premises from which Post Office Limited offers regulatory activity must be maintained with HMRC. All new premises must be registered within 30 days of

POL00400101

commencing trading and the MLRO will maintain a list of registered premises. The HMRC registered number for Post Office Limited is 12137104.

- **Fit and proper test** – The following roles must complete a Fit and Proper Test within 30 days of taking up their post:

  - Post Office Board directors,
  - Group Executive (GE) members,
  - MLRO, and
  - The line manager of the MLRO if not a GE member
    The MLRO will maintain a register of completed Fit and Proper tests.

- **Staff training and awareness** – Post Office will ensure that:

  - All new employees of Post Office (including trainees and temporary personnel), agents (and their employees) receive AML/CTF training,
  - Training appropriate to the role of all staff and agents (and their employees) will be facilitated by regular communications, and at least annually,
  - Records of completion of annual training will be maintained, and
  - Post Office will ensure staff engaged in any outsourced Post Office activity, suppliers and clients are provided with relevant training.

- **Customer Due Diligence (CDD) -** Post Office will establish and maintain risk based customer due diligence, identification, verification and Know Your Customer, including enhanced due diligence for those customers presenting higher risk. In particular,

  - Identification and address verification is required for all single occasional bureau transactions of £5,000 (the 'ID threshold') and above or identifiable linked transactions over a period of 90 days that reach this threshold,
  - Central monitoring will be in place for all bureau on demand transactions above the ID threshold,
  - Risk-based due diligence will be carried out ahead of any new business relationship, product or service implementation,
  - Politically Exposed Persons (PEPs) and Sanctions screening will be undertaken for all direct customer relationships.

  Enhanced Due Diligence (EDD) will be applied where higher risk business relationships, products or services provided by Post Office are identified:
  - Identity information will be obtained and verified for personal customers, including name, address and date of birth,
  - Identity information will be obtained for corporate or business entities including the entity name, registered address and operational address (if different) plus personal identity information for the relevant controllers and ultimate beneficial owners of the entity, and
  - Identity and source of wealth information will be obtained and verified for any PEPs.

POL00400101

Post Office will record and validate the business relationship with the customer to be on-boarded including:

- The nature and details of the business,
- The source and origin of funds,
- The relationship with an ultimate beneficial owner (UBO), and
- The anticipated volume and value of activity that is to be undertaken.

- **Identification and Verification -** Will be performed before entering into a relationship with a new customer or where suspicions are aroused.

- **Controllers and Ultimate Beneficial Owner checks -** Post Office will take sufficient measures to understand the underlying structure and ownership by considering information such as the legal form of the entity (e.g. limited company).

  Post Office will ensure that the entity's controller, directors, UBOs and any other individuals, including signatories where relevant, who otherwise exercise control over the entity are identified and verified.

- **Politically Exposed Persons (PEPs) screening** – Post Office follows the Money Laundering Regulations guidelines relating to PEPs (see definition in Section E Key Terms below) and all PEP relationships must be monitored due to the likelihood that they will pose a higher risk.

  New customers must be screened against publically available PEP lists in order to determine if they are politically exposed, and re-screened periodically on a risk assessed basis.

  Where information indicates negative information or the need to change risk classification, any investigation must be completed and a decision made on the customer within 30 days, adequately recorded and reported to the MLRO.

  All PEP relationships must be agreed and signed off by the MLRO, classified as high risk and included in MI Reports.

  Post Office will regularly screen customers against external PEPS lists to identify personal or non-personal customers who may have become a PEP during the client lifecycle. If any matches are found, additional identification and verification will be conducted to confirm the true identity and status as a PEP - Enhanced Due Diligence (EDD) and appropriate escalation and approval processes must be followed.

- **Enhanced Due Diligence ("EDD") -** must be performed on a risk-sensitive basis, during take-on or review, where the customer represents a higher risk of money laundering or terrorist financing or where the client has other identified risk factors.

  The EDD may lead to a conclusion that the customer does not ultimately pose high risk to our business. However, in all cases the steps taken, tests performed and results obtained for each step of the EDD process must be recorded on the client file and be easily and readily retrievable.

POL00400101

- **Periodic Review of CDD –** information obtained requires update at regular intervals. The intervals may be triggered either by an event or due to the risk level they represent, the following events will trigger an immediate review of all client data held by Post Office:

  - Change of client risk profile,
  - Identification of potential suspicious activity, and
  - Receipt of a Production Order or Subpoena.

- **Reporting Suspicious Activity -** all staff and agents must escalate internally any instances where they have reasonable grounds to have knowledge or suspicion that another person is engaged in money laundering or terrorist financing via the Suspicious Activity Report ("SAR") process.

  Procedures exist for reporting suspicious activity internally and to the relevant law enforcement authorities as appropriate. The MLRO is the Nominated Officer to whom all reports of suspicious activity ('SAR's) from within the business must be sent and who will report to the National Crime Agency ("NCA"), as appropriate.

  Any internally produced SARs that are not disclosed to NCA will be counter-signed by a senior manager. That manager will continue to review the subject matter of the report for a minimum of 3 months to ensure that the appropriate decision was taken.

  Consent Process – a procedure will exist for the requesting of NCA consent where appropriate. The Consent Process allows the police to run checks on an individual and, if necessary, take action to prevent any suspected proceeds of crime from being transferred, disguised or moved around the financial system. Consent must be applied for if anyone is suspicious of a transaction by telephoning Grapevine on 0845 603 4004 to give the details and complete a SAR. Customers must not be advised that Consent is being applied for as this would constitute 'tipping off'.

- **Record Keeping -** records must be kept of all transaction data and data obtained for the purpose of identification, as well as all documents related to money laundering topics (e.g. files on suspicious activity reports). Those records must be kept for a minimum of 5 years from the date of creation/transaction:

  - Records relating to customers with whom a business relationship exists should be retained for 5 years after the business relationship ceased, and

  - If someone else carries out customer due diligence for Post Office Limited, then Post Office Limited must make sure that they also comply with the record keeping requirements.

POL00400101

- **Monitoring –** Post Office will undertake monitoring on a risk based approach to ensure:

    - Transaction activity is consistent with the information known about a customer's source of funds and wealth, and the nature and purpose of the relationship. Where trading patterns change significantly this will trigger a review of client data and consideration of the risk rating of the customer, and

    - Staff and agents are complying with regulatory obligations.

The following must be produced by the MLRO:

- Risk based systems and procedures to monitor branch and supply chain transactions and provide assurance that compliance performance is at an acceptable standard, and
- An annual assurance audit of the supply chain due diligence process.

- **Risk Management –** Post Office will establish and maintain a risk based approach towards assessment and management of money laundering and terrorist financing risks including:

- The establishment of appropriate mechanisms to evaluate and explore options to protect Post Office and de-risk if appropriate, where SARs have been received for the same individual(s) on more than one occasion, and
- Completion of an automated risk assessment model for all new products and services which will determine the level of risk and engagement required between the business and the AML/CTF team to ensure projects adhere to the AML/CTF policy.

- **Management Information and Reporting –** regular management information will be produced and supplied to relevant stakeholders, covering:

- The operation of processes, systems and controls,
- Any changes in the risk environment,
- Any recommended changes to the risk assessment,
- Any breaches of rules or regulations,
- A summary of key findings, along with an action plan for addressing deficiencies, and
- A summary of prior period actions and outcomes for comparison.

POL00400101

Section D. Policy Governance

How do we monitor compliance

The Head of Security and Financial Crime will ensure that this policy is implemented, reviewed and remains effective. Post Office internal systems of risk control ensure that the AML/CTF controls in this policy are assessed for effectiveness, suitability and adequacy. Post Office Internal Audit retains independent third line oversight with regard to this policy.

We assess compliance with this policy on a regular timely basis and regular AML/CTF reports will be issued by The Head of Security and Financial Crime to Post Office's Risk and Compliance Committee.

Annually, the Head of Security and Financial Crime reports on the effectiveness of AML/CTF risk controls to Post Office Audit and Risk Committee via the MLRO Annual Assurance Report.

We require our subsidiaries and third parties to have at least equivalent arrangements, systems and controls to this policy.

How to raise a concern

Every Post Office employee has a regulatory obligation to report suspicions of AML/CTF or concerns via the SAR process. The SAR process details and reporting forms may be obtained from the MLRO or telephone Grapevine on GRO

A Post Office employee who reasonably suspects or reasonably believes there is a breach of this Policy should report their suspicions by telephoning Grapevine on GRO GRO without any undue delay.

