POL00423565

Risk and Compliance Committee Agenda

Date
Thursday, 5 May 2016

Start Time	Finish Time
13.00hrs	16.00hrs

Room
1.19 Wakefield, Finsbury Dials

Present	In Attendance	Apologies
• Jane MacLeod (Chair) • Paula Vennells • Neil Hayward • Nick Kennett • Alwen Lyons • Alisdair Cameron • David Hussey • Kevin Gilliland • Martin George	• Mike Morley-Fletcher • Garry Hooton • Adnan Killedar • John Scott (item 9) • Tom Moran (item 10) • Steve Norris (item 10)	

Agenda Item	Action Needed	ARC?	Purpose	Lead	Timing
GOVERNANCE					
1. RCC minutes and actions	Agree minutes Review actions		Agree minutes of last meeting and review actions	Chair	13:00 – 13:05
2. Review of effectiveness of RCC against TOR	Review paper and agree actions		Review the effectiveness of RCC against its Terms of Reference in 2015/16 and the actions identified	Chair	13.05 – 13.10
INTERNAL AUDIT					
3. Internal audit report	Review report consider appropriateness to go to ARC	✓	Update on progress of audit plan and findings of completed audits	Garry Hooton	13.10 – 13.30
RISK					
4. Risk report **(a) General control framework** **(b) Policy framework** **(c) Business continuity** **(d) Self-assessment** **(e) Risk report in ARA**	Review reports and approve actions; consider appropriateness to go to ARC	✓	Update on progress in implementing the central control framework, policy framework, business continuity management and self-assessment and the draft wording for the risk disclosure in the Annual Report and Accounts.	Mike Morley-Fletcher	13.30 – 14.00

CONFIDENTIAL

POL00423565

Agenda Item		Action Needed	Going to ARC?	Purpose	Lead	Timing
POLICIES						
5.	**Policies for approval**	Approve policies	✓	Approve six policies submitted as part of the Partner Banking Agreement and the revised whistleblowing policy.	Chair	14.00 – 14.10
				BREAK		
COMPLIANCE						
6.	**Financial Services deep dive**	Review appropriateness to go to ARC	✓	Response to ARC request for an explanation of Post Office's oversight of regulatory activity in branch and how issues are escalated.	Kevin Gilliland	14:20 – 14:45
7.	**Gifts and hospitality update**	Review paper and approve actions		Annual review of compliance with gifts and hospitality procedure in 2015/16.	Mike Morley-Fletcher	14:45 - 14:55
8.	**Whistleblowing update**	Review paper and approve actions		Annual review of operation of whistleblowing arrangements in 2015/16	Chair	14:55 – 15.05
9.	**AML update**	Review appropriateness to go to ARC	✓	Response to ARC action requiring a report on AML at every ARC meeting including a stakeholder plan.	John Scott	15:05 – 15:15
10.	**Property compliance update**	Review appropriateness to go to ARC	✓	Response to ARC action requiring update on property compliance to be circulated before next meeting	Steve Norris	15:15 – 15:30
NOTING PAPERS						
11.	**Update on approach to modern slavery**	Note paper	✓	Update on POL's approach to complying with new legislation about modern slavery	Chair	15:30 – 15:35
12.	**Horizon spotting**	Note paper		Update on risks spotted on horizon and reported at last meeting, and any new risks identified.	Chair	15:35 – 15:40
13.	**POMS RCC minutes**	Note minutes		Minutes of most recent POMS RCC	Nick Kennett	15:40 - 15:45
14.	**AOB**			Discuss AOB	Chair	15:45 – 16:00
	CLOSE					16.00

POL00423565

RCC 5 May 2016 Paper 1A

Post Office Ltd – Confidential

Risk and Compliance Committee (R&CC)		**Reference: R&CC March 16**
Date: 02 March 2016	**Venue: Boardroom, Finsbury Dials**	**Time: 13:00 – 16:00**
Attending:		
Jane MacLeod (JM)	General Counsel	Chair
Alistair Cameron (AC)	Chief Finance Officer	Member
Paula Vennells (PV)	Chief Executive Officer	Member
Neil Hayward (NH)	Group People Director	Member
Alwen Lyons (AL)	Company Secretary	Member
Nick Kennett (NK)	Financial Services Director	Member (mid-Item 2 onwards)
David Hussey (DH)	Transformation Director	Member
Kevin Gilliland (KG)	Network and Sales Director	Member (Items 1, 2, 8, 9)
Paul Brown (PB)	Head of Commercial Development	Representing Commercial Director
Tom Wechsler (TW)	Chief of Staff	Supporting CEO
Mike Morley-Fletcher	Head of Risk and Assurance	Report
Garry Hooton (GH)	Head of Internal Audit	Report
Adnan Killedar	Risk Business Partner	Observer
Georgina Blair	Risk Business Partner	Minutes
John Scott (JS)	Head of Security	Report (Items 1, 2, 8, 9)
Jenny Ellwood (JE)	Head of Transformation Risk & Assurance	Report (Item 5)
Julie George (JG)	Head of Information Security	Report (Item 7)
Peter Markey (PM)	Chief Marketing Officer	Report (Item 9)
Apologies:		
Martin George	Commercial Director	

The meeting began at 13.00

The Chair declared the committee quorate and opened the meeting.

JM noted that as well as the papers already marked as going to the ARC in the agenda, the AML risk update (item 8) and the paper on contract management (item 10) were also going to ARC.

JM explained that work is under way to align the pension investment reporting with the schedule of governance meetings. There would be no pension update presented at this meeting, but a pension report would be provided to the next Audit and Risk Committee (ARC) meeting, with the investment advisers present. This report would be circulated to the Committee to discuss by correspondence before the ARC meeting.

Agenda Item 1, RCC minutes and actions

The Committee agreed the minutes of the previous meeting and the attached actions.

JM confirmed that going forward all Group Executive (GE) members would be invited to RCC meetings.

Agenda Item 2, Internal audit report

GH explained the status of the audits on Appendix 1 and 2. The Committee discussed whether the 2015/16 audit plan had been over-ambitious. It was noted that the 2015/16 plan had been signed off by the ARC in March 2015.

Nick Kennett joined the meeting.

The Committee noted that there appeared to be a high number of partially completed and delayed audits in the plan for the current year. MMF explained that the plan had been designed so that

POL00423565

Post Office Ltd – Confidential

audits conducted in quarter 4 would be presented to the May ARC. The Committee queried whether this would give ARC too many reports to review, and it was clarified that only red rated reports go to ARC in full. Only the high rated actions from other reports get reported to ARC.

The Committee discussed the list of action points in Appendix 3. It was noted that some of the actions had been superseded by recent events and were not up to date. Certain GE members stated that the actions had not been escalated to them. The Committee discussed whether some of the action deadlines were overly optimistic and it was agreed that members would challenge unrealistic deadlines against action plans in the draft audit report. The Committee requested that a process be designed and implemented which allows agreed audit actions to be tracked and escalated to the appropriate GE member as necessary (**Action 1706**).

The Committee discussed how the audit actions would be presented to ARC, and it was requested that only overdue actions should be reported, however the methodology to do this was still being considered. It was noted that there was an ARC action requiring the reporting of high rated actions.

22 January 2016 POLARC 16/04 (a)	Internal Audit Update To include post audit assurance in the ARC report in relation to high rated actions.

[ARC action provided for information]

MMF suggested that a regular schedule of quarterly meetings be set up with each GE member. AC confirmed that he had found his first quarterly meeting useful but that he had not been presented with any overdue actions to review at the meeting.

Referring to Appendix 1, NK commented that the POMS audit shouldn't be on the list of work being completed for POL, as the POMS audit is being completed for the POMS ARC and any relevant findings will be reported by the POMS ARC to the POL ARC.

NK also queried why the FRES audit was listed in Appendix 1, as POL pays for Bank of Ireland (BoI) resource to audit FRES and receives reports via the FRES ARC, and it was unclear why POL was spending scare audit resource on FRES when the BoI resource could be used to provide assurance. JM pointed out that unlike POMS, where an appropriate governance structure has been worked out, the POL Board has no oversight of FRES. It was agreed that JM and NK would consider how POL GE and Board should ensure they have oversight of both FRES and POMS performance. (**Action 1707**)

The Committee discussed the 2016/17 audit plan and queried whether it was overambitious and whether the audits were prioritised against the top risks of the business. MMF explained that the top risks and current priorities had been discussed with individual GE members and their representatives in the course of drawing up the plan. It was agreed that it would be helpful to show which risks the proposed audits related to. GH also undertook to provide details of how long it was proposed each audit should take, to address the concerns about ability to complete the plan with the existing resources. (**Action 1708**)

The Committee requested that the "Top 10" audits be prioritised with other potential audits being listed as optional.

Agenda Item 8, AML risk update

JS summarised the main points from the AML risk update (paper 8) for the Committee. The Committee discussed the forthcoming HMRC Anti Money Laundering/Counter Terrorist Financing (AML/CTF) compliance audit, and asked for further detail on the likely cost of remedying the failure to register newly opened PO branches with HMRC; JS confirmed that this is currently being scoped. The Committee noted that the data comes from Network, the registration is paid for by Financial Services and the registration process is done by the AML team in Security, and it was unclear who would be responsible for any fines levied by HMRC.

POL00423565

Post Office Ltd – Confidential

The Committee discussed the AML/CFT compliance requirements required when providing cash delivery, collection and processing services for customers who are themselves Money Service Businesses (MSBs).

The Committee requested that the Promontory Report (an external review of POL's AML/CFT framework, concluded in Dec 2015) be circulated to Committee members to help them understand the work required to prepare for the HMRC audit. (**Action 1709**)

JM explained that steering group with representatives from affected parts of the business had been put together to scope the resources needed and that we would need specialist expertise. DH offered to provide project management resource.

Agenda Item 9, Customer vulnerability review

PM joined the meeting to present an update on recent work relating to customer vulnerability (paper 9). The Committee noted the difficulty in defining vulnerable customers, due to the transitory nature of some types of vulnerability, and the associated difficulty in defining appropriate processes and procedures.

The Committee agreed that customer vulnerability should be included as an aspect of a wider Customer Policy to be written by Commercial (**Action 1710a**, but that there should not be a separate policy specifically relating to vulnerable customers. The Committee requested that NK discuss the advantages and disadvantages of joining the British Bankers Association (BBA) Vulnerability Taskforce with PM before a further decision on this was made. (**Action 1710b**)

PM left the meeting.

Break

A ten minute break took place. KG and JS both left the meeting.

Agenda Item 3, Corporate Governance capability and ARA disclosure

MMF presented the paper on Corporate Governance capability and disclosure (paper 3). The Committee discussed the proposed wording for the corporate governance statement in our next Annual Report and Accounts (Conclusion 3 on p.2) and were supportive of the fact that the wording was now focused on the drivers for PO and was as straight forward and succinct as possible. As POL's accounts are closely scrutinised by some observers, this would make clear what we expected to be held to account for.

It was agreed that the option for reference to future changes was self-evident and so was not needed.

Agenda Item 4, Risk update

MMF presented the risk summary paper (paper 4).

MMF presented the Group Risk Profile update which now included suggestions from risk owners of their Key Further Actions (paper 4a). JM noted that the dates given for completion of key further actions (paper 4a, Appendix 2) were nearly all in the next few months, and asked the Committee to consider whether these were accurate or optimistic, or whether other medium or longer term actions were needed. The Committee agreed that currently the actions were in the main short term steps on the way to achieving the longer term desired risk outcome. The Committee noted that at this stage of the business's transformation there were many significant actions that were short term and that once these were completed longer term actions should become more apparent. The Committee agreed that only the key further actions for the red risks should be presented to the ARC, and requested that the red risks be recirculated to GE members for a further review of actions (to add any relevant medium or longer term actions) before the ARC paper is finalised. (**Action 1711**)

POL00423565

Post Office Ltd – Confidential

MMF presented the risk incident reporting paper (paper 4b). He explained that the purpose of reviewing reported risk incidents was to learn from their occurrence with regard to the appropriateness of our Top Risk, either their descriptions or their evaluation; it was not to discuss the management of specific incidents, which should be handled by respective risk owners. MMF drew the Committee's attention to Tables 2 and 3 in Appendix 1, which showed those incidents reported by business unit Risk Champions since the last RCC meeting mapped against the top risks. NH noted that instances of industrial action could be recorded against Top Risk 1 Industrial Relations as incidents. The Committee requested that the Central Risk Team work with business unit Risk Champions to help them identify other incidents that should be reported and match them to the Top Risks for lessons learnt. (**Action 1712**)

The Committee discussed the Health and Safety risk, noting that while this was currently well controlled it was of such importance that it should appear on the register of top risks. The Committee requested that MMF work with NH to add the Health and Safety risk to the Top Risks and complete a Risk Mitigation Plan. (**Action 1713**)

MMF presented the updates on the General Control Framework (paper 4c) and the Policy Framework (paper 4d). The Committee queried whether a whistleblowing report would be presented to the RCC and ARC and it was confirmed that this was on the agenda for May. The Committee also noted that the identification of policies and policy owners for non-Corporate Services policies (Phase 2 of the Key Policy Framework in Appendix 1) was purely for information and no action had been agreed. Once tools had been developed and lessons learnt from reviewing and remediating the Corporate Services policies, the extension to non-Corporate Services policies would be considered, assisted by benchmarking information on standard policy frameworks to be provided by Ernst & Young, and a proposal would be brought back to the RCC for discussion in May.

MMF presented the update on Business Continuity management (paper 4e). The Committee noted that dealing with business as usual (BAU) activity had taken up some project resource and that buffer in the project plan had been used up, but MMF confirmed that resource had been diverted within the Risk team to address this. Consideration will be given to rebasing the project plan.

MMF presented the paper on the Self-Assurance Regime (paper 4f), explaining the difference between the high-level Executives' Declaration and the more process specific Control Self-Assessment (currently planned solely for Finance Reporting controls). The Committee supported the proposal for both:

- The Committee agreed that an initial Executives' Declaration self-assessment exercise should take place at the end of March 2016 which should be used to identify gaps for a more evidential based dry run at the half year, in preparation for a full roll out at year end, with supporting evidence. (**Action 1714**)

- The further application of CSA at branch level was raised as a possibility for improving conformance with mails segregation requirements. The Committee requested that Mark Siviter, Head of Mails, and KG clarify what would be needed to prove conformance with the mails segregation requirements. (**Action 1715**)

Agenda Item 5, Business Transformation risk report

JE joined the meeting to present the Business Transformation risk report (paper 5). The Committee discussed cost estimation for longer projects. The Committee noted that Project Trinity had changed the risk profile of the business, and reference to this should be made in the ARC papers in the Group Risk Profile presented to the ARC. (**Action 1716)**

POL00423565

RCC 5 May 2016 Paper 1A

Post Office Ltd – Confidential

Agenda Item 7, Cyber Security paper
JG joined the meeting to take any questions on the paper on Cyber Security (paper 7). The Committee queried whether there had been a Distributed Denial of Service (DDOS) attack on the Post Office website in August 2015. JG confirmed that forensic investigation had found no evidence of a DDOS attack.
Agenda Item 10, Contract management
JM presented the paper on contract management (paper 10). The Committee agreed that the detail of the top 30 contracts (Appendix) would not be given to ARC.
Agenda Item 11, Horizon spotting report
JM presented the paper on horizon spotting (paper 11). The Committee agreed that this was very interesting and should be presented to ARC.
Agenda Item 12, Noting papers
JM referred the Committee to the two noting papers. The Committee had no comments.
Agenda Item 13, Any Other Business
No AOB was raised.
The meeting closed at 16.00

Next Meetings – 5 May 2016 Room 1.19 Wakefield 13.00 – 16.00
7 July 2016 Room 1.19 Wakefield 13.00 – 16.00

POL00423565

POL Risk and Compliance Committee
Action List
Status Report as at: 29/04/2016

MEETING DATE	AP REF	ACTION	Action Owner	Due Date	STATUS	Open/Closed
08/15/2015	1674	Provide a regular short update on Vulnerable Customer approach until this work is completed	Martin George	05/05/2016	Last update given at March RCC	Open
02/03/2016	1710a	Create Customer Policy which includes treatment of vulnerable customers	Martin George	tbc	Discussions in progress	Open
02/03/2016	1715	Ask Mark Siviter, Head of Mails, and Kevin Gilliland to clarify what would be needed in terms of controls self assessment to prove conformance with the mails segregation requirements.	Mike Morley-Fletcher	07/07/2016	Discussions in progress	Open
02/03/2016	1712	Central Risk Team to work with business unit Risk Champions to help them identify other incidents that should be reported and match them to the Top Risks for lessons learnt.	Mike Morley-Fletcher	07/07/2016	In progress - discussed in Risk Champions' Forum on 28/04/16	Open
02/03/2016	1707	Consider how POL GE and Board should ensure they have oversight of both FRES and POMS performance.	Jane MacLeod/ Nick Kennett	07/07/2016		Open
02/03/2016	1710b	Discuss the advantages and disadvantages of joining the British Bankers Association (BBA) Vulnerability Taskforce with Pete Markey before deciding whether to join.	Nick Kennett	05/05/2016	FS is currently co-ordinating with both POMS and BoI on addressing customer vulnerability issues. FS has existing working group arrangements in place with BoI to review vulnerability in respect of FCA's recent guidance on this issue. We currently don't anticipate joining the BBA taskforce as the benefits are unclear to PO but we will maintain a watching brief	Closed
02/03/2016	1716	Make reference to the effect of Project Trinity on the risk profile of the business in the Group Risk Profile presented to ARC.	Mike Morley-Fletcher	17/03/2016	Group risk profile updated for effect of Project Trinity before presentation to March ARC.	Closed
02/03/2016	1714	Initial Executives' Declaration self-assessment exercise to take place at the end of March 2016; outputs to be used to identify gaps for a more evidential based dry run at the half year.	Al Cameron/ Mike Morley-Fletcher	31/03/2016	Completed - see May RCC Paper 4d for details.	Closed