Contact us and more information

If you need further information about this policy or wish to report an issue in relation to this policy , please contact John Scott – Head of Security and Financial Crime (MLRO) on GRO or by email at **john.m.scott** GRO

POL00400101

Section E Key Terms and References

Key Terms

Term or Acronym	Description
MLRO	Money Laundering Reporting Officer
MI	Post Office Group Management Information
SARS	Suspicious Activity Reports
Post Office Group ('Post Office')	Post Office Limited and all subsidiaries and entities within the Post Office Group which includes Post Office Management Services (POMS)
Nominated Officer	Businesses that are regulated by the Money Laundering Regulations - HMRC must appoint what's known as a 'Nominated Officer'. The Nominated Officer must be someone in the Post Office Group ('Post Office') business and must be aware of any suspicious activity in the business that might be linked to money laundering or terrorist financing, and if necessary report it to the National Crime Agency. The nominated office is responsible for: • receiving reports of suspicious activity from any employee in the business • considering all reports and evaluating whether there is - or seems to be - any evidence of money laundering or terrorist financing • reporting any suspicious activity or transaction to the National Crime Agency (NCA) by completing and submitting a Suspicious Activity Report • asking the NCA for consent to continue with any transactions that they've reported, and making sure that no transactions are continued illegally

Politically Exposed Person (PEP)	Section 14(5) paragraph (4) of the Money Laundering Regulations 2007, defines a PEP as "a politically exposed person" meaning a person who is—
	
	• (a) an individual who is or has, at any time in the preceding year, been entrusted with a prominent public function by—
	  ○ (i) a state other than the United Kingdom;
	  ○ (ii) a Community institution; or
	  ○ (iii) an international body,
	• including a person who falls in any of the categories listed in paragraph 4(1)(a) of Schedule 2;
	
	• (b) an immediate family member of a person referred to in sub-paragraph (a), including a person who falls in any of the categories listed in paragraph 4(1)(c) of Schedule 2; or
	
	• (c) a known close associate of a person referred to in sub-paragraph (a), including a person who falls in either of the categories listed in paragraph 4(1)(d) of Schedule 2.

POL00400101

Post Office Group
Investigations Policy

POL00400101

Contents Page

Contents

POL00400101

Document Control Sheet

SUMMARY			
GE Policy Sponsor	**Policy Owner**	**Policy Implementor**	**Policy Approver**
General Counsel **Jane MacLeod**	Employment Lawyer **Nisha Marwaha**	Employment Lawyer **Nisha Marwaha**	Post Office **Risk & Compliance Committee**
Version and Policy Status:	**Policy Review Period**	**Effective from:**	**Policy location:**
Draft V1.2	Annual Review (from date effective)	28 September 2016 [to be confirmed]	Z:\NEW COMPLIANCE\New Policy Framework 2015\Refreshed Policies 2016

REVISION HISTORY			
Version	**Date**	**Author**	**Reason For Change**
Draft v1.0	18 February 2016	**Nisha Marwaha**	1st draft for new Policy
Draft v1.1	11 April 2016	**Mark Rodgers & Mike Morley-Fletcher**	Policy standards and Head of Risk review
Draft 1.1	23 April 2016	**Nisha Marwaha**	Policy Owner review
Draft 1.2	30 June 2016	**Mark Rodgers**	Policy standards review

POLICY APPROVAL		
Role/Forum	**Name**	**Date**
Executive Owner and Sponsor	General Counsel (Jane MacLeod)	30 March 2016
Executive Committee	Post Office Risk & Compliance Committee (RCC)	8 Sept 2016 [tbc]
Board Committee	Post Office Audit, Risk and Compliance Committee (ARC)	28 Sept 2016 [tbc]

DOCUMENT DISTRIBUTION STATUS			
Distribution (Mark x as appropriate)		Document Sensitivity (Mark x as appropriate)	
Internal Only	X	Non-sensitive	X
External Only		Sensitive	

QUALITY STATEMENT	
Quality Control	Next review date
This document is periodically reviewed and at least once each year starting from the last effective date. This policy has been reviewed against the latest Post Office policy standards.	January 2017

POL00400101

Section A. Introduction

Chief Executive's Note

Post Office Group ('Post Office') is committed to doing things correctly. Our Business Standards are our code of behaviours that represent the conduct we expect. This policy supports the code to help us ensure the highest investigation policy standards are maintained.

This policy sets out what is and is not acceptable but if you have any doubts or questions, these should be referred in the first instance to the policy owner, our principal employment lawyer within our Legal team who oversees compliance with this policy. It is essential that you read this policy.

Introduction by the Group Executive Policy Owner: General Counsel

As Post Office's General Counsel and the Group Executive Policy Owner I have overall accountability for the governance framework to which this policy relates to the Board of Directors. Post Office's Audit, Risk and Compliance Committee considers investigations and related matters as an agenda item. The Post Office Board is updated as necessary.

POL00400101

Section B. Context

About this Policy

The purpose of this policy is to provide key principles for individuals to consider and use where necessary when conducting internal investigations. The policy sets standards Post Office employees should aim to achieve.

The definition of investigation is the act or process of investigating someone or something.

This policy should be read in conjunction with any other applicable Post Office policies which require an investigation to be conducted, including in particular the Post Office Prosecutions Policy (located on the Post Office intranet). It applies to the Post Office Group as defined in Section C.

This policy is reviewed on a regular basis with relevant individuals and at least at half yearly intervals each year.

This policy enables us to comply with our obligations under applicable legislation and with regulatory requirements. It also protects Post Office's brand and reputation.

This policy's effective date will be determined by the date on which final approval is given by the appropriate governance forum.

Principles to be considered at the outset

- Before commencing an investigation, the following should be considered: Identify the nature of the investigation and its purpose;
- Identify who and what is being investigated;
- Identify if there are any other applicable existing Post Office procedures. For example, Whistleblowing, Bullying and Harassment, Information Security, Fraud or Financial Crime;
- Identify who should 'own' the investigation (who is responsible for it);
- Consider the sensitivity and confidentiality of the investigation and any special measures that are required before proceeding;
- Consider who should or should not be informed prior to commencing the investigation (e.g. person being investigated, the line manager, HR etc.); and whether this is appropriate and/or legally compliant; and
- Remember that the person responsible for the investigation is also responsible for taking legal advice from Post Office Legal as required

POL00400101

Principles to be considered during the investigation

The following principles should be adhered to wherever possible during an investigation:

- **Confidentiality** – where possible and appropriate, maintain confidentiality. Ensure that all communications are labelled 'confidential' and are kept secure. Balance the need for confidentiality with the need to carry out an effective investigation. Be aware of legal obligations regarding disclosure of information;

- **Fairness** – when following any investigation procedure, keep relevant individuals informed as appropriate. Seek expert input where necessary, e.g. from HR, from Security Teams, from Information Security Teams. Advise individuals of their right to appeal, if there is such a right under the applicable Policy;

- **Objectivity** - try to remain impartial and wherever possible base your conclusions on facts. Avoid making snap judgments or assumptions about culpability or wrongdoing;

- **Transparency** – ensure there is an audit trail of your investigation. Keep records of discussions and meetings, and notes of interviews. Retain documents in accordance with Post Office's Acceptable Use and Document Retention policies; and

- **Decision making** - prior to making your decision, ensure you have all the information you reasonably need. Prepare a report of findings. Consider who needs to be: (i) informed of the report outcome in conjunction with any applicable procedures, (ii) provided with the findings/ outcome report, (iii) advised of any follow-up actions. In some circumstances it may not be appropriate to share outcomes/ findings, e.g. in the context of whistleblowing investigations.

Who is responsible for this policy

Post Office's Board of Directors have overall responsibility for ensuring that Post Office has a framework to ensure compliance with legal, regulatory and contractual requirements. The Board is kept abreast of relevant matters relating to the

POL00400101

management of investigations by reports from its committees including its ARC Committee.

Key individuals and their specific responsibilities in relation to this Policy are:

- The General Counsel for Post Office is the Policy Sponsor, accountable to the Post Office Board overall.
- The Principal Employment Lawyer is the Policy Owner responsible for the day to day implementation of and compliance with this Policy. The Employment Lawyer is accountable to the General Counsel.

Who must comply and how

Compliance with this policy is mandatory for all Post Office employees, officers, contractors, casual workers and agency workers. This policy applies wherever in the world Post Office's business is undertaken.

It is important that you read, understand and comply with this policy. Your actions, behaviour and conduct to apply the provisions of this policy are your responsibility.

You must adhere to all parts of this policy. You should avoid any activity which may lead to a breach of this policy. We may request your confirmation of agreement to this policy. You must notify your line manager, in the first instance, as soon as possible if you believe or suspect that a breach of this policy has occurred or may occur.

You may request a policy exception or waiver to this policy, but you must follow the Post Office's exceptions and waivers procedures which can be obtained from the business continuity Policy Owner.

If non-compliance is identified the matter must be referred to the General Counsel. Any investigations should be carried out in accordance with this policy. If the cause is found to be due to wilful disregard or negligence, it will be treated as a disciplinary offence.

How we monitor compliance

The Principal Employment Lawyer will ensure that this policy is implemented, reviewed and remains effective. Post Office's internal systems and controls ensure that this policy is regularly independently assessed for effectiveness, suitability and adequacy. In addition, Internal Audit will periodically test compliance with this policy.

Review and assessment of compliance with this policy is done on a regular and timely basis. Reports are made to the Risk & Compliance Committee.

How to raise a concern

POL00400101

Any Post Office employee who has concerns about a failure to comply with this policy has a duty to:

- discuss the matter fully with their Line Manager; or,
- discuss it directly with their Head of Business Unit; or
- discuss it with Legal Services; or
- bring it to Post Office's attention independently of management, via the Speak Up Line (see Section E 'References' for more information).

Contact us and more information

If you need further information about this Policy, please contact Nisha Marwaha – Employment Lawyer on GRO or by email : nisha.marwaha GRO

Section C. Key Terms and References

Key Terms

Term or Acronym	Description
Post Office Group ('Post Office')	Post Office Limited and all subsidiaries and entities within the Post Office Group which includes Post Office Management Services Limited (POMS)

References

References	Description
Speak Up Line	"Speak Up" is confidential reporting service which is run by InTouch MCS Ltd, an independent company. More details can be found in the Post Office Whistleblowing Policy. The Speak Up service is available on GRO or via a secure on-line web portal http://www.intouchfeedback.com/postoffice.

POL00400101

Post Office Group

Physical Security Policy

POL00400101

Contents Page

POL00400101

Document Control Sheet

POLICY SUMMARY			
GE Policy Sponsor	**Policy Owner**	**Policy Implementor**	**Policy Approver**
General Counsel **Jane MacLeod**	Head of Security & Financial Crime (MLRO) **John Scott**	Senior Security Manager, Physical Security **John Bigley**	Post Office **Risk & Compliance Committee**
Version and Status	**Policy Review Period**	**Effective from:**	**Policy location:**
Current : Draft V1.1	Annually from policy effective date	28 September 2016 [to be confirmed]	Z:\NEW COMPLIANCE\New Policy Framework 2015\Refreshed Policies 2016

DOCUMENT REVISION HISTORY			
Version	**Date:**	**Author**	**Reason For Change**
Draft v1.0	8 April 2016	Diana Maddox	First draft for new policy framework
Draftv1.1	13 April 2016	Mark Rodgers	Policy Standards review
Draft 1.2	21 April 2016	Diana Maddox	Amendments following Policy Standards review
Draftv1.3	14 June 2016	Mark Rodgers/ Diana Maddox	Feedback from Executive Owner
Draftv1.4	30 June 2016	Mark Rodgers	Policy standards review

POLICY APPROVAL		
Role/Forum	**Name**	**Date:**
Executive Owner and Sponsor	General Counsel (Jane MacLeod)	30 April 2016
Executive Committee	Post Office Risk and Compliance Committee (RCC)	8 Sept 2016 [tbc]
Board Committee	Post Office Audit, Risk and Compliance Committee (ARC)	28 Sept 2016 [tbc]

DOCUMENT DISTRIBUTION STATUS			
Distribution (Mark x as appropriate)		Document Sensitivity (Mark x as appropriate)	
Internal Only	X	Non-sensitive	
External Only		Sensitive	X

QUALITY STATEMENT	
Quality Control	Next review date
This document is periodically reviewed, and at least once each year starting from the last effective from date. This policy has been reviewed against the latest Post Office policy standards.	January 2017

POL00400101

Section A. Introduction

Chief Executive's Note

The Post Office Group ('Post Office') is committed to doing things correctly. Our Business Standards are our code of behaviours that represent the conduct we expect. This policy supports the code to help us ensure the highest standards of physical security are maintained, and Post Office has an averse tolerance to physical security risk. This policy sets out what is and is not acceptable but if you have any doubts or questions, these should be referred in the first instance to the policy Owner, the Head of Security & Financial Crime, who oversees compliance with this policy. It is essential that you read this policy.

Introduction by the Group Executive Policy Owner: General Counsel

As Post Office's General Counsel and the Executive Policy Owner, I have overall accountability for physical security framework to the Post Office Board of Directors. Post Office's Audit, Risk & Compliance Committee considers physical security as a standing agenda item and the Post Office Board is updated as required.

POL00400101

Section B. Context

About this Policy

The purpose of this policy is to support the delivery of the Post Office security vision by setting the framework for the physical security protection of Post Office to keep staff safe from harm and Post Office assets secure.
This policy sets out a framework for what we must all do to protect physical security and it is a set of standards to minimise the impact and likelihood of physical security risk and/ or breaches. This policy applies our physical security risk appetite and seeks to support the wider national fight against crime.

This policy's effective date will be determined by the date on which final approval is given by the appropriate governance forum.

What is physical security?

The definition of physical security is the protection of personnel, Post Office assets and data from physical circumstances and events that could harm our people or cause serious losses or damage. This includes protection from crime and terrorism.

At Post Office, physical security framework comprises a set of integrated security measures designed to mitigate against vulnerabilities and risks.

Risk to be managed

Physical attacks such as robberies and burglaries are targeted at Post Office premises including customer support centres, Post Office branches, cash centres, cash depots and vehicles.

Post Office will manage security risk to people, premises and assets by:-

a. Undertaking risk assessments;
b. Making recommendations as to the level and type of physical security required to mitigate the identified risks such as CCTV, upgraded alarms, etc.;
c. Where appropriate, specifying security procedures to be followed ; and
d. Undertaking regular audits/reviews of Post office premises to test the integrity of and compliance with security procedures.

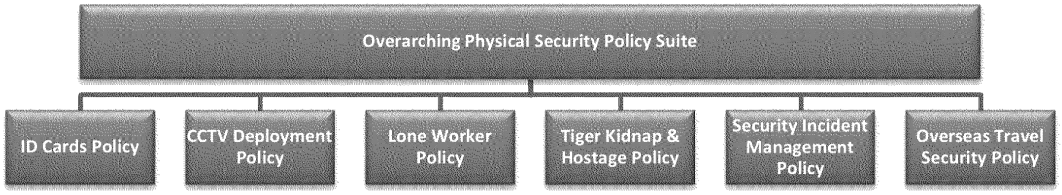
Risk Appetite

Post Office Group has an averse appetite to any physical harm to our people or Post Office assets. We take a risk based approach to prevent and mitigate such threats.

POL00400101

How we organise physical security management?

This policy overarches the broader Physical Security family policy structure. It overarches a suite of policies and each should be read in conjunction with others, and operates alongside the suite of policies that are designed to protect personal data and guard against cyber fraud. The Physical Security Policy structure is shown below:-



Who is responsible?

Post Office's Board of Directors have overall responsibility for ensuring that Post Office has a framework to ensure compliance with legal, regulatory and contractual requirements. The Board is kept abreast of relevant matters relating to the management of physical security by reports from its committees including its ARC Committee. The key individuals and their specific responsibilities in relation to this policy are:

- The General Counsel who is a member of the Post Office Group Executive is the policy Executive Owner and policy Sponsor, accountable to the Post Office Board overall;
- The Head of Security & Financial Crime (MLRO) is the policy Owner who is responsible for the day to day implementation of and compliance with this policy and who is accountable for this policy to the General Counsel; and
- The Senior Security Manager, Physical Security is the policy Implementor who is responsible for and accountable to the policy Owner for the day to day and management of physical security issues within the Post Office as described in this Policy.

Who must comply and how

Compliance with this policy is mandatory for all Post Office Group employees, officers, contractors, casual workers and agency workers. This policy applies wherever in the world Post Office's business is undertaken. All third parties who do business with Post Office Group, including consultants, suppliers and business and franchise partners, will be asked to agree contractually to this policy or to comply with their own equivalent policy.

POL00400101

It is important that you read, understand and comply with this policy. Your actions, behaviour and conduct to apply the provisions of this policy are your responsibility.

You must adhere to all parts of this policy. You should avoid any activity which may lead to a breach of this policy. We may request your confirmation of agreement to this policy. You must notify your line manager, in the first instance, as soon as possible if you believe or suspect that a breach of this policy has occurred or may occur.

You may request a policy exception or waiver to this policy, but you must follow the Post Office Exceptions and Waivers Procedures which can be obtained from the Policy Owner, the Head of Security & Financial Crime.

If significant non-compliance is identified the matter must be referred to the General Counsel. Any investigations should be carried out in accordance with Post Office Investigations Policy. If the cause is found to be due to wilful disregard or negligence, it will be treated as a disciplinary offence.

POL00400101

Section C. Policy Details

Information

Operational Security Management

The extent to which branches and other premises are protected by physical security measures is dictated by contractual requirements, governmental security requirements, legal obligations, risk assessments, business continuity, crisis management and industry best practice.

Post Office has ISO 27001:2013 certification which demonstrates that Post Office has systems in place to protect corporate information and data which is audited on an annual basis. This policy supports that certification from a physical security perspective.

The Post Office Security Operations Manual implements this policy by setting out Post Office physical security procedures and instructions in order to assist postmasters and staff in the operational security management of their branches or premises. These procedures and instructions are to be adhered to at all times.

CCTV Management

Post Office has installed CCTV systems at various branches and premises across the estate. These systems must be deployed in accordance with the Post Office CCTV Deployment Policy and operated in compliance with the Post Office CCTV Code of Practice.

All CCTV systems and their subsequent recordings, regardless of location or installation source, are to be operated in accordance with the Data Protection Act 1998, PCI Data Security Standards.

Where CCTV is installed by an individual postmaster in support of their retail operation, the postmaster will be responsible for ensuring their own compliance with the Data Protection Act 1998 in respect of the branch CCTV system.

Burglar Alarm Management

In accordance with the Security Operations Manual, burglar alarms are installed at various Post Office premises on a risk assessed basis. Each branch with an alarm must have a set of operating instructions specific to the type of alarm that has been installed and these instructions are to be adhered to at all times.

All alarm installations must comply with British Standard BS EN 50131-1:2006+A1:2009.