POL00423565

MEETING DATE	AP REF	ACTION	Action Owner	Due Date	STATUS	Open/Closed
02/03/2016	1713	Add the Health and Safety risk to the Top Risks and complete a Risk Mitigation Plan	Mike Morley-Fletcher/ Neil Hayward	17/03/2016	Heath and Safety risk was added to the Group Risk Profile presented to the March ARC and a Risk Mitigation Plan drawn up.	Closed
02/03/2016	1711	Recirculate red risks to GE members for a further review of actions (to add any relevant medium or longer term actions) before the ARC paper is finalised	Mike Morley-Fletcher	17/03/2016	Input from GE members gathered and included in group risk profile presented to March ARC.	Closed
02/03/2016	1709	Circulate Promontory Report (an external review of POL's AML/CFT framework, concluded in Dec 2015) to Committee members to help them understand the work required to prepare for the HMRC audit.	Jane MacLeod	05/05/2016	Executive Summary circulated to GE members on 26/04/16.	Closed
02/03/2016	1708	Provide details of how long each audit in the 2016/17 plan is expected to take to address the concerns about ability to complete the plan with the existing resources	Garry Hooton	17/03/2016	Incorporated in update on progress to plan - see May RCC agenda item 3 - Internal audit report.	Closed
02/03/2016	1706	Design and implement a process which allows agreed audit actions to be tracked and escalated to the appropriate GE member as necessary.	Garry Hooton	05/05/2016	Completed.	Closed
12/01/2016	1700b	MMF to investigate an appropriate rewording of GCF 3	Mike Morley-Fletcher	02/03/2016	Included in Paper 4c for March RCC.	Closed
12/01/2016	1700a	Update General Controls Framework based on RCC comments	Mike Morley-Fletcher	02/03/2016	Included in Paper 4c for March RCC and will be included as part of risk report in future meetings.	Closed
12/01/2016	1705	Review coverage of RCC against its Terms of Reference	Georgina Blair	05/05/2016	Completed - see May RCC agenda item 2 - Review of effectiveness of RCC.	Closed
12/01/2016	1704	RCC to review options regarding compliance with UK Corporate Governance Code and present them to the ARC.	Mike Morley-Fletcher	17/03/2016	Presented to March ARC.	Closed
12/01/2016	1703	Pensions update to be presented to the March RCC and ARC meetings and then quarterly going forward.	Harpreet Singh	17/03/2016	Update presented to March ARC & item added to standing agenda for future meetings.	Closed
12/01/2016	1702	Business continuity framework to be presented to the RCC	Mike Morley-Fletcher	02/03/2016	Included in Paper 4e for March RCC, and included as standing item in future meetings until project completed.	Closed
12/01/2016	1701	Update Policy framework based on RCC comments and present updated version to the RCC.	Mike Morley-Fletcher	02/03/2016	Included in Paper 4d for March RCC, and to be included as part of risk report in future meetings.	Closed
12/01/2016	1699	Review group risk profile and present updated profile to RCC	Mike Morley-Fletcher	02/03/2016	Included in Paper 4a for March RCC.	Closed

POL00423565

MEETING DATE	AP REF	ACTION	Action Owner	Due Date	STATUS	Open/Closed
12/01/2016	1698	Inform RCC on the sponsor/requestor of FRES audit. GH will discuss scope of the FRES review with NK directly.	Garry Hooton	02/03/2016	Done - see audit plan.	Closed
12/01/2016	1697	Implement improved audit report sign-off process with greater involvement of GE members	Garry Hooton	05/05/2016	Completed.	Closed
12/01/2016	1696	RCC to be provided with follow-up on implementation of audit recommendations	Garry Hooton	02/03/2016	Included in Paper 4a for March RCC and included as standing item in future meetings.	Closed
26/10/2015	1695	Work with risk report authors to improve risk report format	Mike Morley-Fletcher	02/03/2016	Done in preparation of papers for March RCC.	Closed
26/10/2015	1692	Include update from incident owner on current status in incident reporting table	Mike Morley-Fletcher	02/03/2016	Included in Paper 4b for March RCC/.	Closed
07/09/2015	1687	Clarify how POMS will assure itself that POL is complying with POM's compliance requirements	Susie Hayward	05/05/2016	Completed - see May RCC agenda item 6 - Financial Services Deep Dive.	Closed

POL00423565

2) Review of RCC Terms of Reference

Author: Georgina Blair Sponsor: Jane MacLeod Meeting date: 05 May 2016

Executive Summary

Context

In line with best practice and as recommended by the UK Code of Corporate Governance a clear Terms of Reference ('TOR') for the Risk and Compliance Committee ('RCC') should be in place and reviewed on an annual basis. This year's review was completed in April 2016.

Questions this paper addresses

1. Does the RCC have a clear and agreed TOR?
2. Has the Committee fulfilled the requirements of the TOR over the last year?
3. How will the Committee ensure it uses its time effectively in future and fulfils the requirements set out in its TOR?

Conclusion

1. The requirements specified by the current TOR (see Appendix 1) are clear and approved by the Group Executive (GE). The TOR will be updated before the next RCC (July).
2. The analysis carried out (see Appendix 2) confirms that the RCC has fulfilled the requirements of its TOR with the exception of receiving reports from three sub-committees.
3. The draft RCC timetable set out in Appendix 3 is a proposed forward agenda for RCC meetings which will ensure the RCC fulfils the requirements of its TOR in 2016/17.

Input Sought

The members of the RRC are asked to:

1. Confirm they believe they have fulfilled the requirements of the RCC TOR in 2015/16 as specified by the Group Executive.
2. Feedback to the Chair any comments on the proposed forward agenda for 2016/17.

POL00423565

The Report

1. The RCC is responsible for supporting the Group Executive (GE) in fulfilling their responsibilities in the effective oversight of risk management, internal control and compliance. It was decided in March 2016 that RCC membership should be extended to include all members of the Group Executive (GE). The TOR has not yet been updated to reflect this (see Appendix 1). The TOR will be updated for the changes made during 2015/16. This will be completed for the next RCC (July).

2. The areas of the TOR have be assessed against the Committee agendas, papers and decisions to ensure that the Committee has fulfilled its requirements to the Group Executive (see Appendix 2):
   a) The 'Purpose' of the Committee is clear and agreed by the Group Executive.
   b) The 'Meetings' have been convened in accordance with the TOR, although this review of the effectiveness of the Committee did not take place until after the year end (in April 2016).
   c) The 'Responsibilities' have been discharged, with the exception of:
      i) Review of risk reports from the Health and Safety Committee; instead this committee reports directly to the Board.
      ii) Review of risk reports from Commercial Committee and the Business Continuity Committee. The Commercial Committee doesn't report to RCC and the Business Continuity Committee doesn't currently exist.
      iii) No whistleblowing report was provided in 2015/16. One is being provided in May 2016.

3. Areas of specific risk have been reported throughout the year and key further actions agreed, for example cyber security and anti-money laundering in March.

4. The draft RCC timetable set out in Appendix 3 is a proposed forward agenda for RCC meetings which will ensure the RCC fulfils the requirements of its TOR in 2016/17. The scheduling of the various agenda items is yet to be finalised and will be aligned with the ARC timetable.

POL00423565

Appendix 1

RISK AND COMPLIANCE COMMITTEE
TERMS OF REFERENCE
(March 2015)

1. Overview

The purpose of the Risk & Compliance Committee (R&CC) is to support the Executive Team (ET) in fulfilling their responsibilities in the effective oversight of risk management, internal control and compliance.

2. Responsibilities

The responsibilities of the Risk & Compliance Committee include, but are not limited to:

- Reviewing the effectiveness of the risk management framework and risk policy and the oversight of the development and implementation of the risk management framework;
- Oversight of the current risk exposures of the business and advising on the future risk strategy;
- Oversight of the identification and effective management of current key risks and regular reviews of emerging risks;
- Oversight of the key operational risks facing the business including the effectiveness of internal controls;
- Monitoring the implementation of key recommendations and management action plans;
- Monitoring compliance with legal and regulatory obligations, including any significant breaches;
- Receiving and reviewing risk reports from the R&CC Sub-Committees:
  - Health & Safety
  - Commercial
  - Transformation

POL00423565

        - Information Security
        - Security
        - Business Continuity

    - Receiving and reviewing reports related to
        - Anti-Money Laundering
        - Bribery / Gifts & Hospitality
        - Whistleblowing
        - Internal Audit activity;

- Receiving and reviewing the draft annual internal audit plan for onward reporting to the Audit and Risk Committee (ARC);

- Receiving and reviewing of the draft annual risk management plan for onward reporting to the Audit and Risk Committee (ARC), and;

- Reviewing the adequacy of policy governance and recommending changes.

3. Authority

The Risk & Compliance Committee is authorised to:

- Seek any information it requires from anyone in the organisation in order to perform its duties including calling anyone to the meeting to be questioned as required; and

- Obtain outside legal or other professional advice on any matter within its terms of reference.

4. Meetings

- The R&CC shall meet at least six times a year and otherwise as required;

- The quorum shall be two members which will be deemed competent to exercise all or any of the authorities and powers vested in or exercisable by the committee;

- The committee will arrange for an annual review of its own performance to ensure it is operating effectively and recommend any changes it considers necessary to ET for approval; and

POL00423565

- The committee will ensure its terms of reference and membership are reviewed on an annual basis and updated as required

5. Reporting

- The committee shall report to Executive Team on its proceedings on all matters within its purpose and responsibilities highlighting significant risk and compliance matters for their attention;

- The committee shall report to the Board and Audit, Risk and Compliance Committee as requested; and

- The committee shall input to the Post Office annual reporting as appropriate.

6. Membership

Members	
General Counsel (Chair)	Jane MacLeod
Chief Executive Officer	Paula Vennells
Chief Finance Officer	Alisdair Cameron
Group People Director	Neil Hayward
Financial Services Director	Nick Kennett
Company Secretary	Alwen Lyons
Other attendees	
Head of Risk & Assurance	Arnout van der Veer
Head of Internal Audit	Garry Hooton
Chief of Staff	Gavin Lambert
Secretariat	Georgina Blair

POL00423565

Appendix 2

Analysis of performance of RCC against requirements

Verbatim Extracts from TOR		Meeting Dates					
Responsibilities -		**May-15**	**Aug-15**	**Sep-15**	**Oct-15**	**Jan-15**	**Mar-16**
Reviewing the effectiveness of the risk management framework and risk policy and the oversight of the development and implementation of the risk management framework	✓	Approved principles of RM and implementation plan and reviewed effectiveness of risk and internal controls framework	Received update on BCP & incident management process	Reviewed interim incident management process	Received update on risk framework implementation timetable	Received update on general control framework	Received update on general control framework and self-assurance regime
Oversight of the current risk exposures of the business and advising on the future risk strategy	✓	Reviewed principal risks	Reviewed group risk profile	Reviewed group risk profile		Reviewed group risk profile	Reviewed group risk profile
Oversight of the identification and effective management of current key risks and regular reviews of emerging risks	✓		As part of review of updated group risk profile	As part of review of updated group risk profile		As part of review of updated group risk profile	
Oversight of the key operational risks facing the business including the effectiveness of internal controls	✓		As part of review of group risk profile	As part of review of group risk profile		As part of review of group risk profile	As part of review of group risk profile
Monitoring the implementation of key recommendations and management action plans	✓						Reviewed key further actions for red risks in group risk profile

POL00423565

		May-15	Aug-15	Sep-15	Oct-15	Jan-15	Mar-16
Receiving and reviewing risk reports from the R&CC Sub-Committees:							
Health & Safety	X						
Commercial	X						
Transformation	✓				✓	✓	✓
Information Security	✓				Annual deep dive on risk profile		Cyber security update
Security	✓				Annual deep dive on risk profile		AML update
Business Continuity	X						
Receiving and reviewing reports related to							
Anti-Money Laundering	✓		AML annual report				AML risk update
Bribery/ Gifts & Hospitality	✓	G&H annual report					
Whistleblowing	X						
Internal Audit activity							
Receiving and reviewing the draft annual internal audit plan for onward reporting to the Audit and Risk Committee (ARC)	✓						Reviewed 2016/17 Internal Audit plan
Receiving and reviewing of the draft annual risk management plan for onward reporting to the Audit and Risk Committee (ARC)	✓				Reviewed plan to March 2017 (presented to ARC in September)		
Reviewing the adequacy of policy governance and recommending changes	✓	Reviewed policy approvals process			Reviewed approach to POL-wide policy framework	Received update on implementation of policy framework	Received update on implementation of policy framework

POL00423565

Appendix 3

RCC Forward planner – proposed topics (assuming 6 meetings per year) – scheduling to be confirmed

Items		Proposed				
	1) Jan	2) Mar	3) May	4) July	5) Sep	6) Nov
1. Standing Agenda Items						
• Minutes and actions from previous RRC meetings	√	√	√	√	√	√
• Minutes from POMS RCC meetings	√	√	√	√	√	√
2. Governance Items						
• Review of RCC Terms of Reference		√				
• RCC effectiveness against ToR self-assessment		√				
3. Risk Management, Internal Control and Assurance						
• Group Risk Profile		√			√	
• Key Further Actions & Risk Incidents	√	√		√	√	
• Internal Audit update	√	√	√	√	√	√
• Internal Audit – approval of the upcoming plan		√				
• Business Continuity – approval of annual plan		√				
4. Financial Reporting and Disclosure						
• Risk disclosures for annual report and accounts			√		√	
• Board Annual Assessment (including Executives Declaration, Key Policies and Control Self Assessment)			√			
• Corporate Governance Statements			√			
5. Compliance						
• Regulation						
▪ Anti Money Laundering	√	√	√		√	√
▪ Anti Bribery & Corruption	√					
▪ Competition Law	√					
▪ Data Protection	√					
• Conduct/ People						
▪ Customers (e.g. Vulnerable, Conduct issues)		√				

POL00423565

Items		Proposed				
	1) Jan	2) Mar	3) May	4) July	5) Sep	6) Nov
▪ Ethics and Code of Conduct		√				
▪ Fraud and Theft		√				
▪ Whistleblowing		√				
6. **Deep Dives**						
▪ FS Deep Dives on specific issues	√		√			
▪ Pensions		√			√	
▪ Health and Safety					√	
▪ Incident Management, Disaster Recovery & Crisis Management					√	
▪ Transformation Risk	√				√	
▪ Cyber / IT Security					√	

POL00423565

3) Internal Audit Report

Author: Garry Hooton Meeting date: 05 May 16

Executive Summary

Context

The purpose of this paper is to update the Committee on the PO Internal Audit and Business Transformation Assurance activity and key outcomes. This includes details of the work completed since the last Risk and Compliance Committee (RCC) in March and the closing out of the 2015/16 Internal Audit Plan. We have agreed the plan for 2016/17 with ARC and have commenced work on Q1 reviews.

Questions this paper addresses

1. What progress has been made since the March meeting?
2. Is the Internal Audit Plan on track for completion of 2015/16 audit activities?
3. Do we have the resources we need to deliver the plan and actions arising going forwards?
4. Have any significant issues arisen that the committee should be aware of?

Conclusion

1. During the period seven audits, four Internal Audit and three Business Transformation Assurance (BTA); have been completed, with actions agreed with management. These have been finalised with GE Sponsors and five others (three IA and two BTA) are nearing completion. We have been working closely with GE sponsors to remediate overdue audit actions and have made very good progress. The team have also continued to contribute in a business assistance capacity to the Property Compliance Forum, we will cease this in 2016/17. Work on the 2016/17 plan has commenced. Work has continued on the General Controls Framework, Executives' Declaration processes and developing our Controls Self-Assessment capability (subject of separate papers). BTA replanning will take place following the upcoming second series of boot camps.
2. The audits remaining for 2015/16 are now either completed, closed or going through final clearance with senior management. The completion of the Agents Remuneration audit has been significantly delayed by the "Agents pay" issue, work will resume once the business has completed recovery work. (see **Appendix 1, "Audit Plan Status"**). We are working on a paper that identifies the themes from the audits for presentation to the July RCC.

POL00423565

3. We remain one team member short as we continue to seek appropriate temporary maternity cover for the IT audit manager role. Another team member who has been on long term sick leave has returned to the business, full time as of 2nd May 2016.
4. There are no significant issues that we believe the committee should be made aware of.

Input Sought

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

The Report

Reviews in Progress

5. The following reviews are in progress:

Activity	In Progress
Internal Audit	2015/16 • Data Protection • Common Digital Platform • Agent Remuneration 2016/17 • Identity and Access Management • IT and Operations Governance and IT Risk Management • FS Training and Competence Schemes
BTA	• Communications and Stakeholder Management • Digital Programme Mobilisation • Winning with retailers • Target Operating Model • Separation PIR • Planning Boot Camps

POL00423565

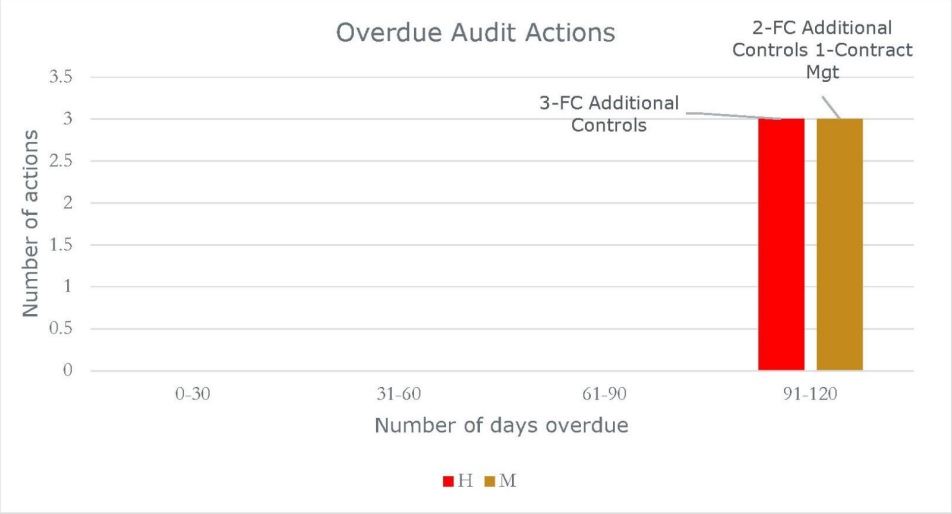
Completed Reviews

6. Four reviews have been completed and are summarised below.

(Detailed summaries to follow for SISD, Treasury Operational Risk Review, Social Media and Critical Metrics Management – pending final GE clearance prior to RCC)

Updates on Internal Audit Overdue Actions

7. We have developed an Overdue Actions monitoring process to ensure clarity of requirements and responsibilities – this involves providing monthly summaries to GE Sponsors and has already shown benefits in assisting them in the tracking and closure of overdue audit actions.
   Since the March meeting, where 32 overdue actions were reported, significant progress has been made by the business. At the end of April, 26 actions have been completed and validated. 6 remain outstanding, but clear work plans are in place to ensure they are closed in the near future.



Business Assistance

8. Internal Audit has continued to work with Legal to assist Property with the implementation of adequate governance and controls to address regulatory compliance requirements. We have also continued to attend the Property Compliance Forum to monitor progress. We are seeking to bring this long term time commitment to an end once we are sure remediation is in place.

9. A formal plan is now in place to address all of the required statutory compliance checks/risks assessments for the elements and sites. A workshop between Property, Health and Safety and Network Operating team is planned for 25th May to co-ordinate

POL00423565

the monitoring control activities of the different teams improving the delivery of effective compliance.

10. Two residential properties (out of the 8 reported last time) are still not compliant as the visits could not be arranged with the tenants by the Facility and Estate management suppliers. The Property Compliance Board has been assured that the two remaining properties will be visited and serviced by 10th May.

11. Electrical testing programme: 91% of all the premises classified as "not satisfactory" have been visited again and any issues fixed. The remaining sites will be visited by the end of May.

12. The Head of Property is bringing an update paper to this meeting prior to sending it to the ARC members as requested at the March ARC.

Resourcing

13. The team has a headcount of 4 with approximately 150 days of Co Sourced resource from PwC for specialised audit work. During the year we have been without one member of the team for a total of 5 months due to long term sickness. In addition we have been recruiting for temporary maternity cover since February and have yet to secure suitable resource. If this situation continues we will consider alternative options for resourcing some of the audits.

Business Transformation Assurance

14. Since the March meeting the BTA team have completed three reviews, with two more due to finalise shortly. 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. The executive summaries are at **Appendix 3.**

15. In this quarter BTA has started following up on observations from earlier reviews. 32 issues have been closed on time. To date there has been a very good engagement with the business and no observations have been remediated late.

16. There have been some underlying changes to the Transformation portfolio, namely the removal of the Financial Services and Commercial projects into a 'non-transformation' change portfolio as well as material changes to some of the individual programmes within Transformation. As such Transformation is running a second series of boot camps in May to revise the integrated transformation plan. Once the revised plan is published, BTA will revise the assurance plan for the rest of this year and ensure alignment with the main Transformation plan.

POL00423565

17. A full summary is included at **Appendix 2,** ("BTA Progress to plan") with report summaries at **Appendix 3.**

POL00423565

Appendix 1 2015/16 Audit Plan Status – May 2016

Activity				Actions			Reporting		
Audit	GE	Status	Report Rating	High	Medium	Low	RCC	ARC	Comments
Completed Reviews									
Contract Management	Al	Issued		4	11	1	Sep 15	Sep 15	Closed out
Financial Crime	Jane	Issued		18	20	2	Sep 15	Sep 15	Closed out
FS Conduct Risk	Nick	Issued		13	-	-	Oct 15	Nov 15	Closed out
Drop and Go	Martin	Issued		2	3	-	Oct 15	Nov 15	Closed out
Wave	Martin	Issued		1	13	8	Oct 15	Nov 15	Closed out
Fujitsu Exit	Al	Issued		-	2	5	Jan 16	Jan 16	Subsequently superseded by the re-engagement of Fujitsu on the Front Office Project
Critical Metric Management	Al	Issued		3	1	1	May 16	May 16	At GE Close out
SISD Delivery	Al	Issued		7	2	-	May 16	May 16	At GE Close out
Social Media	Martin	Issued		-	5	-	May 16	May 16	At GE Close out
Treasury Operational Risk	Al	Issued		6	8	-	May 16	May 16	At GE Close out
POMS Governance Follow up	Nick	Issued		N/A	N/A	N/A	May 16	May 16	Completed

POL00423565

Appendix 1 2015/16 Audit Plan Status – May 2016 Page 7 of 15

Activity				Reporting		
Audit	GE Owner	Timing	Status	Due RCC	Due ARC	Comments
Reviews in progress						
Towers Delivery	Al	On-going (with BTA input)				
Workforce Planning	Neil	Q3	Not Done	-	-	Not resourced due to long term sickness
Data Protection	Al	Q4	Fieldwork	July 16	Sept 16	In progress (Co Source)
Common Digital Platform	Martin	Q4	Fieldwork	July 16	Sept 16	In clearance
Agent Remuneration	Kevin G	Q4	Fieldwork	July 16	Sept 16	Delayed, expected to resume soon

POL00423565

Appendix 2 BTA Plan Status – May 2016 Page 8 of 15

Activity				Actions			Reporting		
Assurance	**Timing**	**Status**	**Report Rating**	**High**	**Medium**	**Low**	**Due to RCC**	**Due to ARC**	**Comments**
Completed Reviews									
EUC Review	Q3	Final Report	N/A	-	-	-	Oct 15	Nov 15	Requested by TESG.
Portfolio Management Design Review	Q3	Final Report	N/A	-	-	11	Jan 16	Jan 16	Jointly resourced by IA / BTA.
Planning boot camps	Q3	Highlight Report	N/A	N/A	N/A	N/A	-	-	Highlight report to management only to inform planning review
From the end of Q3 onwards all reports will be rated – consistent with BAU Audit reporting									
Design of New Benefits Framework	Q3/4	Final Report	Adverse	3	4	1	Mar 16	Mar 16	Final Report Issued
Separation	Q3/4	Final Report	Adverse	6	1	-	Mar 16	Mar 16	Final Report Issued
Cross Towers Governance Structure and Programme Assurance Authority	Q3/4	Draft Highlight Report	Unrated as highlight report	N/A	N/A	N/A	May 16	May 16	Final Highlight Report Issued
End to end financial management of Transformation	Q4	Final Report	Average	1	8	**5**	May 16	May 16	Final Report Issued
Portfolio management OE #1	Q4	Final Report	Satisfactory	-	1	**2**	May 16	May 16	Final Report Issued

POL00423565

Appendix 2 BTA Plan Status – May 2016 Page 9 of 15

Activity			Reporting		
Assurance	Timing	Status	Due to RCC	Due to ARC	Comments
Reviews in progress / planned (All reports below this line will be rated against agreed criteria)					
Digital Programme Mobilisation	Q4	Draft Report	July 16	Sept 16	Draft report issued to management
Communications & Stakeholder management	Q4	Draft Report	July 16	Sept 16	Report with management for comment
Winning with Retailers PIR	Q4	Fieldwork	July 16	Sept 16	Fieldwork in progress
Target Operating Model	Q4	Fieldwork	July 16	Sept 16	Fieldwork in progress
POCA	-	Cancelled	-	-	No longer part of Transformation
Separation PIR	Q1	Fieldwork	July 16	Sept 16	Fieldwork in progress
Planning Boot Camps	Q1	WIP			Due to commence w/c 2/5/16

POL00423565

BTA – Completed Report Summaries Appendix 3

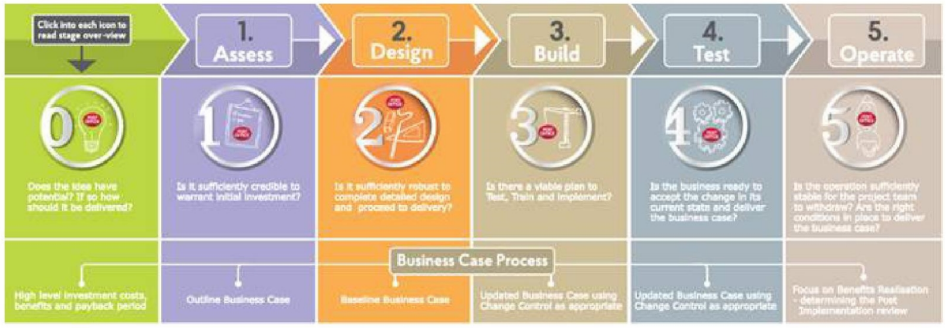
End-to-End portfolio financial management

The end-to-end financial management review undertook an assessment of the portfolio's:

Financial governance;
Budgeting and forecasting;
Quantification of financial benefits; and
Internal financial reporting.

The six gate approvals process that all business cases must pass through is summarised at Figure 1. The approvals process in place that all projects must follow to obtain funding appears to be robust and is consistent with examples of good practice seen elsewhere.

Figure 1: Approval Process Gates



Financial governance. Despite the approval process being in place, the five business cases that were reviewed during the fieldwork all contained a number of issues where they were non-compliant with policies in place on the completion of business cases, although there is recent evidence of TFCG rejecting and deferring business cases which they deem not to be of a standard that warrants approval. This is a positive step by TFCG as there is a risk associated with approving the funding for projects that are not yet mature enough to demonstrate a compelling case and could result in misdirected investment. TFCG should continue to reject business cases that do not provide a compelling case for investment or are not completed correctly. Although this is likely to have a positive impact on the quality of business cases submitted in the future, it does not tackle the problem at source. A matrix of the quality issues identified in each business case is at Appendix 2.

Seven of the thirteen proposed recommendations from this review relate to the quality of the submitted business cases. A checklist of common failings in the business cases should be circulated to portfolio leads instructing them to focus on these elements in all new business cases before submission for approval.

Budgeting and forecasting. The portfolio follows POL's standard budgeting process, with the budgets for all projects allocated to a specific theme within the portfolio itself. The budgeting process was robust and there was evidence demonstrating that the programme ensures that the requests for funding are matched to the budget available. The individual portfolios and the projects follow POL's forecasting process of submitting formal forecasts every quarter. Individual projects re-forecast monthly and provide these updates to the portfolio's central finance team for inclusion in the finance MI pack to ensure the latest financial position is available to management.

Quantification of benefits. A recent review on the portfolio's benefits framework was undertaken and reported on separately. This review focused on analysing the process adopted by project teams

POL00423565

on valuing the financial benefits included in the business case. There were no issues identified with the methodology adopted to value the benefits in the five business cases analysed during this review, although there was no evidence of any independent financial review being undertaken which is related to a recommendation made for all financial elements of the business case.

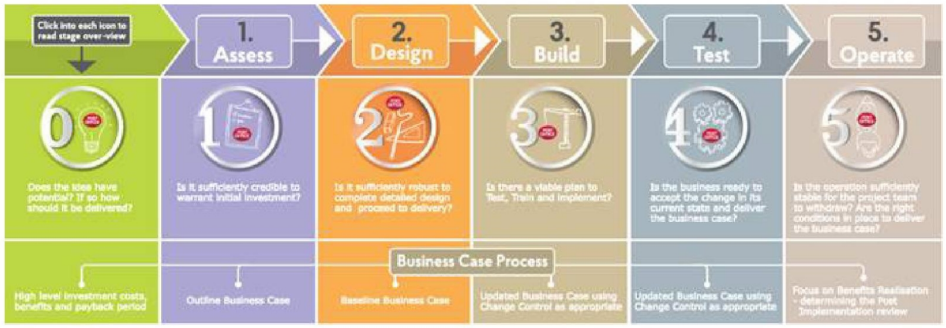
Financial reporting. The internal reporting of budgets, forecasts and actual expenditure is based on data held within POL's finance system. As the system does not hold specific data fields that the financial values need to be reported against, most of the report preparation is performed in an offline MS Excel spreadsheet. This approach is inherently risky due to it being manual and onerous; recommendations have been made to incorporate the financial reporting into the finance system.

POL00423565

Portfolio Management Operational Effectiveness

Since BTA's last review management has designed and implemented a number of improvements into how the Transformation Portfolio is governed and controlled. One of the key aspects implemented by management since the last review is the 'One Best Way' framework. This is a standard change framework which includes approval gateways enabling management to control POL's financial and risk exposure (see Figure 1). In support of this implementation the Change Director for Business Transformation has introduced training on the framework as well as compliance monitoring of project documentation for both completeness and quality.

Figure 1: One Best Way Approval Process Gates



From the Portfolio Governance, Management and Change Methodology review dated 05 October 2015, 11 issues were identified, of which four were in scope for this review. Two are now considered to be operating effectively, two have been partially implemented and the rest will either be followed up as part of other reviews or remediation is not yet complete. A summary is below:

Initial Finding*	Follow up status	Reference
ToR and Meeting Agenda alignment	Closed / Implemented	
Programme Managers (PM) forum	Closed / Implemented	
Portfolio Management Methodology	Partially Implemented	Issue 1 (moderate)
Portfolio roles and responsibilities	Partially Implemented	Issue 2 (minor)
Agile projects / programmes change methodology	Not assessed as remediation still underway	
Portfolio Status Reporting / Single View		
Dependency management		
Communication and Stakeholder Engagement Planning	Not assessed as being followed up as part of another review	
Benefits management framework		
Delegation of authority		
Completion of Target Operating Model (TOM) Design		

***BTA Portfolio governance, management and change methodology design review**

POL00423565

Overall, since the first BTA review the portfolio management governance and processes have been significantly improved. A number of the previous findings and the associated actions have been implemented. However, further work is required to close out all of the findings from the first review and, in addition, the findings from this review. This report has identified a total of three findings, where one is moderate and two are minor; of which one finding was self-identified by management. The moderate finding relates to Portfolio Management Methodology - portfolio prioritisation criteria and process, which is yet to be fully remediated from the previous review and is summarised below:

- **Portfolio prioritisation.** Projects within the portfolio are broadly categorised as Regulatory, In-Flight or New. This categorisation does not determine a priority and therefore does not inform how or when it will be initiated. We note there are no formal prioritisation standards to manage the transformation portfolio on a continuous basis. Project approval is given via committee at the TDA and TFCG as a means to approve individual projects based on their business case, rather than reflecting the overall priority of the project and contribution to the programme. It is recommended that a set of objective prioritisation criteria is designed and implemented.

Based on the work performed, as stated in the Scope and methodology sections, we have given our review of the Portfolio Operating Effectiveness within POL a **Satisfactory (with exceptions)** risk rating. A **Satisfactory (with exceptions)** report rating is defined as:

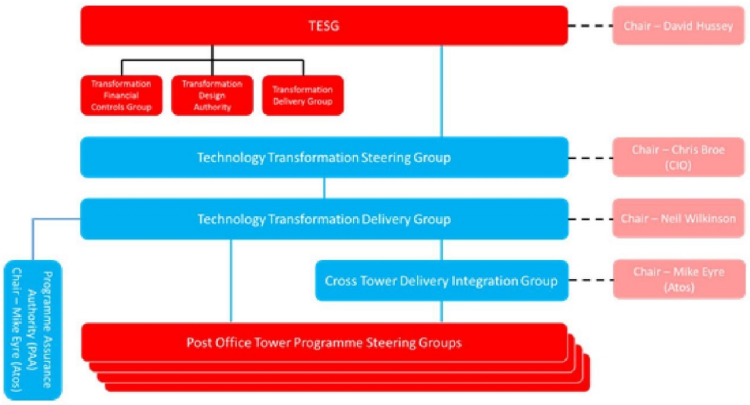
Overall control environment is sound in almost every operational aspect. However, a low level number of minor non-compliance with internal and external requirements, and weaknesses in records, systems and controls were identified. Examples may include: only minor or process improvement findings.

POL00423565

Cross Tower Governance and Programme Assurance Authority

Background

In June 2015, Post Office deployed a revised IT governance structure to clarify the respective roles and responsibilities of POL and Atos, where POL is accountable for the overall Technology Transformation Programme and Atos, as the Service Integration (SI) supplier, is responsible for providing oversight of the activities performed by third parties delivering IT tower services. The diagram below illustrates the IT governance structure and its relationship to the overall transformation governance, where blue represents the scope of this review. The text that follows provides a brief summary of the purpose for each element of the IT governance structure as stated in the terms of reference for each.



Technology Transformation Steering Group (TTSG): The purpose of this Group is to support and provide advice to the Sponsor (CIO) to realise the programme benefits, deliver the programme within the approved business case, align the programme with organisational strategy and other programmes, as well as identify and manage significant risks. The Group is intended to meet at least monthly, with twice monthly reports to the TESG.

Technology Transformation Delivery Group (TTDG): The purpose of this Group is to provide oversight and leadership to the Technology Transformation programmes, be the most senior operational decision making forum and point of escalation for the "*POL Tower SRO*", manage the Technology Transformation budget, and escalate issues and risks that require decisions or support from TTSG. The Group is intended to meet bi-weekly and report to TTSG.

Programme Assurance Authority (PAA): The purpose of this Group is to provide assurance to POL of the service integrator and service desk (SISD) tower implementation activities, evidenced through assurance controls and reviews. The PAA is thus accountable for ensuring Atos-delivered activities (as well as the tower services delivered by third parties) are in line with POL contracted services, technology, architecture, commercial/financial and information security terms. The PAA is chaired by the Atos Implementation Director, who for this specific forum acts as a POL facilitator to the POL assurance leads. The Group is intended to meet weekly and report to TTDG.