POL00400101

Access Control Management

Access to branch secure areas will only be given to formally identified and authorised persons, whether Post Office employees, contractors or visitors. The branch manager/postmaster must ensure that access is be controlled in accordance with the Admittance of Visitors instructions in the Post Office Security Operations Manual.

Access to customer support and supply chain locations must be controlled in accordance with the Post Office ID Cards Policy or Supply Chain Process S 5.2.9: Control of Visitors and Staff, which includes a formal authorisation and identification procedure. The site manager at each location is responsible for deploying a procedure at their site to ensure that all staff, contractors and visitors shall at all times be recognisable by the wearing of a photographic identity card (staff and contractors) or a visitor's badge.

Furthermore, the site manager must deploy a procedure to ensure that all Post Office employees, branch managers, postmasters and contractors must at all times observe the access control arrangements of any building in which they are working or visiting. All employees and contractors have a duty to maintain this security process in a robust and continuous manner.

Branch Format Management

Post Office operate a suite of branch formats which are defined by a number of risk factors. Risk assessments are conducted and the format of individual branches is specified by the outcome of this assessment and in accordance with the guidance within the Format Standards documentation. Thereafter, any changes to branch format may only be implemented following an updated branch risk assessment.

ATM Protection Management

The Bank of Ireland has installed ATMs at many branches across the Post Office estate; some of these ATMs are serviced directly by Post Office Supply Chain team staff, whilst others are serviced by branches themselves following delivery of cash by Post Office Supply Chain. To assure the physical security of each ATM across the Post Office estate, branches must adhere to the security instructions within the Post Office Security Operations Manual.

Safe Management

In accordance with the Post Office Security Operations Manual, regardless of safe type it is incumbent on branch managers/postmasters to ensure that the safe(s) they have installed are operated correctly and that they are used for their designated purpose

Supply Chain Management

Post Office is a member of the Bank of England Note Circulation Scheme and must comply with the security standards of the Scheme at all times in order to retain

POL00400101

membership. These standards include specific physical security measures which must be in place and these standards are audited by the Bank on an annual basis. Post Office Supply Chain have a robust set of security processes that are operated across cash centres, depots and vehicles to assure compliance with those standards.

Risk assessments are carried out to review the threat of a criminal attack directed against Post Office Supply Chain cash centres, depots and vehicles and assess the impact on employees who may in the course of their work be exposed to injury from such incidents. Security control measures are constantly reviewed to reduce the risk of criminal attack, taking into account the available intelligence to minimise the likelihood of robbery and resulting injury against either the employees or loss of assets.

Other Physical Security Tools Management

All other security tools are installed as a result of the risk assessment process outcomes. It is incumbent on postmasters and their staff to ensure that the tools function correctly, they are used for their designated purposes and are operated in accordance with the security instructions within the Post Office Security Operations Manual (as defined in section E of this policy).

Our Controls and arrangements

Post Office key general controls are designed to prevent, detect, investigate and review security risks. These are:-

- Post Office carry out a programme of unannounced visits by Security Managers to random branches to test the integrity of and compliance with branch security procedures in accordance with the Post Office Security Operations Manual;
- Post Office implement a programme of initiatives across the Post Office Supply Chain network to test the integrity of and compliance with Post Office Supply Chain security procedures;
- Post Office complete an annual review of customer support centres to assess vulnerabilities/ risks and make recommendations for additional physical security measures to mitigate those risks;
- The Physical Security team own the robbery/ burglary risk model which is based on various key influencing factors to support the Physical Security strategy. The model supports branch formats, identifying branches at risk of further incidents, helping to target robbery and burglary prevention activities so that fewer incidents occur and identify the parameters affecting risk and the likely impact that implementing mitigation will have on risk. The model is reviewed on an annual basis to ensure it includes changes to the underpinning influencing factors;

POL00400101

- The Physical Security Forum will assess compliance with the Physical Security family of policies on a regular basis as part of the overall governance detailed in Section D;
- Regular supplier service reviews are completed to ensure governance with supplier contracts and to address any service issues identified;
- When a robbery/burglary incident occurs at branches, post-incident visits are carried out to investigate the incident thoroughly working in conjunction with law enforcement agencies. If physical security risks are identified during the visit, recommendations for additional security measures are made to mitigate those risks; and
- Security management information reports are issued on a regular basis to the Physical Security Forum for oversight and review.

POL00400101

Section D. Governance

How we monitor compliance

The Head of Security & Financial Crime will ensure that this policy is implemented, reviewed and remains effective. Post Office internal systems of risk control ensure that physical security controls in this policy are regularly independently assessed for effectiveness suitability and adequacy. Post Office Internal Audit retains independent third line oversight with regard to this policy.

We assess compliance with this policy on a timely basis and regular Physical Security reports will be issued by the Head of Security & Financial Crime to Post Office's Risk & Compliance Committee and the Post Office ARC.

We require our subsidiaries and third parties to have at least equivalent arrangements, systems and controls to this policy.

How to raise a concern

Any Post Office employee who has concerns about a failure to comply with this policy has a duty to:

- discuss the matter fully with their Line Manager; or,
- discuss it directly with their Head of Business Unit; or,
- bring it to Post Office's attention independently of management, via the Speak Up Line (see Section E 'References' for more information).

Contact us and more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact John Scott – Head of Security & Financial Crime on GRO or by email at john.m.scott GRO

POL00400101

Section E. Key Terms and References

Key Terms

Term or Acronym	Description
Post Office Group ("Post Office")	Post Office Limited and all subsidiaries and entities within the Post Office Group which includes Post Office Management Services and FRES
Executive Policy Owner	As defined by the Post Office Policy Framework-Roles and responsibilities Matrix document V0.5
Policy Owner	As defined by the Post Office Policy Framework-Roles and responsibilities Matrix document V0.5
CViT	Cash and Valuables in Transit
Supply Chain	Cash centres/depots and vehicles

References

References	Description
Security Operations Manual (issued July 2013 – currently under review)	A set of procedures and instructions for postmasters to follow in the operational security management of their branch
CCTV Deployment Policy v1.1	Defines the framework for CCTV deployment throughout Post Office estate, CViT fleet and customer support centres
CCTV Code of Practice v0.1	Details requirements by Post Office for the operation of CCTV systems in it premises to ensure compliance with the Data Protection Act 1998
Data Protection Act 1998	This Act sets out legal requirements for compliance where personal data is captured and processed

POL00400101

ID Cards Policy v1.2	Sets out policy for access control for staff and visitors at Post Office cash and stock centres, cash depots and customer support centres
Bank of England Security Standards of the Note Circulation Scheme v7	These standards are the minimum standards set and updated by the Bank of England from time to time that must be met by cash centres who are part of the Note Circulation Scheme
S5.2.9 Control of Visitors and Staff – Supply Chain Operational Unit	Procedures for access control at Supply Chain centres and depots
PCI Data Security Standards v3.0	Standards/controls established by the PCI Security Standards Council to maximize security of cardholder data
Formats Standards	A set of standards documents that define security requirements for different branch formats
Physical Security Forum	The Physical Security Forum provides governance and decision making for all security matters, both policy-wise and operational
Whistleblowing (Speak Up Line)	In case of concerns staff may contact their line manager, a senior member of the HR Team, or if either or both are not available staff can contact Post Office's General Counsel, Jane MacLeod who can be contacted by email on: 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

POL00400101

Post Office Insurance renewal

Author: Paul Hemsley Sponsor: Alisdair Cameron Meeting date: 28 Sept 2016

Executive Summary

Context

The business has a series of insurance policies due for renewal on 1 October 2016.

Question addressed in this report

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

Conclusion

A summary of the policies and cover can be found in the broker's report, attached.

These cover the business for most major risks albeit with high deductibles.

No significant changes are proposed.

The Broker notes that POL claims are low and that this is reflected in premium levels, which reduce by IRRELEVANT year on year.

Input Sought

The ARC is asked to approval the renewal as set out in the brokers' report, for submission to the Board for its approval.

Attachment 1: Report of brokers (Lockton) to Post Office

POL00400101

Post Office

2016/17 Insurance Renewal

Summary Report - August 2016

LOCKTON®

POL00400101

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 1 st 2016. The key points to note include:

- Lockton were appointed as insurance broker to post Office last year and for the 2015 renewal achieved overall savings in premiums of circa IRRELEVANT together with various improvements to our policies.

- This year Lockton were tasked with driving further cost savings whilst maintaining appropriate levels of cover for this renewal and we have achieved overall premium reductions of circa IRRELEVANT IRRELEVANT again with some improvements to our policies.

- This has been achieved through developing insurers' understanding of our risks, working closely in a tri-partite fashion with you and your insurers and leveraging your risk quality and buying power with insurers.

- Your Professional Indemnity and Cyber insurances renew in December and April respectively; we also arrange a 3 year Special contingency insurance policy that renews next October. These are shown in this paper for the sake of completeness.

- Your risks and risk register have been reviewed as part of the renewal process and we consider the insurances you purchase to be reasonable and appropriate for Post Office. There are wider coverages now available for your crime risks which we are reviewing with you and are obtaining costings for these. Lockton are also suggesting you consider broadening your Cyber insurances to the organization as a whole.