POL00423565

Cross Tower Delivery Integration Group (CTDIG): The purpose of this Group is to provide leadership and oversight to each tower programme, ensure cross tower delivery / architecture / service deliverables are defined and produced, manage the Cross Tower RAID, resolve cross tower delivery conflicts, and ensure effective cross tower test planning and acceptance. The Group is intended to meet weekly and report to TTDG.

Post Office Tower Programme Steering Groups: When implemented in June 2015, this governance structure involved the creation of new POL Programme Manager roles to provide the business with clearer accountability for solution delivery, as well as to help manage some of the issues linked to POL obligations management. The POL Programme Managers each lead their tower's Programme Steering Group and attend both CTDIG and TTDG, along with the any wider business transformation governance as required. Note: the scope of our review has not included the operation of these Steering Groups, only the relationship between them and the other parts of the IT governance.

Overall conclusions

As management has already identified, the current governance structure is not operating effectively. Based on our review, we understand the underlying reasons for this include:

- Lack of clear accountabilities and roles at each level of governance that is aligned to the needs of both the technology transformation and business transformation programmes.
- Conflict in Atos' role and insufficient segregation of duties for assuring SISD and cross tower implementation activities.
- Uncoordinated and incomplete management of all contractual obligations – including of SISD role and across towers.

POL00423565

4) Risk & Control Report

Author: Mike Morley-Fletcher

Meeting date: 5 May 2016

Executive Summary

Context

This paper updates the RCC on progress against the project plan for developing POL's Risk Framework, in particular how we have been developing POL's Group Risk Profile, Internal Control Environment, Assurance mechanisms and Corporate Governance capability. Please note, our Risk Profile is NOT reviewed at this RCC as it is covered at the other four meetings.

Questions

1. Is implementation of the Risk Framework on target?
2. What has been the primary focus?
3. What else has been progressed?

Conclusion

1. The plan is mostly on schedule (see appendix 1), despite some resource shortages (through illnesses and recruitment holds). However, we have had to reschedule developing the Route Map to Corporate Governance Compliance until September. This will map out our plan over the next 2 to 3 years. Many of our initiatives will contribute to greater compliance and so it was felt that formalisation of the plan could wait until the next RCC/ ARC. A summary of Work Done since the March ARC and Next Steps is included in appendix 2.

2. This period has been primarily focused on developing our risk, control and assurance disclosure statements for our stakeholders in the Annual Report. We have used our revised position on corporate governance compliance to guide the content and extent of our disclosures, but also compared these with other relevant organisation's reports and discussed them with our external auditors.

3. We have also progressed our work on improving our Internal Control Environment (e.g. dry running/ testing our Internal Control Framework, competing the review and remediation of our Corporate Services key policies, continuing to enhance our Business Continuity capability) and our Assurance Mechanisms (e.g. completing our first Executives' Declaration and starting the control self-assessment of our Financial Reporting controls) – see attached papers.

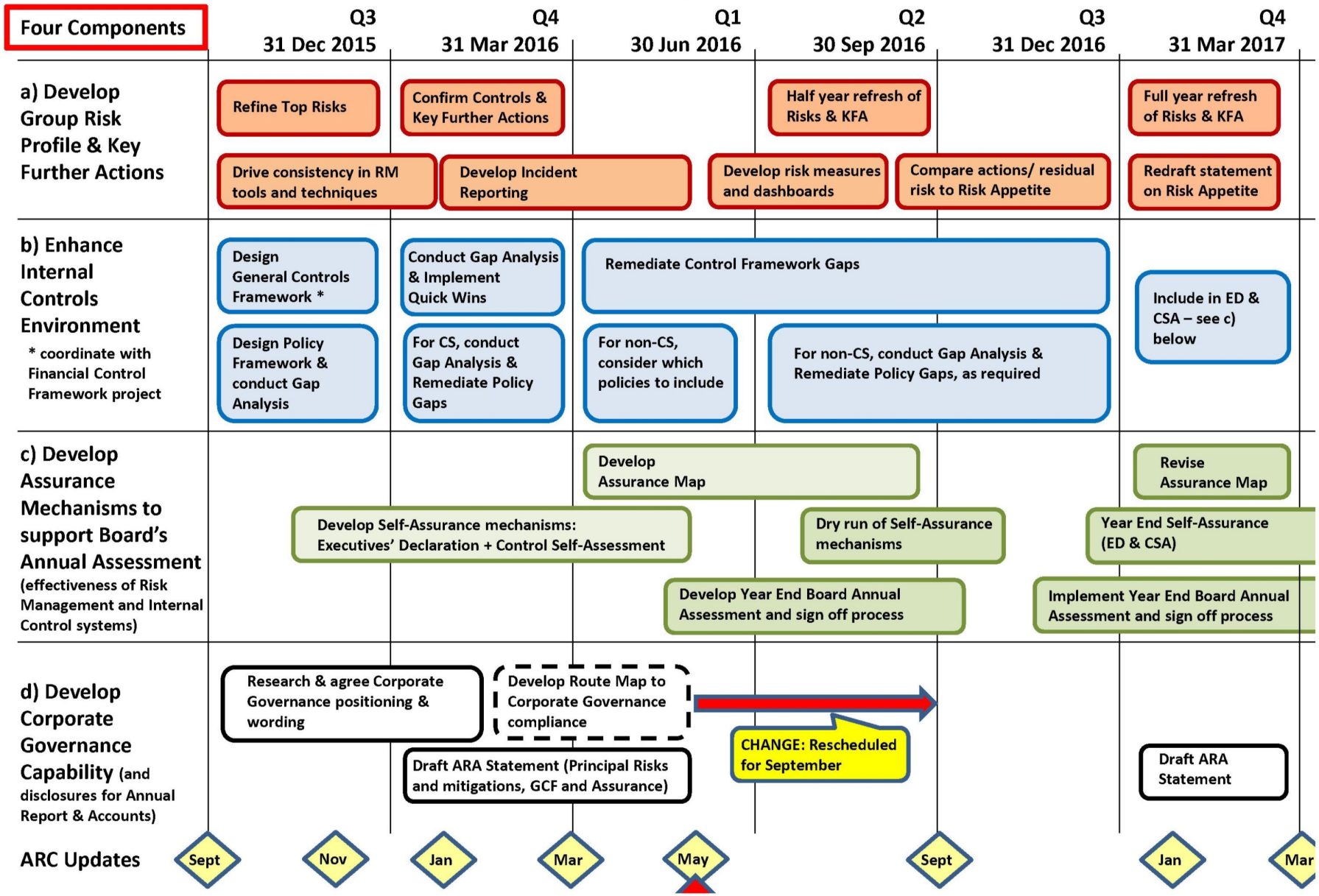
Input Sought

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

POL00423565

Appendix 1: Risk Framework - Project Plan

Version: 25th April 2016



POL00423565

Appendix 2 –Risk and Control Framework: Summary of Work Done and Next Steps

We have completed all key and time-critical components against the four main components of the plan (see Appendix B for a copy of the updated plan). Some of the main achievements have been, and next steps:

Work Done	Next Steps
a) Risk Profile and Actions – no paper provided	
Group Risk Profile: • Details are **NOT** reviewed at this RCC/ ARC. • Drafted Principal Risk and Mitigations for disclosure in Annual Report, per d) below. • Provided information on the Top Risks and Key Further Actions to the Strategy Team for consideration in the Business and Strategy planning process for 2016/ 17.	• Risk owners will review Principal Risks and Key Further Actions for reporting to September RCC/ ARC.
b) Internal Controls Environment	
bi) General Controls Framework (GCF) – see paper 4a): • Reviewed the General Control elements of the Financial Controls Framework project to confirm the design of our GCF, assess its current state, ensure any appropriate remediations have been identified and prepare templates for our subsequent Self-Assessment exercise. • Details of our General Controls have been included in this year's Annual Report in the risk note. • Started to embed risk and control accountabilities into GE objectives (or job profiles)	• Conduct dry run at half year 2016/ 17 and full roll out at year end (to help the Board complete its year-end Annual Assessment of Internal Controls for 2016/ 17). • Ensure risk and control accountabilities are reflected in GE objectives/ or job profiles (June)

POL00423565

Work Done	Next Steps
bii) Policy Framework (key policies) – see paper 4b): • Completed remediation of all Corporate Services policies. • Used EY's benchmarking to develop a list of non-Corporate Services key policies.	• Consider implementation needs of CS policies, ensuring pragmatic and co-ordinated. • Formalise monitoring mechanism to ensure we can evidence compliance with policies. • Complete a current state assessment of non-Corporate Services key policies to steer which polices need remediating and identify any implementation and monitoring needs.
biii) Business Continuity – see paper 4c): • Major Incident Management processes introduced, in conjunction with Crisis Management Team Construct • Initiation of Business Impact Assessments across business units, with aim to develop and test continuity planning.	• Complete phase 1: - Business Protection Team Training & Invocation Test - CMT Exercise • Continue phase 2: - BC Programme Management Structure Development.
c) Assurance Mechanisms (& assessment of effectiveness of Risk Management and Internal Control systems) – see paper 4d)	
• To provide assurance to Management and the Board (via the ARC): 1. Completed a dry run/ test of the Executives' Declaration return, completed by the General Executive (GE), and 2. Implemented Control Self-Assessment (CSA) techniques for the General Control Framework and Financial Reporting processes.	• Use any lessons learnt to improve self-assessment at half year 2016/ 17 • Conduct full roll out at year end 2016/ 17 (to help the Board complete its year-end Annual Assessment of Internal Controls for 2016/ 17).
d) Corporate Governance Capability (& disclosure in the Annual Report & Accounts) – see paper 4e)	
• For this year's disclosures, we reviewed previous declarations and enhanced the risk information in the Strategic Report (our approach to risk, our Internal Control Framework and more details on our principal risks) as well	• Ernst & Young have provided a review of our compliance gaps, which the Central Risk team will analyse to develop a route map to compliance (over the next 2 or 3 years). This will enable RCC and ARC to determine if this is appropriate for our needs and practical.

POL00423565

as in the Governance section (description of internal audit's approach and audits, plus how the Board conducts their assessment of the risk management framework and systems of internal control), in discussion with our external auditors. • In particular, following RCC and ARC suggestion, compliance with the UK Corporate Governance Code is not sought at present and our compliance statement is now, *"PO maintains standards of corporate governance appropriate for our ownership structure, our commitment to our social purpose and our strategy for commercial sustainability"*.	• This was originally estimated for presentation in May, but has been rescheduled to September.

POL00423565

4a) General Control Framework

Author: Deana Herley Sponsor: Mike Morley-Fletcher Meeting date: 5 May 2016

Executive Summary

Context

This paper provides an update on progress made on the General Controls Framework (GCF) project. Successful completion of this activity will give the business confidence over the effectiveness of its General Controls for business as usual operations and when pushing forward with transformation.

The initial focus is in support of the Financial Controls Framework project, but other areas will be considered subsequently.

The General Controls Framework has been included in this year's Annual Report in the risk note. Ultimately, our review of the GCF and the subsequent self-assessment by control owners will help the Board complete its year-end Annual Assessment of Internal Controls for 2016/ 17.

Details of the General Controls Framework:

<table>
<tr><td colspan="5">A) PURPOSE & DIRECTION</td></tr>
<tr><td colspan="2">1) Strategy, objectives and targets</td><td colspan="2">2) Code of Business Standards and Tone from the Top</td><td>3) Social Purpose</td></tr>
<tr><td colspan="5">B) PLANNING & REVIEW</td></tr>
<tr><td>4) 3 Year and Annual Plans</td><td>5) Change is planned and monitored</td><td colspan="2">6) Risk assessments</td><td>7) Performance monitoring</td></tr>
<tr><td colspan="5">C) ORGANISATIONAL DESIGN & DELEGATION</td></tr>
<tr><td rowspan="2">8) Organisational Structure, with Responsibilities and Segregation of Duties</td><td rowspan="2">9) Delegation of Authority, including Capital Investment limits</td><td rowspan="2">10) Staff calibre, experience and qualifications, including personal development and appraisal</td><td rowspan="2">11) Senior Management remuneration</td><td>12) Operational, financial and regulatory policies (and control activities) framework</td></tr>
<tr><td>13) IT policies (and control activities) framework</td></tr>
<tr><td colspan="5">D) GOVERNANCE & FEEDBACK</td></tr>
<tr><td>14) Board and Audit Committee</td><td>15) Assurance capability</td><td colspan="2">16) Whistleblowing and Complaints</td><td>17) External Reporting</td></tr>
</table>

Questions this paper addresses

1. What progress has been made since March? Are we progressing to plan?
2. What is happening to any significant gaps identified?
3. How do we ensure the GCF remains focused on the right areas?

POL00423565

Conclusion

1. During the period, Internal Audit reviewed the General Control elements of the Financial Controls Framework project and used this to confirm the design of our GCF, assess its current state, ensure any appropriate remediations have been identified and prepare templates for our subsequent Self-Assessment exercise.

   The project is progressing per our original project plan (see appendix 1 for details and timing). We aim to complete the full Current State Assessment of the GCF by mid June (ahead of plan). Self-assessment templates will be completed, in preparation for a dry run/ test attestation by GE Owner at next half year and full roll out at the year-end.

2. Where the Finance project team and KPMG have identified gaps or controls that need strengthening, these have been reviewed by Internal Audit. A pragmatic view has been taken on gaps and remediation activities, recognising not everything can be fixed straightway, and effort will be focused on fixing only what is needed.

3. As we progress we continue to review and challenge the GCF to ensure it is focused on the right areas. We believe that an additional element is required to reflect the importance of controlling change (e.g. "**change is planned and monitored"**). This has been added as a separate element under Planning and Review (see appendix 2).

Input Sought

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

POL00423565

Appendix 1 – General Control Framework – Project Plan

Set out below is an overview of our approach and timings to prepare the business for attestation of GCF effectiveness reporting in March 2017, including key activities and reporting milestones.

Overview

Month	Activity	Update to ARC
2016		
January	Design GCF	✓
February	Scope testing and developing tools	✓
March	Current State Assessment preparation	✓
April	Current State Assessment of GCF components	*50% complete*
May		
June		
July	Dry Run Preparation & Engagement	
August	Dry Run Assessment	
September	Dry Run Reporting	ARC
October	Remediations	
November		ARC
December		
2017		
January	Year End Preparation & Engagement	ARC
February	Year End Assessment	
March	Year End Reporting	ARC
April	Lessons Learnt	

POL00423565

Appendix 2 – General Controls Framework – Detail - Revised

Includes additional element "Change" as 5)

A) PURPOSE & DIRECTION
1) The **strategy**, objectives and targets are agreed and communicated, both internally and externally.
2) A **Code of Business Standards** is communicated and understood, and reinforced by the **Tone from the Top**.
3) Our **Social Purpose** is agreed and communicated, both internally and externally.

B) PLANNING & REVIEW
4) **3 Year and Annual Plans** (operating and capital) are prepared and reviewed by Management, before approval by the Board.
5) **Change is planned and monitored** to ensure its meets the business objectives, that risks are managed and appropriately mitigated and that approved benefits are realised.
6) Pre-emptive **risk assessments** of Business Plans, projects and business as usual operations are conducted, with current controls reviewed and additional actions identified where necessary to bring the desired level of control back within an acceptable level of risk taking (our risk appetite).
7) **Performance** is monitored and variances between forecast/ budget and actual are analysed and investigated. Change is planned and monitored to ensure benefits realised and user acceptability.

C) ORGANISATIONAL DESIGN & DELEGATION
8) An **Organisational Structure** has been put in place aligned to strategy, with lines of responsibility and appropriate segregation of duties.
9) Formally defined **Delegation of Authority**, including capital investment limits.
10) **Staff** have been appointed of appropriate calibre to fulfil their allocated responsibilities, with appropriate experience and qualifications checked on entry and monitored, with defined job descriptions. **Personal development** and appraisal procedures are in place to ensure an effective workforce.
11) **Senior Management remuneration** is designed to align personal and business objectives, as well as to discourage dishonest, illegal or unethical acts.
12) **Framework** of appropriate **policies**, standards and procedures **and control activities**, including **operational, financial and regulatory requirements**, are in place, communicated and compliance monitored. Significant changes are reported to the Board and relevance monitored.
13) **Framework** of **IT policies and control activities**, including segregation of duties, are designed and implemented to protect the completeness, integrity and security of our operations and data.

D) GOVERNANCE & FEEDBACK
14) The **Board** and **Audit Committee** have defined Terms of Reference and an effectiveness review process.
15) The Audit & Risk Committee seeks and receives appropriate **assurance** on key risks and controls (specifically including financial control and reporting) from sources such as Management representations, self-assessment and independent assurance functions (Internal Audit).
16) A **Whistleblowing policy** and service is available to all staff and calls are actively followed through and appropriately reported to the Board. Similarly a Complaints procedure is available to customers, suppliers and other external stakeholders.
17) **External reporting procedures** are formalised to present a fair, balanced and understandable assessment of the company's position and prospects to stakeholders, in compliance with the applicable regulations.

POL00423565

POST OFFICE
RISK AND COMPLIANCE COMMITTEE

4b) Policy Framework Project update

Author: Mark Rodgers | Sponsor: Mike Morley-Fletcher | Meeting date: 05 May 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 also supports other Post Office initiatives such as the Partnership Banking Agreement work.

The project aims to develop a suite of key policies for Post Office and splits this into two sequential phases: the first is to confirm Corporate Services ("CS") policies, review them and, where necessary re-revise or develop them; the second phase will identify key policies from other areas of the business and ensure these are reviewed, re-drafted or developed and implemented too. Our external auditors have provided benchmark data which has been used to ensure the reasonableness and completeness of the final suite of policies (both CS and non-CS). As policies are developed or revised they will be presented for approval to the RCC/ ARC.

Questions?