- 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*.

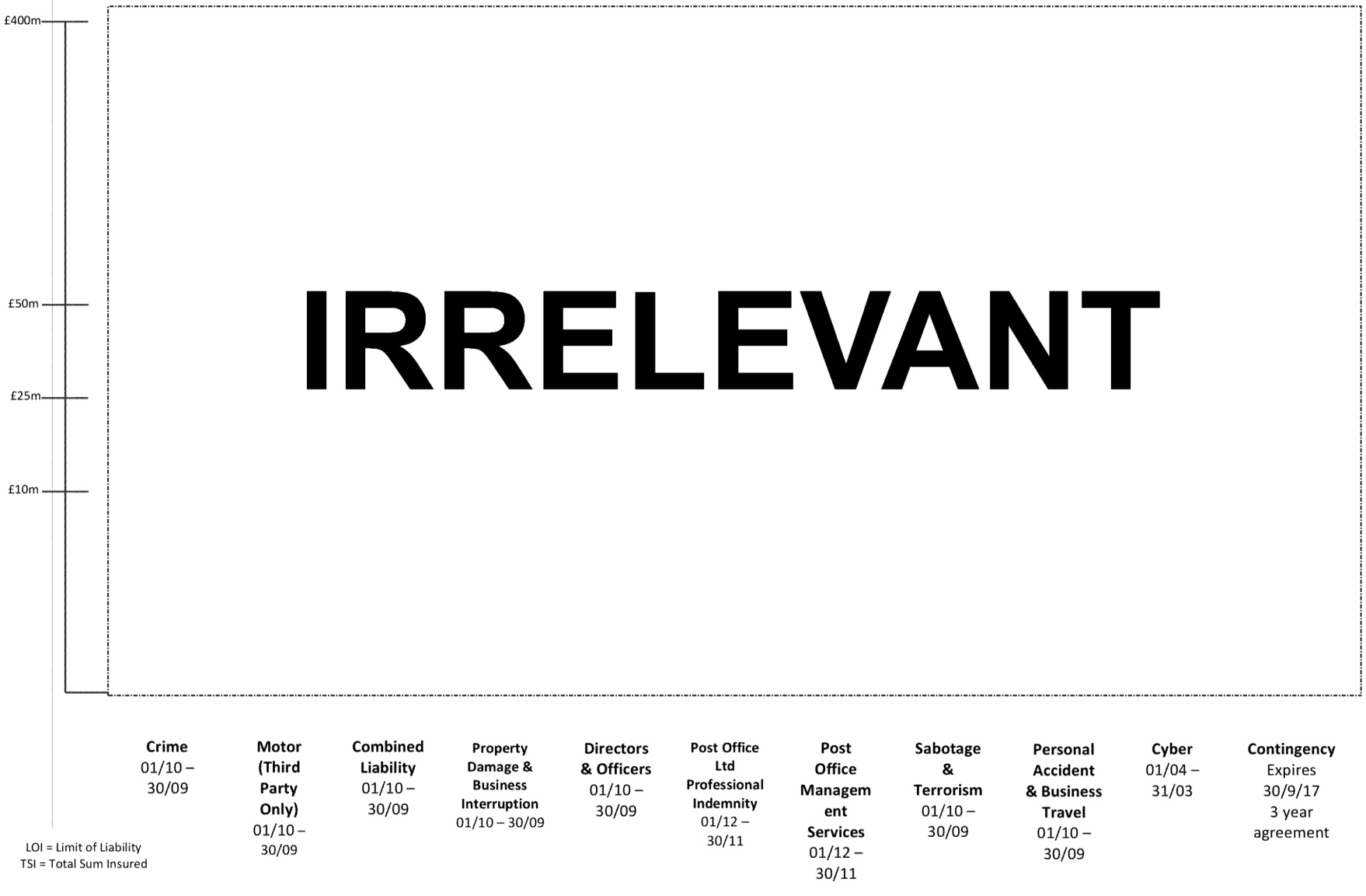
- All policy deductibles for this renewal are as per expiry; apart from Motor and Combined Liability where the deductibles have reduced from IRRELEVANT any one claim to IRRELEVANT (you also have a cap on the accumulation of losses within the motor and casualty deductibles, which has been reduced from IRRELEVANT in 2015 to IRRELEVANT for 2016) .

* 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.

POL00400101

Programme structure chart

The chart below shows the various insurances Post Office currently purchase (details as proposed for renewal at 1/10/16).



LOI = Limit of Liability
TSI = Total Sum Insured

POL00400101

Summary of policy cover

Crime

This insurance is made up of a primary IRRELEVANT policy with 'excess layer' policies providing an overall limit of IRRELEVANT with a IRRELEVANT deductible). The key risks are your cash centers but this policy also includes the general theft and fraud risks you face.

Motor Liability

Third party only cover against liabilities arising out of the use of your road vehicles, including contingent cover that protects Post Office wher e employees use their own vehicles for Post Office business. This is also, of course, a statutory insurance.

Combined Liability

Employers Liability cover (a statutory cover for liabilities to employees) and Public/Produ cts Liability cover protecting you against liabilities to third parties.

Property Damage and Business Interruption

An 'all-risks' basis of insurance cover for your physical assets, although as with all insurances the policy does have exclusions. You only insure individual properties with a value over IRRELEVANT The policy is 'full value', based upon the property values you declare to insurers. The policy also includes business interruption cover in the form of 'increased costs of working' with a IRRELEVANT t and a IRRELEVANT month Indemnity Period.

Terrorism

Insurance against damage to your physical assets arising out of a terrorist incident, with a policy limit of IRRELEVANT per claim. This limit is based upon your largest exposure at Swindon.

Directors and Officers Liability

Covers the cost of compensation claims made against your business's directors and key managers (officers) for alleged wrongful acts.

Wrongful acts include:

- breach of trust
- breach of duty
- neglect
- error
- misleading statements
- wrongful trading

Professional Indemnity

Professional Liability arising out of certain specific activities – you have two policies, one for POMS and another for POL in respect of two contracts which require you to have this cover.

Cyber

Applies only fo r risks arising out of two contracts and covers first party cyber risks such as extortion and Notification and PR Expenses. It also includes liability cover for Privacy, Breach of confidentiality, Regulatory fines, Mitigation costs and Cyber Liability .

POL00400101

Personal Accident/Business Travel

Provides fixed benefits following bodily injury for all Employees whilst in pursuit of occupation al duties on your behalf away from usual place of employment or whilst travelling directly to or from the usual place of employment from their permanent or temporary residence, but only where the Bodily Injury is as a result of Terrorist attack.

Provides fixed benefits for all Employees including their accompanying Partner and/or children during Foreign and Domestic Business Travel including incidental holiday.

Also provides fixed benefits for all Post Office Sub-Post Masters and Sub-Post Mistresses and their substitutes, their registered Assistants and their substitutes including those working under franchise and modified Sub Post Contracts , at any time as a direct result of an unprovoked malicious assault by another person where the assault is directly in connection with the I nsured Persons duties or position with the Insured.

Special Contingency

Details of this are not widely circulated .

POL00400101

Premium summary

Policy	2014/15 Future Annual Premium	2015/16 Premium	2016/17 Premium	Percentage Premium Saving 2015/16 – 2016/17	2016/17 Premium Comments
Crime					
Motor					
Combined Liability					
PD & BI					
D & O					
Terrorism					
PA & Travel					
Total					
Total inc. IPT					

Other policies, not due fo

PI – POL	
PI – POMS	
Cyber	
Contingency	

IRRELEVANT

POL00400101

Lockton Remuneration

The remuneration agreement with Lockton is set out in our contract with Post Office and includes a base fee plus a performance fee based upon premium savings. This was designed to ensure incentivisation against your key objectives and to ensure sustainability over the long term of the cost reductions achieved.

In addition Lockton receive certain insurer services brokerage for administrative functions they fulfill, which Lockton declare and were taken into account during our contract negotiations (the value to Post Office is that Lockton's' fee is lower as a result of this, a further cost benefit for Post Office).

Lockton's' remuneration for 2016 is as follows:

Fee	IRRELEVANT
Performance bonus	
Insurer services brokerage	
Total	

Please note that these figures include the PI and Cyber policies which renew in December and April respectively (other than any additional performance bonus that might be achieved) .

POL00400101

Financial Reporting Update

Author: Paul Hemsley Sponsor: Al Cameron Meeting date: 28 September 2016

Executive Summary

Context

During 2015-16, the CFO identified that a systematic programme was required to improve financial reporting controls. Increased assurance was provided around the 2015-16 year-end with additional income reconciliations and balance sheet reviews undertaken by POL staff, KPMG and our external auditors, EY.

In 2016-17 the focus is on implementing a sustainable Financial Controls Framework ('FCF') that maps end to end financial process and risk, identifies remediating controls and introduces evidenced self-assessment and monitoring. The purpose of this paper is to update the ARC on the progress made in implementing a FCF and the priorities for the second half of the year.

Questions addressed in this report

1. What progress has been made in implementing the Financial Control Framework, what are the next steps and when do we expect to complete the work?
2. What other control improvements are planned or in progress?

Conclusions

The development of the FCF is well underway, with the majority of processes mapped, controls identified and assessed. Some 77 control gaps are open, of which 10 are considered higher risk. Self-assessment technology is in place and control and process owners have been identified.

By the end of the financial year we expect all gaps to have been identified and remediated, at least with work-around controls. Every control will have been through at least one round of self-assessment and every process will have had a sample of controls independently assessed.

Input Sought

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

POL00400101

The Report

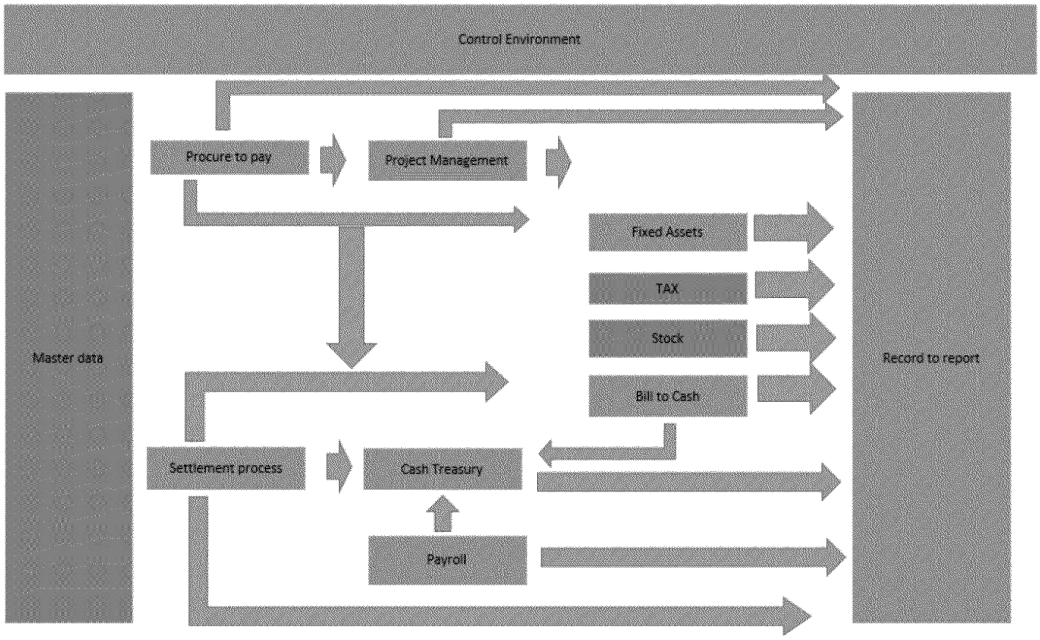
What progress has been made in implementing the Financial Control Framework, what are the next steps and when do we expect to complete the work?

1. The Financial Control Framework follows standard steps, as follows:

Process Mapping	End to end process mapping to identify risk and create a permanent record of how we work. Each process will have an identified owner and a senior sponsor.
Risk and Control Matrices (RACMs)	Identify the risks in the process and the controls required to remediate them. Each control will have an identified owner.
Gap identification	Identify where controls are absent, badly designed or inadequate.
Gap remediation	Agree the steps required to make the controls fit for purpose and implement required changes.
Self-assessment	Control owners confirm on established software that they have the evidence that their control was operating effectively in the previous period. Process owners confirm quarterly that any changes to processes have been approved and updated in the documentation and controls are operating effectively.
Assurance	Random testing of controls evidence.

2. The content of the financial reporting framework can be summarised as set out in the diagram below. The areas in green are already underway.

POL00400101



3. In summary, for the areas marked green, with the support of KPMG, the following steps have been undertaken:
   - Processes have been formally documented
   - RACMs have been created
   - Controls have been assessed and gaps identified
   - Process and control owners and process sponsors have been identified

4. Overall, 242 key controls have been identified for us to rely on, of which 87 had some gaps. 10 gaps have been remediated and the remainder graded by impact with 10 having a high impact, 27 medium and 40 low – low risk gaps are typically where we believe that an effective control is in operation but the evidence is not routinely collected.

5. The current high risk gaps and the next steps are as follows:

High Risk Gap	Action
The period end checklist does not cover the full set of accounts, tasks and dependencies	The checklist will be completed and communicated to relevant team members (Phil Birds, end November 2016)
Journals receive a sense check versus previous months but are not formally approved by a member of the FLT	Formal monthly approvals will be in place (FLT, December 2016)
Monthly balance sheet probity reviews by the central Finance team are not signed off by the Finance Directors for each area	Increased focus from October 2016, with sign offs in place by December 2016 (FLT)
Balance sheet probity reviews are not independently reviewed	Independent reviews in place (Financial Controller, December 2016)

POL00400101

Branch cash balances are not routinely reconciled between POLSAP and Horizon	Unreconciled difference reduced from IRRELEVANT Fully operational as part of month-end in Q3 (David Jordan, from October)
Goods receipting is done inconsistently with limited reviews of open purchase orders	Formal monthly reviews in place (David Jordan, December 2016). Underlying systems changes to enhance process consistency (TBD)
Lack of segregation of duties between staff updating payroll master data and staff processing the payroll	The duties will be split as a priority (Joe Connor, TBD, Q3)
No central review and quality check of bank reconciliations	All bank reconciliations will be reviewed by head of financial reporting or the Treasurer. (Danielle Goddard, Tim Walker, 30 November 2016)
Balance sheet reconciliations of variable quality	Training for owners being undertaken through September/October. All reconciliations reviewed in P3 and reviews will be repeated Q3.
Policies to manage and control spreadsheets are inconsistently applied	Formal controls over passwords, change, IS back up etc have been identified: full application to key spreadsheets (Phil Birds 31 January 2017)

6. The next steps are to:
   - Train all process and control owners on their new accountabilities by end December 2016.
   - Rectify the remaining identified gaps. This is scheduled to be completed in most cases during Q3 and entirely by end January 2017.
   - The areas in grey have not yet been started and represent the priorities for the remainder of the year, in the following order: master data management; indirect taxes; stock; direct taxes. Gap analysis and remediation is expected to be complete by end January 2017.
   - Agree an approach to proving the operation of underlying routines in IT systems such as SAP. Based on experience, this may require spreadsheet replication of a sample of transactions.
   - The self-assessment software is in place and is being populated with the processes referred to above. Controls in the Client Settlement process will be formally self-assessed and audited as at the end of September. All of the processes noted above will have been through a round of controls self-assessment by end February 2017
   - All processes will have had some sample checking of self-assessment before year-end.

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

POL00400101

8. Other questions are:
   - Do we undertake sufficient audits of cash held in branches (in discussion, CFO and Network Director)
   - Do we need to physically verify tangible fixed assets with no carrying value (no: CFO decision)

What other control improvements are planned or in progress?

9. As noted in the update presented to the ARC on the BCV issue, we are undertaking a systematic review of the way we manage customer and agent fraud. While this has presented limited risk from a financial reporting perspective, the additional controls and transparency will give additional assurance over balances with agents, customers and clients.

10. Over the remainder of 2016-17, we will continue to work to improve our control over IT and change projects, ensuring that we identify and report issues and overruns at the first opportunity. Again, while this has not led to recent errors in financial reporting, stronger controls will provide additional assurance.

11. We are working with EY to improve the quality and ease of the audit of IT controls. A planned internal audit review of joiner and leaver processes may help us to identify improvements.

12. Working with EY, we will assess in Q4 whether and to what extent we need to replicate the additional testing performed for the 2015-16 audit.

POL00400101

Horizon Scanning Report

Author: Jane MacLeod
Meeting date: 28 September 2016

Executive Summary

Context

As part of its remit, the Board Audit Risk & Compliance Committee should consider legal, regulatory and other external developments on behalf of the Board in order to ensure that impacts on Post Office (including its customers, staff, suppliers and stakeholders) are understood and being appropriately managed. This report highlights current developments of relevance to Post Office and the work that is being done to monitor these.

Questions this paper addresses

1. What are the material legal, regulatory and other external risks the Post Office executive and Board should currently be aware of?
2. What work is being undertaken to assess, monitor and mitigate these risks?
3. Who is accountable for this work and how will it be reported through Post Office governance structures?

Conclusion

1. There are a number of material developments which either will or could impact Post Office and details of these are set out in this summary.
2. In each case work is being undertaken to monitor and assess the risks arising from these developments. The Corporate Services team is working with the different stakeholders to progress this assessment.
3. Governance structures and reporting lines will be developed to ensure there is appropriate representation from across Post Office in formulating responses to, and mitigation plans for, these developments.

Input Sought

The ARC is asked to note these developments.

POL00400101

The Report

Brexit

1. Following discussions at the Group Executive in July 2016, it was agreed that a group of senior staff would be brought together to co-ordinate Brexit-related work across the Post Office. It will also provide a more formal vehicle for the identification and management of other significant external legislative, regulatory and political developments. The External Affairs Steering Group, chaired by Mark Davies (Communications and Corporate Affairs Director) met for the first time on 8 September 2016 to agree its terms of reference and gather views as to early priorities. It will report to the RCC and ARC on a regular basis.