PHASE 1

a) Are we still on plan for phase 1?
b) Can RCC ratify the policies we have developed or revised?
c) How will we manage subsequent implementation of the policies from phase 1?

PHASE 2

d) For phase 2, can RCC agree the proposed suite of policies, which have been subject to the benchmarking exercise, from other business areas?
e) What are the next steps?

Conclusion

PHASE 1

a) We are on track with phase 1 work for the seventeen CS policies and lessons learned are being documented. Drafting of the CS policies, review and sponsor/ Executive policy Owner sign off is nearing completion, due at the end of April 16 (see appendix 1). As part of phase 1, the review and remediation of policies for the March 2016 (Partnership Banking Agreement ("PBA") project deadline was met.
b) Seven key policies are presented for RCC approval (five from CS and one from IT and one from HR). A summary of the policies is attached (see appendix 5) and policy documents are included in agenda item 5, were approval will be considered.
c) These policies, once approved, will be rolled out to the business by the policy Owner. A policy implementation process has been developed with implementation owners and a suggested timeline for embedding the CS policies (see appendix 2). These will require agreement by key stakeholders for details and timelines. Arrangements to use a dedicated Sharepoint site as a repository are progressing with support requested from the Communications team.

PHASE 2

d) To establish a full suite of policies, including other business areas, we have developed a strawman list from reviewing other organisations and then used data provided by Ernst & Young to benchmark the list. The resultant set of key policies (see appendix 3) is presented for RCC review and agreement. A summary of the benefits of including and the consequences of not

POL00423565

including the three policies we believe we do not currently have, or do not have in adequate condition is attached (see appendix 4).

e) Once the final suite of policies is agreed by RCC, prioritised remediation will commence and then rolled out to the business.

Input Sought

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

a) the progress to date for the phase 1 CS policies, and

b) the benchmarked suite of policies from other areas of the business for phase 2.

Please note: policies submitted for approval are included in agenda item 5, where approval will be considered.

Appendices

Appendix 1: Corporate Services – progress to date
Appendix 2: Policy Implementation Process
Appendix 3: Key Policy Framework – latest update of strawman
Appendix 4: Key Policy Framework – benefits of including three further policies
Appendix 5: Policy Approval – Summary of policies and rationale

POL00423565

Appendix 1: Corporate Services – Progress to date

We are on track with phase 1 work for the seventeen CS policies and lessons learned are being documented. Drafting of the CS policies and review and sponsor/ Executive policy owner sign off is nearing completion, due at the end of April 16.

Five of these CS policies, highlighted in bold, are being presented for approval by the RCC/ ARC.

Policy	Policy Owner	Existing Policy reviewed	Policy Drafted/ Stakeholder review completed	Target for Policy RCC/ARC approval
Corporate Governance, including				
1) Board Constitution	Alwen Lyons	No existing policy	N/A (*See Note 1)	N/A (*See Note 1)
2) Conflicts of Interest	Alwen Lyons	Yes	ETA:End of April	July 2016
3) Enterprise Risk	Mike Morley-Fletcher	Yes	Completed	Not required, RCC Approved during 2015 (*See Note 2)
4) Internal Audit Charter	Garry Hooton	N/A *(*See Note 3)*	N/A (*See Note 3)	N/A (*See Note 3)
5) Whistleblowing	**Nisha Marwaha**	**Yes**	**Completed**	**May 2016**
6) Investigations	Nisha Marwaha	Yes	Completed	July2016
Security				
7) Physical Security	John Scott	Yes	Completed	July 2016
Information Security, including				
8) Cyber and Information and Security	Julie George	Yes	Not required, RCC Approved during 2015 (*See Note 2)	Not required, RCC Approved during 2015 (*See Note 2)
9) IS - Acceptable Use	Julie George	Yes		
10) Business Information Systems	Julie George	Yes		
11) Information Assurance (incl. Data Protection)	Julie George	Yes		
Financial Crime, including				
12) Financial Crime	**John Scott**	**Yes**	**Completed**	**May 2016**
13) Anti-Bribery and Corruption (incl. Gifts and Hospitality)	**Ben Foat**	**Yes**	**Completed**	**May 2016**
14) Anti-Money Laundering (incl. Counter Terrorism & Sanctions)	**John Scott**	**Yes**	**Completed**	**May 2016**
15) Cyber Fraud (including Forensics)	Julie George	Yes	Not required, RCC Approved during 2015 (*See Note 2)	Not required, RCC Approved during 2015 (*See Note 2)
16) Prosecution (England & Wales)	Rodric Williams	Yes	Completed Feb 2016 (*See Note 4)	Completed Feb 2016 (*See Note 4)
Business Continuity, including				
17) Business Continuity	**Jonathan Waples**	**Yes**	**Completed**	**May 2016**

* Note 1. There is no overarching Board Constitution policy. Direction is provided by the existing Articles of Association, Matters referred to Board, ToRs, Delegation of Authority
* Note 2. These policies have been reviewed and already meet policy standards. RCC approved these policies during 2015 and no remediation is required for these policies. Policies will be reviewed as per the documented policy review cycle in each case.
* Note 3. The Internal Audit Charter is denoted N/A because it is already a compliant document with Internal Audit International Professional Practice Framework Standards which incorporate qualitative documentation standards.
* Note 4. The Group Prosecution Policy (England & Wales) was approved by the Board in February 2016.

POL00423565

Appendix 2: Policy Implementation Process

These are the steps we identified for planning and monitoring implementation of policies. They will be trialled with CS polices before being recommended to other business areas. An estimated timeline of 6 months has been used.

Implementation Steps	Details	Example timeline (estimated at 6 months)
1) Establish accessible storage and maintenance protocols	❑ Publish documents to SharePoint ❑ Update Intranet and links (checking searches) ❑ Define maintenance	By 31/05/16
2) Communicate policy and requirements	❑ Agree audience (for communication and training) ❑ Develop communications policy and messages ❑ Communicate policy and requirements	By 30/06/16
3) Develop and deliver supporting training	❑ Identify resources and compile modules/ materials (Learning Academy) ❑ Coordinate and deliver training ❑ Publish to SharePoint	Develop by 31/07/16, deliver by 31/08/16
4) Identify and develop associated controls	❑ Confirm associated controls framework and catalogue controls library ❑ Create matrix of responsibilities (include RACI if required) ❑ Confirm controls operating as expected	Identify by 30/06/16, develop by 31/08/16
5) Monitor and measure compliance	❑ Identify and define compliance monitoring procedures, systems and controls ❑ Identify measures and test monitoring plans ❑ Commence monitoring routines ❑ Capture results, evaluate, define management information and report to governance committees	By 30/10/16
6) Review policy	❑ Use monitoring results to evaluate current policy controls and continuing appropriateness of policy ❑ Maintain policy review log ❑ Conduct annual/ bi annual policy reviews and report to relevant governance body	By 31/12/16

POL00423565

Appendix 3: Key Policy Framework – Latest update of strawman

Phase 1 is the suite of Corporate Services policies which have been reviewed and remediated.

Phase 2 is a proposed strawman of possible key policies* from other business areas. Through review of other organisation's policy suites and on consideration of our specific needs we have developed a proposed strawman list of key policies. We have then used data provided by Ernst & Young to benchmark this policy suite to produce our recommendations below. In addition to the CS policies already agreed, we are proposing a further fourteen policies. Of these, we already have most in a reasonable state. The three highlighted in yellow and bold either are not formalised policies or are in fragmented form: all have some reference material to help with drafting of a full policy. Suggested benefits of including these three further policies are included in appendix 4.

Key Framework Policy (Big P)	Policy Sponsor (GE Owner)	Policy Owner
PHASE 1 – CORPORATE SERVICES		
Corporate Governance, including 1) Board Constitution (Articles of Association, Matters referred to Board, ToRs, Delegation of Authority)** 2) Conflicts of Interest 3) Enterprise Risk 4) Internal Audit Charter 5) Whistleblowing 6) Investigations	Jane MacLeod	1) Alwen Lyons & Victoria Moss 2) Alwen Lyons & Susie Hayward 3) Mike Morley-Fletcher 4) Garry Hooton 5) Nisha Marwaha 6) Nisha Marwaha
7) Physical Security	Jane MacLeod	7) John Scott
Information Security, including 8) Cyber and Information and Security 9) IS - Acceptable Use 10) Business Information Systems 11) Information Assurance (incl. Data Protection)	Jane MacLeod	8) Julie George 9) Julie George 10)Julie George 11)Julie George
Financial Crime, including 12) Financial Crime 13) Anti-Bribery and Corruption (incl. Gifts Policy) 14) Anti-Money Laundering (incl. Counter Terrorism, Sanctions) 15) Cyber Fraud *(same as 8)* 16) Prosecution (England and Wales)	Jane MacLeod	12) John Scott 13) Ben Foat 14) John Scott 15) Julie George 16) Rodric Williams
17) Business Continuity	Jane MacLeod	17)Jonathan Waples
PHASE 2 – NON-CORPORATE SERVICES		
18) Customer Treatment (including Elderly/ Vulnerable)	Martin George	18)To be confirmed
19) Social Purpose - Distribution Network Coverage (Entrustment Letter, Nov 2013)**	Kevin Gilliland	19)Kevin Seller
20) Business Change Management	David Hussey	20)Alison Thompson
Finance, including 21) Accounting and Reporting Manual 22) Treasury Risk Management **23) Procurement** **24) Travel & Expenses** 25) Disaster Recovery	Alisdair Cameron	21) Dave Carter 22) Dave Carter/ Charles Colquhoun 23) Mark Dennis 24) Mark Dennis 25) Stephen Hayes
Human Resources, including 26) Talent and Resourcing 27) Reward and Recognition 28) Learning and Development 29) Performance, Attendance and Behaviour 30) Health & Safety 31) Code of Business Standards	Neil Hayward	26) Tom Moran 27) Tom Moran 28) Tom Moran 29) Tom Moran 30) Martin Hopcroft 31) Colin Stretch

Notes
** 'Big P' or key policies are those which are "materially" important because they provide direction to the content, extent and style of how our Board expects the company and our staff to act and behave in response to "key" needs of our stakeholders.*
*** Where there is no actual policy document, details of alternative documentation which provides the direction of a policy is given in italics. For instance we do not have a Board Constitution policy, but direction is provided by the Articles of Association, Matters referred to Board, Terms of References, Delegation of Authority, which have been approved by the Board.*

POL00423565

Appendix 4: Key Policy Framework – Benefits of including three further policies

We have used data provided by Ernst & Young to benchmark this policy suite to produce our recommendations (see appendix 3). Of the In addition to the CS policies already agreed, we are proposing a further fourteen policies. Of the fourteen, we have eleven already and three we do not have. Below is a view of why we need the three additional policies. The rationale is in terms of the benefits for inclusion and the negative consequences if we do not set policy.

Rationale

Proposed Policy	Benefits of this Policy	Consequences of not having this policy
18) Customer treatment	• Focuses identification of target customers • Supports customer-centric reputation • Enhances social purpose commitments • Supports customer service (e.g. sector NPS, Effort, CSAT, Wait time) • Helps accuracy of management reporting and effectiveness of customer understanding	• Potential censure and sanctions around vulnerable customers by regulators • Raises potential conduct risk challenges • Potential complaints due to uncertainty in standards •
23) Procurement	• Supports consistent contract management dealings with third parties (depending on TOM) • Supports procurement efficiency and cost control • Helps accuracy of management cost information for decision making • Efficient, clear processes make us good to work with	• Additional cost through inefficient and inconsistent procurement • Lack of contract certainty • Potential risk of poor service provision and impaired or failed service levels • Potential FCA SYSC8 censure and sanctions • Increases litigation risk
24) Travel & Expenses	• Supports cost control consistency • Helps accuracy of management cost information for decision making • Clarity for staff on what can/ can't do, should/ shouldn't do	• Additional cost through inefficient travel and inappropriate expenses • Increased potential for financial crime • Reputational risk • Potential accounting standards breaches • Increased complaints from staff

POL00423565

Appendix 5: Policy Approval – Summary of policies (7) and rationale

See agenda item 5 for policy documents, where approval will be considered.

Ref	Key Framework Policy	Sponsor (GE Owner)	Policy Owner	Why is this policy needed?	Approved by?	How will the policy be implemented?	How will policy compliance be monitored?
12) (PBA)	Financial Crime	Jane MacLeod	John Scott	To help Post Office meet legal and regulatory obligations within appetite, and to manage financial crime risks reducing actual loss, avoiding potential losses.	RCC and ARC May 2016	Proposal for process to implement policies, including: • where they should be stored • how they should be communicated and supported with training • how they should be controlled, monitored and reviewed. Please refer to appendix 2 for more details.	1. Policy Compliance Manager will coordinate, and ensure QA standards, including compliance monitoring. 2. Policy Owner undertakes compliance, and will identify measures, develop monitoring processes, track results and provide reporting with MI to the relevant governance body.
13) (PBA)	Anti-Bribery and Corruption (incl. Gifts & Hospitality)	Jane MacLeod	Ben Foat	To help Post Office meet its legal and regulatory obligations within appetite, to help manage ABC risks, and support good conduct standards in all dealings.	RCC and ARC May 2016		
14) (PBA)	Anti-Money Laundering (incl. Counter Terrorism, Sanctions)	Jane MacLeod	John Scott	To help Post Office meet its legal and regulatory obligations within appetite, and to help manage AML (CTF and Sanctions) risks whilst reducing actual loss, and avoiding potential losses.	RCC and ARC May 2016		
17) (PBA)	Business Continuity	Jane MacLeod	Jonathan Waples	To embed a framework to identify potential threats to business continuity, and to help manage impacts to business operations. It is a set of standards which support resilience and sets out the capabilities to respond.	RCC and ARC May 2016		
25) (PBA)	Disaster Recovery	Alisdair Cameron	Stephen Hayes	To embed a framework to identify potential threats to disaster recovery, and to help manage impacts to IT/ business operations. It is a set of standards which support resilience and sets out the capabilities to respond.	RCC and ARC May 2016		
26) (PBA)	Talent and Resourcing: HR Vetting	Neil Hayward	Sean Leahy	To ensure Post Office operates vetting processes in a legal, and compliant way. To embed standards to control and reduce the risks of error, theft, fraud or misuse of facilities. To ensure Post Office engages with suitable workers.	RCC and ARC May 2016		
5)	Whistleblowing	Jane MacLeod	Nisha Marwaha	To help Post Office meet its legal and regulatory internal and external obligations. To implement good practice and engender good standards in this context.	RCC and ARC May 2016	As above	As above

POL00423565

POST OFFICE
PAPER FOR RCC

4c) Business Continuity & Crisis Management Project update

Author: Jonathan Waples Sponsor: Jane MacLeod Meeting date: 5th May 2016

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 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 and is divided into three phases:

- Phase 1: Gap analysis; Business Continuity policy creation; Crisis Management review; pilot Business Continuity activity
- Phase 2: Expanded BC activity; Business Continuity Management Systems Framework delivery
- Phase 3: Improved BCMS awareness; BCMS integration to BAU.

In addition, the Business Continuity Project Manager is available to assist the business with its ongoing BC and CM support needs.

Questions this paper addresses

1. How have we progressed our plan?
2. How is this bringing us in line with ISO 22301?
3. Can we answer the ARC's request on top suppliers yet?
4. Can we answer the ARC's request on Crisis Management process yet?

Conclusion

1. 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 processes (end of April 2016). Business Impact Assessments for the three priority areas are in progress and

POL00423565

will enable review of BC Plans (for these areas) by the end of May. Phase 1 is near completion and Phase 2 is underway. See Appendix 1 for details.

Planned progress was for 40% of achievement to conformity to ISO 22301 at this stage, which has been achieved. The majority of effort in the opening stages of the project related to discovery and gap analysis of current capability against the agreed standard. From this point, activity is focused on achieving alignment to the best practice principles, and will therefore deliver significant advances in conformity over the coming months.

2. The ARC requested a view on top suppliers and their Business Continuity capabilities, and a reach-out was initiated to request visibility of BC planning, capability & testing regimens. Results have been slow in delivery, despite persistent follow-up by POL relationship managers, and project resources.

3. Additionally, the ARC enquired about how their potential engagement in the Crisis Management process might be managed during an invocation. This is described in sections 5.4 and 5.5 of the Major Incident Response Procedure (Appendix 2). Designed to engage the right stakeholders, at the right time, during any invocation, the procedures state that NED involvement would be requested – by the Gold Team (all GE) - at the height of a Crisis event.

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.

POL00423565

Appendix 1

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	Activity - BPT Invocation Test Publish Major Incident Response Procedure	
- Schedule and begin Business Impact Assessments	Develop BIA Methodology Documentation Business Impact Analysis Process Documentation Business Impact Analysis Workbook	Supply Chain BIA - Sean Farrow Business Impact Assessment: Supply Chain	Financial Services BIA - Business Impact Assessment: Financial Services IT BIA - Andy Garner Business Impact Assessment: IT
- Schedule and begin Business Continuity Plan Development		Supply Chain Business Continuity Plan - Sean Farrow	Business Continuity Plan: Supply Chain Activity: Business Continuity Rehearsal: Supply Chain - Earliest Possible Date
- On-going BCM Planning for priorities (embedding to BAU)			Property Business Continuity Plan - Kevin Seller Business Continuity Plan: Property Activity: Business Continuity Rehearsal: Property - Earliest Possible Date IT Business Continuity Plan - Andy Garner Business Continuity Plan: IT Activity: Business Continuity Rehearsal: IT - Earliest Possible Date
Phase Two: Expanded BC activity; BCMS Framework delivery			**End of July Completion Target**
- BC Management Programme Structure		Procedure for the Management of Non-Conformity	Continuous Service Improvement Process Business Continuity Programme Auditing Process Business Continuity Programme Audit Plan Business Continuity Exercising & Testing Schedule Business Continuity Test Plan Business Continuity Test Report Procedure for the Control of Documents Procedure for the Control of Records Business Continuity Communication Plan BC Risk Assessment Process BC Risk Assessment Report BC Risk Assessment Workbook BC Risk Treatment Plan
- 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

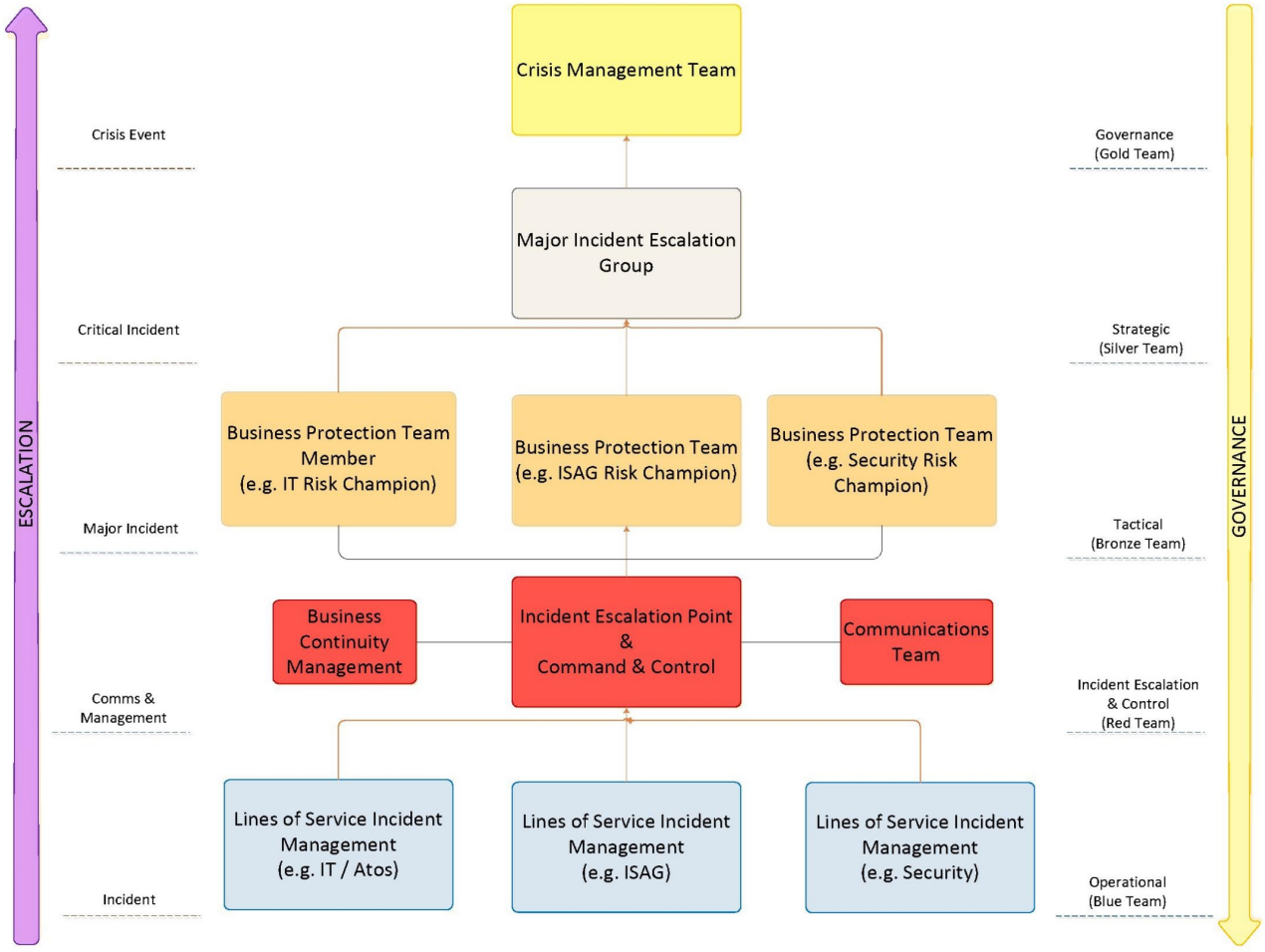
POL00423565

Appendix 2

The following is an extract from sections 5.4 & 5.5 of "Major Incident Response Procedure", detailing the Major Incident Response Teams' construct and each levels roles and responsibilities, including senior stakeholder engagement during a Crisis Management invocation.

Designed on the principle of escalation to the relevant business stakeholders and specialists, the construct swiftly engages appropriate resources efficiently in resolving the incident. In consequence, GE involvement will be on a selective basis if invoked at Silver Team level, or on a full basis at Gold Team level. An invocation of the Gold Team may instigate, the involvement of our major stakeholders, such as the NEDS or ShEx.

5.4 Major Incident Response Teams' Construct



POL00423565

5.5 Major Incident Response Teams' Responsibilities

GOLD TEAM – Crisis Management Team (CMT)

All GE Members (potentially other major stakeholders – NEDs, Ministers, etc.); Instigated at point of high crisis (escalated Major & Critical Incidents; prolonged severe operational disruption across majority of business units; reputational damage or risk; Ministerial or Judicial scrutiny, etc.)

SILVER TEAM – Major Incident Escalation Group (MIEG)

Selected, appropriate, GE membership supported by senior management teams; instigated in response to major incident event (escalated Major incidents; significant operational disruption across multiple business units; major disruption to individual office / operational locations; major disruption to IT service(s) provision across all / majority of network; significant staff abstraction events (snow days, transport strikes etc.). Tactical guidance to BRONZE team, in response to GOLD, as appropriate.

BRONZE TEAM – Business Protection Team (BPT)

Senior management representation from across all business units. Invoked on escalation from any departmentally managed Incident to a Major Incident. Remains in direct control of Operational resources during ALL levels of response above Incident, receiving tactical and strategic guidance from SILVER & GOLD teams respectfully.

RED TEAM – Incident Escalation Point & Command and Control (EIP / C&C)

Permanently assigned resource dedicated to managing incident escalation and communication across the POL network (branch & offices). Single, direct line of communication to Operational Teams. Operates across all levels of Crisis Management Construct from the moment of Incident escalation to the point of closure. Has direct engagement with Business Continuity function and Communications Team, to ensure adherence to CM & BC process and appropriate internal and external comms.

> *Caveat: At this point in time, there is no single capability for this function within POL. Escalation is affected by a call to Atos Service Desk requesting they contact the Business Protection Team and provide a conference call bridge for this group. At that point the central management of incident logging, comms, BC response etc. concludes, and reverts to BPT. This is inefficient, and the recommendation is that this hub activity be brought back in-house, potentially utilising an enhanced, permanent Command & Control Centre.*

BLUE TEAM – Operational Incident Management

Incident Management activities currently controlled within respective business units, either internally or via a third party (e.g. Atos) will need to develop an escalation route into the RED Section in order to engage Major Incident or Crisis Management

POL00423565

4d) Assurance Mechanisms: Executives' Declaration and CSA

Author: Deana Herley Sponsor: Mike Morley-Fletcher Meeting date: 5 May 2016

Executive Summary

Context

The purpose of this paper is to provide an update on the progress made in enhancing our Assurance Mechanisms. In particular, how we have started:

- the **Executives' Declaration** return, completed by the General Executive (GE), and
- **Control Self-Assessment** (CSA) techniques to provide assurance to Management and the Board (via the ARC) over key control areas – we have started with the Financial Reporting processes and then will move to the General Control Framework.

Questions this paper addresses

1. How have we progressed with trialling the Executives' Declaration?
2. What are the results of the Executives' Declaration, are further disclosures required?
3. Is the implementation of CSA on target?

Conclusion

1. **Executives' Declaration**. At the last RCC we launched a new exercise, run by Internal Audit, to support GE members in considering (and attesting) if any additional disclosures were required in our Annual Report as part of our year-end procedures. Against a set of key question areas, this involved GE members consulting with their lead teams and making further enquires with relevant Finance, Risk and Legal representatives to identify any additional issues or concerns that have not been already recorded as a part of normal management processes. Going forward, GE members will be asked to attest twice annually, at half year and year end in support of our Interims and Finals.
2. **Executives' Declaration exceptions.** Outputs have been collated and reviewed for consistency against Internal Audit reviews. **Seventeen exceptions were identified:**
   - six exceptions have already been disclosed
   - one exception (qu 5, item i) requires disclosure but this has not been made yet – re mobile decision
   - nine were considered by the owner, but the decision is that no disclosure is required
   - one exception (qu 8, item o) has been identified which requires further debate over whether we should disclose – re "extent of oversight over levels of compliance of sales of regulated products in the network".

   All items noted are summarised in appendix 1 and exceptions highlighted in yellow.
3. **Control Self-Assessment.** To enable automation of CSA of the Financial Reporting processes, a task management workflow solution has been selected (TrAction hosted by PWC). We will start with **Fixed and Intangible Assets** in May. A phased approach will then be taken to on-board the 11 other financial reporting processes (**Jun-Sept**). Independent testing over the Financial Controls Framework project deliverables by Internal Audit will be planned for June. As noted previously the General Control Framework will also be self-assessed using TrAction.

POL00423565

Input Sought

The Committee is asked to review the information provided in appendix 1 and confirm whether:

- the exception noted should be disclosed
- agree with exceptions where decided is NOT to disclose
- after consideration of these items, any other exceptions should be considered.

POL00423565

Appendix 1 – Exceptions

EXECUTIVES' DECLARATION SUMMARY			
Statement	**Exceptions**	**GE Member**	**Decision**
1) any material **risks** to PO that are not captured in the Group Risk Profile	**None.**	**All**	**N/A**
2) any material **control** failures or breaches, including of the **General Control Framework** and **policies** that I am accountable for	**a) Postmasters' Compensation re-statement,**	**Alisdair Cameron**	**Disclosed already**
	b) General weakness in consistency and transparency of **financial reporting controls.**	**Alisdair Cameron**	**Disclosed already**
	c) The **General Control Framework** ('GCF') is of recent implementation within Post Office and therefore work to assess the level of controls already in place and whether they are fit for purpose, is still at a preliminary stage.	**Jane MacLeod**	**Disclosed already (in Risk note)**
	d) Further, the **policy suite** to support the GCF is not complete and those policies for which I am responsible have not yet been through governance, nor do we yet have a **self-assessment process** against those controls and policies.	**Jane MacLeod**	**Disclosed already (in Risk note)**
3) any material **frauds**, **irregularities or losses** that have come to light, whether carried out by our staff, agents, contractors, suppliers or partners	**None.**	**All**	**N/A**

POL00423565

4) any complex or subjective **accounting judgements, estimates and revenue transactions**	**e) Accounting for Gamma**.* **(see below)** Under the agreement with Bank of Ireland, in 2012 POL received one-off, non-refundable income in lieu of providing distribution for Bank of Ireland products, including insurance products. This income (Gamma) is being recognised over the period of the agreement. Following the Project Hawk acquisition, POL no longer has any obligations to Bank of Ireland in respect of insurance and a paper has been submitted to the external auditors by Group Financial Control setting out the rationale for recognising an appropriate portion of the Gamma income (c£4.5m) in 2015/16.	**Alisdair Cameron & Nick Kennett**	**Disclosed already**
	f) Exceptionalisation of the costs of project Hawk in POL and POMS*: A paper setting out the rationale for this has been submitted to the external auditors by Group Financial Control. Total amount treated as exceptional is £3m.	**Nick Kennett**	**Disclosed already**
	g) Estimation of FRES profit share at year end: The draft financial statements for 2015/16 include income of £35.3m in respect of POL's share of profits of its FRES joint venture. Of this, £2.4m relates to the profit share for March 2016. This amount is consistent with estimates from FRES management but will not be confirmed before POL closes its 2015/16 books.	**Nick Kennett**	**Proposed no disclosure required**
	h) Estimation of Credit Card profit share: The financial statements for 2015/16 include income of £750k in respect of profit share on credit cards under the arrangement with Bank of Ireland. This amount has been confirmed verbally by Bank of Ireland, but the actual amount will not be confirmed before POL closes its 2015/16 books.	**Nick Kennett**	**Proposed no disclosure required**
5) any **provisions or exceptional items** not already recorded	**i)** We are just disclosing the need to provide on the **Mobile decision**.	**Alisdair Cameron**	**Decision to disclose made, but disclosure is currently outstanding**
6) any **liabilities and contingencies**, including those associated with guarantees	**j)** There is a risk that the **RMG Resource Costs and Incentives claim** as a result of delayed IT separation will exceed the estimate. POL received an invoice for £837,783 on 13 November 2015. This was formally disputed with RMG. It is not clear what further	**Jane MacLeod**	**Proposed no disclosure required**

POL00423565

	amounts they may claim for the period through to end of March 2016, but in conversations RMG have made reference to their claim potentially amounting to approximately £3m (and this is similar to the projected costs of this claim identified as approx. **£2.3m** by Roger Middleton).		
7) any material **legal action** being taken by or against PO	**k)** Threat from British Gas in the last couple of days for **unpaid energy bills**.	**Alisdair Cameron**	**Proposed no disclosure required**
	l) On 13 April 2016 we received a letter from Freeths Solicitors advising that they have **lodged a claim in the High Court on behalf of some 91 claimants**. They have not as yet served the claim on us and accordingly as at the date of this declaration we remain unsighted on the grounds of the claim, who it is brought on behalf of, or the remedy they are seeking.	**Jane MacLeod**	**Proposed no disclosure required**
	m) As proceeding against Post Office may be commenced by service on any POL business address (which includes Customer Service Centres and Crown Offices), there is **no guarantee that the relevant documents will be forwarded to the legal team with the consequence that we may not be aware of such proceedings**.	**Jane MacLeod**	**Proposed no disclosure required**
8) any **legislative**, **regulatory or contractual compliance issues** that have come to light	**n)** We are managing **risks around public procurement**, especially the **contract extension with Fujitsu**, which was published in February.	**Alisdair Cameron**	**Proposed no disclosure required**
	o) Post Office Limited as Appointed Representative for POMS has limited **oversight over the levels of compliance of sales of regulated products in the network**, in particular in **relation to over 50s life insurance and travel insurance**. While complaint levels are low, this does not of itself provide **assurance that sales are compliant**.	**Jane MacLeod**	**Debate if this should be disclosed (in the Risk note[1])**

[1] The Risk Note (Control environment: 2016/ 17) has wording to inform the reader of the current state of our ICF and policies (e.g. subtle reference to need for some improvement) and that we plan to progress this next year. In addition, however, we can add the following wording, ***"As part of embedding the risk management framework, we will review the model for oversight of regulatory compliance across the various sales channels to consider whether enhancements are required."***

POL00423565

	p) During 2015-16 I became aware that POL had entered into **network contracts with operators who were at the time, appointed representative of third parties**, giving rise to potential regulatory and contractual breaches.	**Jane MacLeod**	**Proposed no disclosure required**
	q) I am aware that during 2015/16 there were a number of **branches which operated under expired contracts or without a written contract.**	**Jane MacLeod**	**Proposed no disclosure required**
9) any material **new contracts** entered into, and where I have not followed the **contract process**	**Same as n) Fujitsu extension, CSC extension**.	**Alisdair Cameron**	**Refer to question 8, item n**
10) any direct or indirect **personal interest** in any transaction, arrangement or related parties entered into by PO	**None**.	**All**	**N/A**
11) any material events that could **crystallise** before the end of the reporting period above	**Same as j) Mobile decision**.	**Alisdair Cameron**	**Refer to question 5, item i**
12) any **other information** that could have an impact on period (indicated above) when drawing up our annual report.	**Same as b)** I am aware of a review of **POL internal controls** being carried out by KPMG for the CFO and that preliminary findings suggest some potential gaps versus an ideal control environment. However, I am not aware of the conclusions of this work, their implications or their potential materiality in the context of POL group.	**Nick Kennett**	**Refer to question 2, item b**

POL00423565

4e) Disclosure in Annual Report

Author: Mike Morley-Fletcher Sponsor: Jane MacLeod Meeting date: 5 May 2016

Executive Summary

Context

As agreed by RCC and ARC, compliance with the UK Corporate Governance Code is not sought at present, however, we intend to maintain *"standards of corporate governance appropriate for our ownership structure, our commitment to our social purpose and our strategy for commercial sustainability"*. We have used this to guide our disclosure notes.

For this year's risk, control and assurance disclosures, the Risk and Internal Audit team reviewed the previous PO Annual Report, discussed best practice with our external auditors and considered other relevant organisation's reports to ensure we are providing appropriate, up to date and informative disclosures to our stakeholders. Several enhancements have been made and are detailed below. *Please read in conjunction with relevant sections in the draft Annual Report – see appendix 1.*

Questions this paper addresses

1. How have we explained our approach to Corporate Governance compliance and disclosure?
2. What changes have we made to the risk and control disclosures on how we manage risk (as part of the GE note)?
3. What changes have we made to the risk and control disclosures on how we govern risk (as part of the ARC note)?

Conclusion

1. Corporate Governance compliance statement – redrafted by RCC/ ARC:
   - Includes our redrafted Corporate Governance statement, *"PO maintains standards of corporate governance appropriate for our ownership structure, our commitment to our social purpose and our strategy for commercial sustainability"*.
2. Managing Risk – fuller details are provided on how we manage risk and what our principal risks – see appendix 1 and 2:
   - Explains in greater detail our approach to risk, our risk management framework and our risk governance.
   - Includes for the first time a description of our Internal Controls Framework, now that we have defined it, are assessing and remediating it, to explain to stakeholders the key general controls we use to manage the business.
   - Provides more details on our principal risks, disclosing all 14 risks identified by the RCC (8 included last year), with updated details of causes, consequences, mitigations and trends compared with last year.
3. Governing Risk – fuller details are provided on how Internal Audit assures the Board and how the Board conducts its annual assessment of our risk management framework and internal controls:
   - Includes for the first time a description of Internal Audits activity, how the annual plan is developed and details of the types of audits conducted in 2015/ 16.