2. Given the lack of specificity from Government about what, precisely, the UK's exit from the EU will entail even at the macro level, it is not possible meaningfully to define a 'Brexit Risk' per se. Instead, the risks which do manifest themselves at whatever point, will be mainstreamed into the risk registers and profiles of the functions they affect.

Investigatory Powers Bill (IPB)

3. The Committee will be aware of long running controversies ("Snoopers' Charter") surrounding both the Coalition Government and current Government's various attempts to update the law relating to investigatory powers by law enforcement and intelligence agencies.

4. In November 2015, the Government published its latest proposals in the draft Investigatory Powers Bill, which will govern not only the use but critically the enhanced oversight of investigatory powers by law enforcement and the security and intelligence agencies.

5. Since the start of 2016, three Parliamentary Committees published their scrutiny of the draft Bill, drawing on evidence submitted by a host of interested parties. These three reports outlined significant concerns with the draft Bill and highlighted key areas of improvement necessary for the Bill to generate the confidence and trust necessary for the exercise of surveillance powers. These related, inter alia, to the compatibility of the proposed UK system with international norms, riles governing the collection of bulk data, the obligations of communication service providers (CSPs) to facilitate access to data (and encrypted data), and transparency.

6. In response, the Government has published a revised Bill that has attempted to bring together the key recommendations of the three reports. The revised Bill went through line by line scrutiny during the Public Bill Committee stage in late April/early May. Following the work of the Public Bill Committee, and the very comfortable passing of the Bill in the Commons at Third Reading, the Bill is now in the House of Lords.

POL00400101

7. Now that the precise provisions of the Bill are becoming more stable, Post Office will need to assess the impact of these on a number of aspects of its business, from the more obviously affected in telecoms, to perhaps less obvious potential impacts, including on current and future digital services. The External Affairs Steering Group noted the need for a number of subject matter expert colleagues to be mobilised to assess and, where necessary, adapt to the forthcoming changes at its on 8 September and is taking steps to ensure this happens.

POL00400101

Appendix

STATUS OF PREVIOUSLY REPORTED DEVELOPMENTS

Issue	Brief Description	Update
Money Laundering	Implementation of the recommendations in the Promontory Report HMRC compliance audit	Please refer to separate paper in this pack. To note, however, consultants Thistle Initiatives work on the Risk Assessment required to assess and progress the Promontory recommendations on 26th July 2016 is well advanced.
Brexit	Assessing impact on Post Office should the result of the referendum be to leave the EU	We continue to monitor the developments with a view to assessing the possible impact of an 'exit' vote, notably through the newly established External Affairs Steering Group, referenced in the body of this paper.
GDPR	New and more onerous EU Data Protection Regulation	Work to begin the development a two-stage implementation project, to meet the compliance deadline is underway. A GDPR 'Readiness Assessment' workshop took place on 26/08/2016, in conjunction with PwC. The second phase 'special characteristics' workshop will take place in October to define priorities at more granular level and the outputs from both workshops will then inform the priorities for the GDPR project as a whole, to ensure that the activities required to achieve compliance by May 2018 can begin in a focused, methodical, manner.
Networks and Information Security Directive	New EU Directive to support GDPR	

POL00400101

Outstanding Audit Actions - Contract Management

Author & Sponsor: Jane Macleod Meeting date: 28 September 2016

Executive Summary

Context

The Contract Management Audit undertaken in late 2015 recommended a series of further actions. As a result, in October 2015 all Business Areas were requested to, and did, provide information about the material contracts which they managed and it was planned to undertake further work to map obligations arising from material contracts. This paper summarises progress to date.

Questions this paper addresses

- What progress has been made to date?

Conclusion

1. The outstanding action from the audit was for all Business Areas to map obligations under material contracts and validate they had a documented process to demonstrate:
    - obligations on Post Office
    - obligations on Supplier/Client
    - frequency of obligations
    - processes by which performance of obligations are monitored and
    - what MI is produced to demonstrate performance (both quantitative and qualitative) of obligations.
2. In early 2016 over 50 contracts were identified as 'material' (being value/cost of > £5m per annum or otherwise critical to operations).
3. Subsequently during July 2016 a subset of 25 key contracts was defined (as set out in the Appendix). GE members were requested to arrange for the obligations on each contractual party to be mapped in a standard template. The expectation was that the completed template would assist the Contract Manager to identify:
    - what obligations were required to be performed by each party to the contract;
    - the frequency of performance of those obligations;
    - the standard to which obligations were required (or identifying where in the contract the standard was stipulated)

POL00400101

- which role/individual within Post Office was required to perform those obligations (where it was not the contract manager); and
- how Post Office would demonstrate its compliance with the contract.

4. Once completed the template would provide a working tool for the ongoing management of each of the relevant contracts, as well as a useful guide for knowledge transfer when responsibilities for the contract changed.
5. Work on this exercise is ongoing, with material progress having been made across the 25 contracts. Workshops have been held for the contract managers responsible for completing the exercise and these have proved successful in further articulating the value of the exercise.
6. Once work on these contracts has been finalised, we will roll out a programme to update other material contracts. We are also considering options to provide assurance as to the quality of completion of the templates.
7. In parallel, 15 contract managers have begun an e-learning training programme on contract management though the International Association of Contract & Commercial Management. Subject to the feedback from that cohort, we expect further cohorts of contract mangers to undertake the training.
8. Going forward all new contracts will be required to have gone through a similar mapping process as part of the transition from procurement to live management.
9. In addition, GE members have been requested to include the following in the quarterly objectives of any person nominated as a contract manager:
    - that the contract manager has access to a complete signed copy of the contract in question, together with all contractually agreed changes, alterations etc;
    - that the obligations mapping exercise has been completed in respect of each such contract (which should also include changes driven by CCNs etc)
    - that copies of the contract and the competed obligations mapping template are stored in the centralised digital datebase.
10. Contract management will be included in the General Control Framework.

11. Input Sought

The Committee is asked to note the status and agree plans to address this work.

POL00400101

APPENDIX

KEY CONTRACTS

Contract Owner	Contract	Contract Manager
Infrastructure		
Al Cameron/IT	Fujitsu (Horizon)	Sharon Gilkes
Al Cameron/IT	Accenture (Back Office and CDP)	Sharon Gilkes
Al Cameron/IT	BT/Verizon	Sharon Gilkes
Al Cameron/IT	Computacentre	Sharon Gilkes
Al Cameron/IT	Atos	Sharon Gilkes
Al Cameron/IT	AEI /3M	Sharon Gilkes
Al Cameron/IT	NCR	Sharon Gilkes
Supplier		
Martin George/ Commercial	Royal Mail	Mark Siviter
Martin George/ Commercial	Home Office (Passports, UKVI)	Chris Doutney (David Mercer, Charles Brown)
Martin George/ Commercial	DWP (POCA)	Chris Doutney (David Mercer, Charles Brown)

POL00400101

Contract Owner	Contract	Contract Manager
Martin George/ Commercial	DVLA	Chris Doutney (David Mercer, Charles Brown)
Nick Kennett/FS	Moneygram	Paul Wordsworth/ Chrysanthy Pispinis
Nick Kennett/FS	FRES	Paul Wordsworth/ Chrysanthy Pispinis
Nick Kennett/FS	Santander	Paul Wordsworth/ Chrysanthy Pispinis
Nick Kennett/FS	Bank of Ireland	Paul Wordsworth/ Chrysanthy Pispinis
Al Cameron/ Finance	SAP	Ben Cook
Al Cameron/ Finance	RBS	Charles Colquhoun/Paul Hemsley
Al Cameron/ Supply Chain	Transtrack	Sandra Murray
Al Cameron/ Supply Chain	NCS	Charles Colquhoun/Paul Hemsley
Martin George/Commercial	Fujitsu (telco)	Geoff Smyth
Martin George/Commercial	HP Europe/JP Morgan	Chris Doutney (David Mercer, Charles Brown)
Nick Kennett/ FS	HH Global	Mark Dennis
Kevin Gilliland/ Network	Servest	Steve Norris
Kevin Gilliland/ Network	BNPP	Steve Norris

POL00400101

Contract Owner	Contract	Contract Manager
Kevin Gilliland/ Network	CBRE	Steve Norris
Kevin Gilliland/ Network	WH Smith	Julie Thomas

POL00400101

Property Compliance Update

Author: Steve Norris Sponsor: Thomas Moran Meeting date: 28 September 2016

Executive Summary

Context

This noting paper updates the ARC on progress in improving property compliance. It, and the actions noted in it, are the result of the significant risks identified through the initial property risk assessment undertaken earlier this year.

Questions this paper addresses:

1. What improvements have we made to property compliance and its governance?
2. To what extent have we addressed the fire, electrical and fabric compliance issues raised in the July report and what is our overall risk profile?
3. What further matters have arisen since the last update in July?