POL00423565

- Includes for the first time a description of how the Board, via the ARC, assesses the risk management framework and systems of internal control.

Input Sought

The Committee is asked to review the disclosures presented, in particular the details of our Principal Risks and Mitigations in appendix 2, and provide any input or feedback, before they are presented to the ARC for approval.

POL00423565

Appendix 1: Risk Extracts from the draft 2015/ 16 Annual Report - Managing our risks

Points to consider:

- section on Internal Control could be shortened?

Our Approach to Risk

We define risk as anything that can adversely affect our ability to meet the Post Office's objectives, maintain its reputation and comply with regulatory standards.

Risk is not something that we can avoid. It is an inherent part of how the PO seeks to grow and create value. Instead we seek to understand and harness risk in the pursuit of our aims and business plan objectives. As we progress, our aim is to operate within an acceptable level of risk taking, in accordance with risk appetite parameters set by the Board.

All staff are expected to be aware of risks in their areas of responsibility and manage those risk intelligently in their day-to-day activities.

Risk Management Governance

The Board is accountable for the risk management and internal control systems in the Post Office, for reviewing their effectiveness and for determining the nature and extent of the principal risks. Responsibility for day-to-day operations rests with members of the Group Executive. The Risk and Compliance Committee, on behalf of the Group Executive, reviews the operation of the risk management process and management of the principal risks. The committee is chaired by the General Counsel, membership includes all of the Group Executive and the output is reported to the Audit, Risk & Compliance Committee (ARC).

Assurance for the Board over the effectiveness of our risk management and internal controls is provided by the Audit, Risk and Compliance Committee, through review of reports from Management, particularly the Risk And Compliance Committee (RCC), Internal Audit, external advisers and External Audit.

For further details on Governance of our risk management and internal controls see XXX on page YYY.

Our Risk Management Framework

To improve our ability to consistently spot, manage and monitor risks, and take advantage of opportunities we might otherwise miss, we have developed a structured framework for assessing, managing and communicating risk. The framework identifies roles and responsibilities, the policies for how risks are managed, the tools and processes used, a risk appetite statement and the reporting outputs to inform both Management and the ARC.

Material risks are identified by business areas (bottom up analysis) for their own risk management; Group Executive members review these and add further strategic and external perspectives (top down review). The scope of risks to consider is facilitated by a Risk Universe. Impact and likelihood is assessed for evaluating each risk, after consideration of the controls we have in place. Where the resultant, "net", risk profile is considered in excess of our risk appetite, a response will be needed to bring the risk back within an acceptable level of risk taking. For other risks we may want to introduce monitoring procedures. Details of our Principal Risks are included on page ZZZ.

Our Control Framework

Our risk management efforts are underpinned by our internal control framework. The Board has put in place an organisational structure with formally defined lines of responsibility and delegation of authority. Executive Management have established procedures for setting our direction, planning and controlling the operation of our business, and reviewing and monitoring our performance and conduct. These include:

POL00423565

- communication of the Group's strategy, objectives and targets
- expectations of standards of conduct by our colleagues as set out in our Code of Business Standards
- definition and review of our social purpose
- setting by operating divisions of the annual and three-year operating and capital plans and review by Board. This includes the identification and assessment of risks compared to our appetite
- monthly comparisons of operating divisions actual financial performance with budget, with consideration by the Board of year end forecasts
- an organisational structure with lines of responsibility and appropriate segregation of duties
- change management approach, resources and governance are used to manage significant projects
- formally defined delegation of authority, including capital investment limits and a treasury policy
- appointment of employees of the necessary calibre to fulfil their allocated responsibilities, with formal personal development and appraisal procedures
- senior management remuneration designed to align personal and business objectives, as well as to discourage dishonest, illegal or unethical acts
- a framework of operating, financial and IT policies and procedures, communicated and monitored
- a whistleblowing procedure for colleagues to raise concerns in confidence and if required, anonymously; a complaints procedure is available to customers and third parties.

Progress during the year and plans for next year

During the year, we have continued to develop our risk management capability. Highlights of what's been achieved and what is planned for next year include:

Risk assessment: during 2015/ 16, there has been more regular use of the risk management framework in business areas and by RCC, with greater focus on defining further actions required to manage risks and the introduction of longer term horizon scanning	**Risk assessment:** for 2016/ 17, we plan to focus our incident reporting process to provide lessons learnt on our risk assessments and operationalise our risk appetite further
Control environment: during 2015/ 16, we have reviewed the appropriateness of our Internal Control Framework and our key policies and identified appropriate remediations	**Control environment:** for 2016/ 17, we plan to formalise our monitoring mechanisms for both our Internal Control Framework and our key policies

POL00423565

Appendix 2: Risk Extracts from the draft 2015/ 16 Annual Report – Principal Risks

Points to consider:

- descriptions for changes in risk profile
- direction for changes in risk profile.

These are our principal risks, detailed with their potential impact and how the Post Office manages them, plus trends of changes to the risk profile from last year.

Any of these risks could have a material impact on our results, condition and prospects. However, these risks should not be regarded as a complete and comprehensive statement of all potential risks; some risks are not yet known and some that are not considered material could later turn out to be material.

Potential risks **Description of risk and causes**	**Consequences**	**Change in Risk Profile**	**Key Mitigations** **Details of risk management and mitigation**
STRATEGIC RISKS			
Competitive threat Post Office faces both opportunities for and threats to income from our competitive market place. - The Mails and parcels market remains intensely competitive and has seen some high profile failures due to inadequate margins. - Government Services are impacted by increased use of digital channels and reduced public spending. - Financial Services is a challenging market where responding quickly to different strategies, business models, and products is essential to growth.	This could result in not achieving our growth objectives, losing market share and revenues.	Increasing competition across the markets in which Post Office operates leads to an increasing risk profile	• Competitor impact tracked and customer perceptions used to inform our decisions. • Our strategy is focussed on customer requirements, utilising new technology to help us introduce customer centric propositions backed by robust distribution channels. • Each product proposition has a tailored strategy and business diversification provides different response options if there is significant threat to one business area.
Dependency on strategic relationships Post Office has strategic relationships which are key to its product offering and growth, for instance with Royal Mail Group and Bank of Ireland. Misalignment with our strategic partners could result in products that do not support our growth strategy or meet our customer or market requirements.	This could result in not achieving our growth objectives, losing revenue and market share.	Risk profile is unchanged	• Close working relationships established with our strategic relationships. • Scheduled interactions with our strategic partners to improve the product offering and service to drive growth and profitability for us and them. • Contractual arrangements monitored to ensure they provide value and security.
TRANSFORMATION RISKS			

POL00423565

Benefits from business transformation not realised Planned for savings from our transformation programme may be delayed or not achieved, or overall service compromised, due to inadequate capability, capacity and the scale of change.	This could result in not achieving our growth objectives, loss of revenue and cost savings, reduced customer satisfaction and damage to reputation with stakeholders.	Risk profile is unchanged	• Programme management office established, with assurance oversight. • Detailed plans in place to manage the transformation, and identify risks to ensure transformation activities are delivered within budget and on time. • Benefits are tracked from inception to delivery and into business as usual operations through formalised reviews during the lifecycle.
IT transformation not delivered in full Our programme of IT transformation may not be delivered in full due to the level of complexity of replacing legacy IT and simultaneously implementing new integrated service model	This could result in systems and infrastructure that are not fit for purpose, may add costs and lead to business interruption.	Risk profile is unchanged	• Developed and monitoring the implementation of our Strategy and Integrated Service model. • Programme teams and operational business teams work closely to ensure that the objectives of the strategy are delivered. • Transformation assurance and oversight plan in place.
Industrial action Continued progress has been made in industrial relations, however the withdrawal of support from our staff or postmasters to the ongoing implementation of Post Office strategy via industrial action remains a risk.	This could result in business disruption leading to loss of revenue, reduced customer satisfaction and brand damage.	Risk profile is unchanged	• Well defined agreements with relevant unions. • Comprehensive engagement programme in place with staff, unions and postmasters so as to ensure that there is alignment with our vision and strategy around transformation. • Contingency planning in place to minimise the impact of potential industrial action.

OPERATIONAL RISKS			
Lack of appropriate capability The Post Office is dependent on its dedicated work force to meet the expectations of its customers and stakeholders. The ability to continue to attract, motivate, develop and retain people is key to its success.	This could result in not achieving our strategic objectives and loss of staff engagement.	Risk profile is unchanged	• Continue to review our organisational structure to ensure it evolves and supports our requirements. • Operate a capability heatmap to identify key capabilities for our current and future state needs. • Continued investment in developing our people.
Decline in customer experience If we are unable to deliver an attractive customer experience, via our products, service and channels, we risk losing the support of our customers.	This could result in reduced customer satisfaction and brand reputation, with consequential loss of market share and revenues.	Increasing customer expectations and competitive pressures in the market mean the risk profile is increasing	• Our customer strategy is continually monitored to ensure that it meets changing customer product and service expectations and reflects current market and competitor trends. • Our channel strategy ensures we meet the changing customer requirements for access and utilises available and emerging technology to reflect changing customer needs.
Unattractive network proposition	As well as loss of revenue, this	Risk profile is unchanged	

POL00423565

As we transform, there is a risk that the Post Office may not be able to retain, or attract sufficient new, retail partners because of the complexity of our network proposition and lack of profitability for a retail partner.	could result in shrinkage to our network and breach our public purpose commitment.		• Branch level proposition designed to provide appropriate profitability for our retail partners. • New branch model also ensures that we use modern technology to drive efficiency and cost reduction for operators, as well as a better customer experience. • Branch model continually reviewed and updated to ensure we support our retail partners and are attractive to new ones.
Business interruption and cyber threat Post Office is dependent on the continued availability of its information systems and associated infrastructure. These could be threatened, either due to internal issues, external events or cyber attack.	This could result in disruption of service leading to negative customer experience, breach of contractual obligations and brand damage.	Risk profile is unchanged	• Business continuity plans are updated through review, testing and enhancements. • New contracts have provisions covering the security, resilience and availability of our IT systems and infrastructure. • Robust policies are in place to cover information security, with continuous improvements where required. • Rigorous schedule covering penetration testing to assess and improve the security of our systems.
Dependency on third parties Post Office works in partnership with a number of third parties to deliver high quality services. These depend upon us successfully selecting, contracting and monitoring our key in-source or out-source relationships and avoiding any unintentional breaches of contractual terms.	This could lead to business interruption and additional costs through failure to meet contractual obligations.	Post Office actions to deliver separation from Royal Mail and revised partnership structures means risk profile is decreasing	• Contract management framework to monitor our contracts and suppliers. • Assessment of risks and ensure monitoring of mitigating actions. • Defined key policies that we require our suppliers to comply with and attest to compliance.

FINANCIAL RISKS			
Stakeholder funding The cost of delivering the public purpose of the Post Office and meet the expectations of stakeholders may exceed current forecasts.	This could result in not achieving our growth objectives, failing to meet our public purpose commitment and damaging our reputation with stakeholders.	Risk profile is unchanged	• Proactive engagement with stakeholders to ensure there is full understanding of, and alignment with, the strategic goals and the investment case required to deliver them. • Annual and three-year operating and capital plans developed and risk assessed. • Scheduled feedback to stakeholders and review.
Financial reporting and controls failure Our financial controls are fundamental to delivering our fiduciary responsibilities, management information, financial reporting and compliance with accounting and	This could result in loss of revenue, increased costs, financial misstatement and damage to	Increased regulatory requirements across the markets in which the Post Office operates	• Defined and structured delegation of authority which is reviewed and approved by the Board. • A Financial and Accounting manual and a framework of supporting general controls – see Our Control Framework on page SSS. • Documented financial controls, with additional assurance to be provided

POL00423565

governance standards. These may not operate effectively if they are not documented, reviewed and monitored regularly.	reputation with stakeholders.	mean the risk profile is increasing	from a Control Self-Assessment process.
Pension cost increases The cost of servicing the current Defined Benefits scheme could become unbearably onerous as a result of the prolonged low interest rate environment, resulting in substantially increased contributions.	This could result in material increases in required contributions, adversely affecting our ability to achieve commercial sustainability.	Economic conditions relating to the cost of servicing schemes means the risk profile is increasing	• Valuation assumptions and pension funding strategy have regular external and internal monitoring and review. • Working with professional advisors to develop options to minimise the impact of an adverse valuation. • Consultation process is currently underway on options for the future of the Defined Benefit plan. • Alternative de-risking plans can be investigated if required.
LEGAL & REGULATORY RISKS			
Financial regulatory breach	This could result in regulatory censure, fines, litigation or curtailment of trading, which could damage our reputation with customers and suppliers.	Increasing regulatory requirements across the industries in which the Post Office operates means the risk profile is increasing	• Corporate services works closely with the relevant business owners to identify new regulatory obligations. • On-going training to our staff on legal and regulatory matters. • Regular compliance tests and monitoring are conducted. • Programme in place of internal and external assurance (including by our regulatory principals) including in relation to our financial services business, its sales practices and products to ensure that on an ongoing basis these continue to meet regulatory requirements.

POL00423565

5) Policy Approval

Author: Mark Rodgers Sponsor: Mike Morley-Fletcher Meeting date: 05 May 2016

Executive Summary

Context

Policies are a fundamental part of our General Control Framework. We use them to articulate our intent, setting clear rules and expectations, to communicate how we want to standardise and monitor specific activities and behaviours. They also enable us to evidence our intentions to third parties, for instance business partners, suppliers and regulators. We have a Policy Framework to ensure 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.

On a regular basis we review the framework of policies and Policy owners review the content to ensure both are up to date and relevant for our needs. The proposed Framework for our most important policies is included in paper 4b) appendix 3, Key Policy Framework, and review work has been progressing on theses polices. At this stage seven key policies are presented for RCC approval (five from CS and one from IT and one from HR) and subsequent presentation to the ARC.

RCC is asked to review these policies, invited to provide feedback and comments, with the intention of ratifying these seven key policies submitted for approval. Once approved the policies will need to be implemented by the policy Owner, including monitoring of performance and compliance.

Questions?

a) Can RCC ratify the seven policies we have developed or revised?
b) How will we manage subsequent implementation of the policies?
c) What lessons have we learnt so far?

Conclusion

a) Seven policies have been reviewed and where necessary revised. They have been signed off by policy Owner and are ready for approval by RCC and ARC. A summary of the policies is attached (see appendix 1) along with the policy documents (see appendix 3 - 9).
b) Once approved policies will need to be implemented. This will involve deciding where they should be stored, how they should be communicated and supported with training, how they should be controlled, monitored and reviewed. This is the primary responsibility of the policy Owner, but will be supported and monitored by the central Policy Manager. Further details of what this requires is provided in appendix 2, Policy Implementation Process.
c) In addition, we are identifying lessons learnt from our review of phase 1 polices and these will be used to assist policy Owners during phase 2.

Input Sought

RCC is asked to review this paper and invited to provide feedback and comments. In particular to:
a) Ratify the seven key policies submitted for approval, and
b) Consider the requirements for implementation.

Appendices

Appendix 1: Policy Approval – Summary of policies and rationale
Appendix 2: Policy Implementation Process
Appendix 3 - 9: Policy Approval – Copies of documents

POL00423565

Appendix 1: Policy Approval – Summary of policies (7) and rationale

Ref	Key Framework Policy	Sponsor (GE Owner)	Policy Owner	Why is this policy needed?	Approved by?	How will the policy be implemented?	How will policy compliance be monitored?
12) (PBA)	Financial Crime	Jane MacLeod	John Scott	To help Post Office meet legal and regulatory obligations within appetite, and to manage financial crime risks reducing actual loss, avoiding potential losses.	RCC and ARC May 2016	Proposal for process to implement policies, including: • where they should be stored • how they should be communicated and supported with training • how they should be controlled, monitored and reviewed. Please refer to appendix 2 for more details.	1. Policy Compliance Manager will coordinate, and ensure QA standards, including compliance monitoring. 2. Policy Owner undertakes compliance, and will identify measures, develop monitoring processes, track results and provide reporting with MI to the relevant governance body.
13) (PBA)	Anti-Bribery and Corruption (incl. Gifts & Hospitality)	Jane MacLeod	Ben Foat	To help Post Office meet its legal and regulatory obligations within appetite, to help manage ABC risks, and support good conduct standards in all dealings.	RCC and ARC May 2016		
14) (PBA)	Anti-Money Laundering (incl. Counter Terrorism, Sanctions)	Jane MacLeod	John Scott	To help Post Office meet its legal and regulatory obligations within appetite, and to help manage AML (CTF and Sanctions) risks whilst reducing actual loss, and avoiding potential losses.	RCC and ARC May 2016		
17) (PBA)	Business Continuity	Jane MacLeod	Jonathan Waples	To embed a framework to identify potential threats to business continuity, and to help manage impacts to business operations. It is a set of standards which support resilience and sets out the capabilities to respond.	RCC and ARC May 2016		
25) (PBA)	IT Disaster Recovery	Alisdair Cameron	Stephen Hayes	To embed a framework to identify potential threats to disaster recovery, and to help manage impacts to IT/ business operations. It is a set of standards which support resilience and sets out the capabilities to respond.	RCC and ARC May 2016		
26) (PBA)	Talent and Resourcing: HR Vetting	Neil Hayward	Sean Leahy	To ensure Post Office operates vetting processes in a legal, and compliant way. To embed standards to control and reduce the risks of error, theft, fraud or misuse of facilities. To ensure Post Office engages with suitable workers.	RCC and ARC May 2016		

5)	Whistleblowing	Jane MacLeod	Nisha Marwaha	To help Post Office meet its legal and regulatory internal and external obligations. To implement good practice and engender good standards in this context.	RCC and ARC May 2016	As above	As above

POL00423565

Appendix 2: Policy Implementation Process

These are the steps we identified for planning and monitoring implementation of policies. They will be trialled with CS polices before being recommended to other business areas. An estimated timeline of 6 months has been used.