Conclusion

1. The backlog of statutory inspections and risk assessments across the estate is now cleared, so all inspections are now 'BAU'. A new 'RAG' compliance report was launched in September to monitor this as BAU. The fortnightly Property Compliance Forum holds our contractors and Post Office to account.
2. On fire, our risk assessments identified 6,800 issues. We have resolved 1,167 (98%) of the 1,190 high risks. The remaining 23 are work in progress and will be completed by the end of October 2017. All electrical remedials are on track to be completed by the agreed FY end, to budget. All high risk building fabric H&S issues are resolved and we are now undertaking a due diligence process with BNP Paribas to avoid overspending on non-essential repairs at sites we are due to vacate, eg. through franchising. As a result of this work, our overall risk profile is now between medium and low with a few remaining high fire risks as stated above.
3. It is clear we need more work to embed a strong compliance and risk management culture which will be shown in up to date log books and other 'good housekeeping'. We have also identified an opportunity in the way we deal with environmental issues across our business. We could improve our brand by simply reporting what we already do more effectively, and by focusing on this agenda without material extra cost. The Head of Health & Safety has set up a focus group to review this.

Input sought

The Audit & Risk Committee is asked to approve this report and to support the management actions noted in it.

POL00400101

The Report

What improvements have we made to property compliance and its governance?

We have previously reported on the well-established '5 pillars' of good governance and do so again here for ease of reference. We have progressed well against each as follows:

1. Leadership, accountability and culture

   a. All relevant suppliers and internal teams who take part in the Property Compliance Forum have robust plans aligned to the risk averse appetite set by the Board;
   b. We are working towards a culture of good housekeeping, particularly on fire safety, to ensure recent improvements are maintained and built on. To that end, CBRE (our outsourced FM provider) engineers have visited all sites to offer assistance to the Person in Charge (PiCs) to understand their site fire risk assessments. This has been followed up with Comms to all sites and phone calls by the H&S team to emphasise the criticality of compliance and to offer help. As of the 20th September, of the 1,190 high fire risks identified, 1167 (98%) have been addressed and 23 are work in progress.
   c. We have completed over 60 people days' worth of regulatory compliance training for the Post Office Team and recruited a Compliance Manager; and
   d. We have more PiC training planned for Q3/4 which will support a culture of property compliance risk management across our organisation.

2. Structure, processes and performance oversight

   a. The hiring of an experienced Compliance Manager, Yvonne Berry, brings our Property team to full strength. Yvonne chairs the Compliance Forum;
   b. We are fully compliant with our legal and statutory duties regarding responsible roles for compliance. These are, as noted to the ARC in May 'Duty Holders', 'Responsible Persons' and 'Competent persons';[1]
   c. We have risk profiled all sites using information from CBRE, Servest and BNP Paribas. This is based on 7 risk criteria and 32 sites have been classified as representing the highest risk to the business. A comprehensive of remedial works, supported by site visits and audits, will ensure they are, along with all other sites, low risk by the end of 2016/17.

[1] *The Duty Holder is Tom Moran, General Manager, Network; the Responsible Person for each area (eg. fire, electricals, legionella) is a named person within the Property or Health & Safety team; and the Competent Persons are our suppliers: CBRE, Servest and BNP Paribas.*

POL00400101

There are 31 inherently high risk sites which require particular attention on an ongoing basis. These are all Crown branches as follows (sites destined for exit in italics):

Aldwych	Ashford	Canning Town
Clacton on Sea	Clapham Common	Cosham
Crossgates	Great Portland Street	Guildford
Harringay	Hyde	Lancing
Old Street	Stockport	Sutton
Vauxhall Bridge	World's End	York Lendal
Beeston	*Bromsgrove*	*Dunraven Place*
Eastleigh	*Fiveways*	*Londonderry*
Lowestoft	*Peterborough*	*South Ockendon*
Southend on Sea	*Stevenage*	*Walworth*
Warrington		

d. Our PiC handbook is being refreshed and we are updating all relevant policies. For example, we have updated our asbestos management plan and halved the length. Our objective is to complete a new standard indexed site log book which includes the PiC Handbook by the end of September and refresh all our policies by year end.
e. It became clear from our fire risk assessments that we need to improve PiCs' level of knowledge on compliance. Further PiC training and support meetings in H2 of this year will address this.
f. Although not a statutory requirement, we are establishing Deputy PiCs for additional site cover which we have assessed as being more suitable than 'peer to peer PiC' approach. All supply chain sites now have trained Deputy PiCs. We are in the process of identifying and training Deputy PiCs for Crown Offices and some have been trained. In the interim, the Health & Safety Business Partners and Crown management team will provide any additional support needed.

3. Risk Monitoring

a. Our new statutory compliance tracker went live on 2nd September. This tracks our KPIs, in particular:
   - Statutory inspections & Risk Assessment by due date; and
   - Remedial work by close out and percentage completion rate.
b. The Compliance Forum receives monthly reports from suppliers and any other part of the business on 'near misses' and incidents. This is working well but can be improved – we are introducing a new reporting template which will include contractor incidents that relate to Post Office property from an H&S and compliance perspective. We aim to implement this over the next quarter.

POL00400101

4. Engagement with stakeholders

Engagement between key stakeholders concerning property compliance continues to be strong through representatives attending the Compliance Forum. The Property and H&S teams are now working very closely with our operational teams on a day-to-day basis.

5. Management of information

All information is kept on secure sharepoint sites for current and future reference. We continue to report regularly to the RCC and ARC and the GE Health and Safety sub-Committee.

To what extent have we addressed the fire, electrical and fabric compliance issues raised in the July report and what is our overall risk profile?

1. Regulatory risk Monitoring

All overdue statutory risk assessments have been completed, and Statutory Compliance inspections and assessments will now be undertaken as business as usual. Eliminating this 'backlog' is a significant milestone which allows us to plan time and resources more effectively, and should prevent any issues being overlooked. The focus is now on completion of remedial works to address medium level risks:

a. Electricals: Remedial actions to address the remaining medium level risks have started and are on track. They will be completed by March 2017 at a total cost of £1.1m to achieve a low risk level outturn;
b. Building fabric: All fabric remedial work plans and costs to address medium level risk have been submitted by CBRE and we are reviewing them at present. These will cost a maximum of c£1.4 million over two years. We are currently conducting due diligence to make sure we do not waste money on non-essential works at sites which will soon be vacated due to Crown or Supply Chain transformation;
c. Fire: This has been the highest risk area and priority. We identified 6,800 total fire risks during the statutory risk assessments completed in June. All actions are the responsibility of either PiCs, 3rd party landlords or CBRE as our contractors.
    - A total of 1,190 high fire risks were identified for PiCs and CBRE to resolve and 1167 (98%) have been closed out.
    - PiCs were assigned 1,024 high risk tasks and to date 1,009 have been closed and 15 remaining outstanding. The Crown and Supply Chain lead teams have worked with the Property Services & the H&S Team to impress this on all PiCs and make clear that closing all outstanding

POL00400101

actions is essential. We are confident that these will all have been addressed by early October and will keep up the pressure until this has happened.

- CBRE was assigned 166 high risk actions and have completed 158. The remaining 8 are work in progress due to lead times in ordering fire doors and will be completed in October.
- Landlord issues raised have been handed to BNP Paribas and correspondence has been issued to the landlord to address the FRAs.

2. Environmental
   a. In training of relevant staff on best practice in environmental issues, it became clear we can do better in terms of how we address environmental issues across the business. These include: waste, noise, water, energy use, carbon/climate change and fuel efficiency.
   b. Environmental breaches can carry significant criminal and civil penalties and it would benefit Post Office's reputation and comes at minimal cost. We have set up training and a new focus group, led by the Head of Health & Safety to look at six priority areas where we can improve. We will report back on progress on this before year end:
      - Environmental policy and reporting;
      - Site level environmental issue management;
      - Setting and reporting on energy targets;
      - Environmental impact assessments;
      - Supplier compliance to CSR and environmental targets; and
      - How clear, single point accountability is established at Director level.

3. Residential risk compliance

As reported on 14th July, Post Office currently has ten residential properties at five sites with seven of those residential properties being occupied. These represent an avoidable and unsustainable risk and we are systematically ceasing this activity as quickly as possible in line with our current duties to tenants.

In relation to remedial work required at premises that do not give rise to an immediate, and high, risk to health and safety, we will continue to manage those risks proportionately and in line with existing controls and measures. Notwithstanding our aim to cease being a residential landlord by year end, we will continue to undertake remedial work in the event of a new or increased serious risk emerging.

POL00400101

Our current portfolio (21 September 2016) consists of:

Site	No. Flats	No. Flats Occupied	Commentary
Gt Portland St	3	2	Site being sold, on completion all residential duties cease.
Harringay	2	1	Notice given on occupied unit for termination of lease on 14 October 2016.
Golders Green	2	2	Awaiting completion of works at one unit – once done both will be given termination of lease notice to end tenancy mid-Jan 2017.
Crouch End	2	2	One tenant on protected lease. Negotiating with landlord with a view to them taking back the units but with dilapidations agreement.
Leigh Park	1	0	Will not let out.
TOTAL	**10**	**7**	**All units to be vacant by March 2017**

What further matters have arisen since the last update in July?

While we have made significant progress since July, and our risk profile has trended from high to medium/low (taking in to account the small number of outstanding high fire risks) over the last 9 months, we still have a lot of work to do. There is a now a robust framework of assessment, remediation and assurance in place which gives us confidence.

This work is led by Property through close working with Health & Safety, all operational teams, Legal and others. We welcome the continued support and scrutiny from the ARC.

ARC input needed

We request the ARC note and endorse the current status of property compliance (medium to low) and the programme of future actions.