Implementation Steps	Details	Example timeline (estimated at 6 months)
1) Establish accessible storage and maintenance protocols	❑ Publish documents to SharePoint ❑ Update Intranet and links (checking searches) ❑ Define maintenance	By 31/05/16
2) Communicate policy and requirements	❑ Agree audience (for communication and training) ❑ Develop communications policy and messages ❑ Communicate policy and requirements	By 30/06/16
3) Develop and deliver supporting training	❑ Identify resources and compile modules/ materials (Learning Academy) ❑ Coordinate and deliver training ❑ Publish to SharePoint	Develop by 31/07/16, deliver by 31/08/16
4) Identify and develop associated controls	❑ Confirm associated controls framework and catalogue controls library ❑ Create matrix of responsibilities (include RACI if required) ❑ Confirm controls operating as expected	Identify by 30/06/16, develop by 31/08/16
5) Monitor and measure compliance	❑ Identify and define compliance monitoring procedures, systems and controls ❑ Identify measures and test monitoring plans ❑ Commence monitoring routines ❑ Capture results, evaluate, define management information and report to governance committees	By 30/10/16
6) Review policy	❑ Use monitoring results to evaluate current policy controls and continuing appropriateness of policy ❑ Maintain policy review log ❑ Conduct annual/ bi annual policy reviews and report to relevant governance body	By 31/12/16

POL00423565

Appendix 3 - 9: Policy Approval – Copies of documents (7)

These policies have been reviewed and signed off by policy Owners. Six have been provided to the Banking partners and Whistleblowing has been updated. They are presented to the RCC/ ARC for approval.

POL00423565

Post Office Financial Crime Policy

POL00423565

Contents Page

Contents Page 2
Document Control Sheet 3
Section A. Introduction 4
Section B. Context 5
About this Policy 5
What is financial crime? 5
Risk Appetite 6
How we manage financial crime 6
Who is responsible 7
Who must comply and how 7
Section C. Policy Details 8
Information 8
Our Controls 8
Section D. Governance 10
How do we monitor compliance 10
How to raise a concern 10
Contact us and more information 10
Section E Key Terms and References 11
Key Terms 11

POL00423565

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 V0.6	Annually from policy effective date	19th May 2016	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

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)	5 May 2016
Board Committee	Post Office Audit, Risk and Compliance Committee (ARC)	19 May 2016

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.	No later than 19th May 2017

POL00423565

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 is directly related to this code ensuring 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 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 management of financial crime to the Board of Directors. Post Office's Audit, Risk and Compliance Committee considers financial crime as a standing agenda item and the Post Office Board is updated on a regular and timely basis.

POL00423565

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.

Failure to comply with the requirements of this policy by any person 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 refers to permanent staff, temporary including agency staff, contractors and consultants.

Financial crime risks are reviewed with relevant individuals on a regular basis and at least quarterly. This policy's effective date is 19th May 2016.

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.

POL00423565

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:

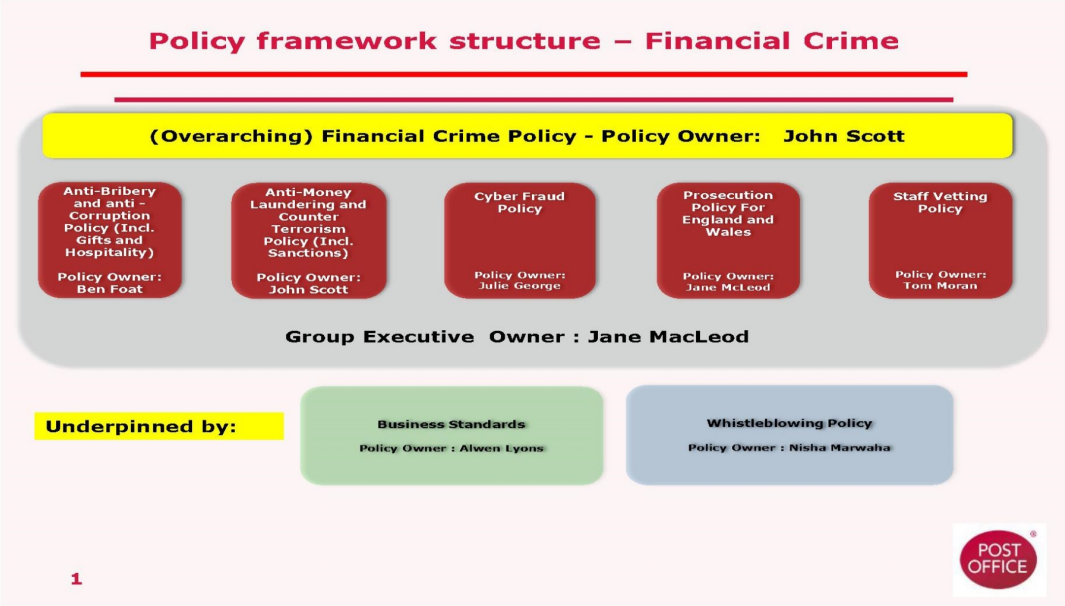
- Any dishonest or fraudulent act,
- Profiteering as a result of insider knowledge of Post Office activities,
- Theft of assets from Post Office or its customers,
- Manipulation of transactional data at Point of Sale,
- False expense or payroll claims,
- Manipulation of Post Office accounts or financial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

Risk Appetite

Post Office has an averse appetite for regulatory and legal risks. This policy reflects this and sets out controls to reduce and/ or mitigate financial crime risks.

How we manage financial crime

This policy is one of Post Offices key policies forming a broad suite of Financial Crime 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. .



POL00423565

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 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 Security and Financial Crime (MLRO) is the policy Owner, who is responsible for the day to day implementation of and compliance with this policy, and is accountable to the General Counsel, and
- The Senior Security Manager, Financial Crime is the policy Implementor who is responsible for the day to day implementation of the policy lifecycle (including monitoring) and is responsible for and accountable to the policy Owner for reporting all policy matters.

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 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 Head of Security and Financial Crime (MLRO).

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.

POL00423565

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
- 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

- All 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 mitigating controls aligned to the inherent risk must be put in place.
- The head of each Business Unit must confirm annually that a formal risk assessment has been undertaken and that adequate controls are in place in accordance with Post Office's central Risk Management Framework.
- Business Units must consider both internal and external risks and past experience (including any litigation), 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 the Head of Security and Financial Crime.

POL00423565

- Each Business Unit must have processes in place for managing and reporting both internal and external financial crime incidents. These processes must be in line with the Post Office's central risk team's reporting requirements.
- 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 will take all reasonable measures to prevent, deter and detect all 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 all third parties, 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. Details of losses and the cause of the loss will be reported regularly to the Post Office ARC by the General Counsel.

POL00423565

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. In addition, Internal Audit will periodically test compliance with 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 Board 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 suspects dishonest or fraudulent activity 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 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 GRO

POL00423565

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: 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

POL00423565

Post Office Anti-Bribery and Anti-Corruption Policy

(Incorporating: Gifts & Hospitality Policy)

POL00423565

Contents Page

Contents Page 2
Document Control Sheet 3
Section A. Introduction 4
Section B. Context 5
About this Policy 5
What is Bribery and Corruption? 5
Risk Appetite 6
How we organise ABC risk management 6
Who is responsible 7
Who must comply and how 7
Section C. Policy Details 9
Information 9
Our Controls 11
Section D. Governance 14
How do we monitor compliance 14
How to raise a concern 14
Contact us and more information 14
Section E. Key Terms and References 15
Key Terms 15
References 15
Appendix 1 – Post Office Gifts & Hospitality Policy 17
Approvals Procedure 17

POL00423565

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:**
Final V1.5	Annually from policy effective date	19th May 2016	Z:\NEW COMPLIANCE\New Policy Framework 2015\Refreshed Policies 2016

DOCUMENT REVISION HISTORY			
Version	**Date**	**Author**	**Reason For Change**
Draft v1.4	30th March 16	**Jane MacLeod**	Sponsor review and sign – off
Final v1.5	30th March 16	**Ben Foat**	Policy Owner final review and sign off

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)	5 May 2016
Board Committee	Post Office Audit, Risk and Compliance Committee (ARC)	19 May 2016

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.	No later than 19th May 2017

POL00423565

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 is directly related to this code ensuring the highest standards of ethics 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 on a regular basis.

POL00423565

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 on a regular basis and at least at quarterly 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.

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; and
- 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 the appendices, assist Post Office in preventing and detecting corrupt conduct and form an essential component of Post Office's adequate procedures.

POL00423565

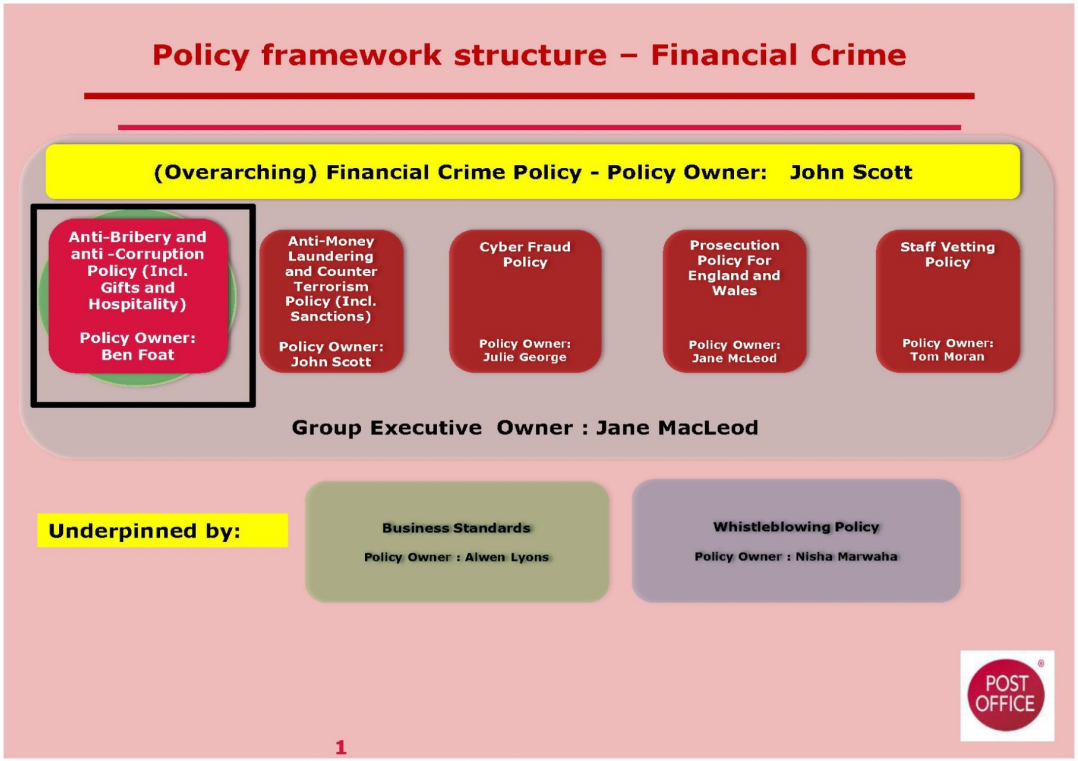
Post Office Ltd must also comply with particular regulatory obligations arising through contracts with directly regulated companies or directly through its subsidiary, Post Office Management Services (POMS). As an Appointed Representative of each of the Bank of Ireland and POMS, Post Office Ltd is contractually 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 this regulatory obligation.

Risk Appetite

The Post Office risk appetite is averse for not complying with law and regulations or deviation from its business conduct standards. Post Office is therefore intolerant of bribery and corruption risks (i.e. Post Office has zero tolerance). 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)

POL00423565

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; and
- 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; and
- 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.

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.

POL00423565

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 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.

POL00423565

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.
- 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; and
- Associated Parties, which include persons or entities that perform services for or on behalf of Post Office.

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; and
- Charitable Donations.

POL00423565

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

The specific types of ABC risks can be classified as:

Payment Risks – arising from, for example, charitable or political donations, facilitation payments, gift and entertainment, client training programs and ex gratia/ legal settlements. Payment risks include:

- 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 Entertainment (G&E): As these are part of corporate life, it is important that such G&E 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&E Policy annexed to this Policy;
- 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;
- Client training programs: 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&E, the training provided should not be excessive or lavish. Records of any training should be kept by the relevant business areas;
- 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. There must be no perceived inducement for the purpose of improperly obtaining or retaining business or securing an advantage for Post Office; and
- Ex gratia payments/ legal settlement: an ex gratia payment or a legal settlement is the usual 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.

POL00423565

Third Party/ Associated Party Risks – arising from third parties who provide services on behalf of Post Office and engage in bribery and corruption while performing those services. The scope of this would include, for example, agency operators within the Post Office network as well as suppliers who are procured through the Procurement Team. Examples of Associated Parties include agents, consultants, suppliers, introducers, and intermediaries. Before engaging with an Associated Party, the business area and employee should:

- Undertake a risk assessment and due diligence on the proposed Associated Party to determine the ABC risk profile of the Associated Party; and

- When undertaking the ABC risk assessment and due diligence consider whether there are any red flags or heightened risks arising from that assessment.

Employment Risks – arising from Post Office employees breaching ABC legal and regulatory requirements by requesting something of value from a third party in exchange for providing employment or a work opportunity at Post Office or providing work opportunities, paid or unpaid, to Connected Individuals (see Section E for definition of this term) with the purpose of improperly obtaining or retaining business or securing an advantage for Post Office.

Post Office employs a merit based approach in its hiring of staff. 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. 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.

Our Controls

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.

POL00423565

Business areas systems and controls

All business areas must ensure that they have in place adequate systems and controls to comply with this policy and manage bribery and corruption risks including:

Specific ABC Controls	Description
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 the following specific issues are incorporated into the design, management and implementation of its ABC processes and procedures: • Payment Risks – arising from, for example, charitable or political donations, facilitation payments, gifts & entertainment, and client training. • 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 would include agency operators within the Post Office network and suppliers procured through the business or through the Procurement Team. • Employment Risks – arising from Post Office employees breaching ABC legal and regulatory requirements by 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.
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: • Payment Risks – as set out in Section C and including the Gifts and Entertainment process which is set out in Appendix 1 of this Policy. • 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. In addition, each business area must identify, escalate and resolve any heightened risks arising from the ABC risk assessment and due diligence. Examples of these heightened risks include: ○ Remuneration which is not proportionate with the services being rendered or consistent with the market or relevant industry.

POL00423565

	○ 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. • Each business area is required to ensure that the relevant mandatory ABC contract clauses are included in the agreement with that party. Please liaise with Legal and Procurement Departments to ensure that all contracts include the appropriate ABC clauses. • Employment Risks – such assessment should include, for example, identifying employment and work opportunity risk, identifying relevant connections, managing candidates for employment with relevant connections, managing employee disclosure of relevant connections, identify and managing a risk based and proportionate PEP screening, bonus and compensation structures are based on objective and merit-based grounds and do not incentivise an employee to improperly exploit their relevant connections, and managing requests for work opportunities from external stakeholders.[1]
Incident reporting, response and recording	Each business area 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 in all cases escalated to the Central 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.
Risk Indicators	Each business area is to escalate existing and new bribery and corruption risks to the head of that area who shall, in turn, inform the Central Risk team. The Central Risk team determines the risk indicators and MI required.
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.
Audit	Each business area should test the effectiveness of its processes to ensure that the Post Office is able to monitor the application and effectiveness of this Policy and its controls.

13

POL00423565

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. In addition, Internal Audit will periodically test compliance with 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 Board 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

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** Ben Foat Head of Legal – Financial Services on **GRO** or by email at **GRO**

POL00423565

Section E. Key Terms and References

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
Whistleblowing 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 can contact Post Office's General Counsel, Jane MacLeod who can be contacted by email on: GRO or by telephone on: GRO 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.
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

POL00423565

	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.

POL00423565

Appendix 1 – Post Office Gifts & Hospitality Policy

Approvals Procedure

Gifts

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, such as when giving or receiving a gift from an overseas postal administration in an official capacity as a representative of Post Office, 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@postoffice.co.uk

Register of Gifts

The Central Risk team maintains a Register of all Gifts given and received over £20.

Hospitality - Purpose

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.

Hospitality – Practice and Register of Hospitality

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

POL00423565

location of the hospitality and the cost per person, along with the written approval from your line manager, to the Central Risk team at GRO ;

- The Central Risk team maintains a Register of all Hospitality given and received.

Hospitality – Awareness and Reporting

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.

POL00423565

Post Office Anti-Money Laundering and Counter Terrorist Financing Policy

POL00423565

Contents Page

Contents Page 2
Document Control Sheet 3
Section A. Introduction 4
Section B. Context 5
About this Policy 5
What is AML and CTF? 5
Risk Appetite 6
How we organise AML/CTF management 6
Who is responsible 6
Who must comply and how 7
Section C. Policy Details 8
Information 8
Our Controls 9
Section D. Governance 14
How do we monitor compliance 14
How to raise a concern 14
Contact us and more information 14
Section E Key Terms and References 15
Key Terms 15

POL00423565

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 V2.8	Annual (from effective date	19th May 2016	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

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)**	5th May 2016
Board Committee	**Post Office Audit, Risk and Compliance Committee (ARC)**	19th May 2016

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.	No later than 19th May 2017

POL00423565

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 is directly related to this code ensuring the highest standards of fraud prevention, detection and management are maintained.

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 and Risk Committee considers AML and CTF matters as a standing agenda item and the Post Office Board is updated on a regular basis.

POL00423565

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 and it is a set of standards to minimise the likelihood of regulatory breach. This policy is effective from 19th May 2016.

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.

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

POL00423565

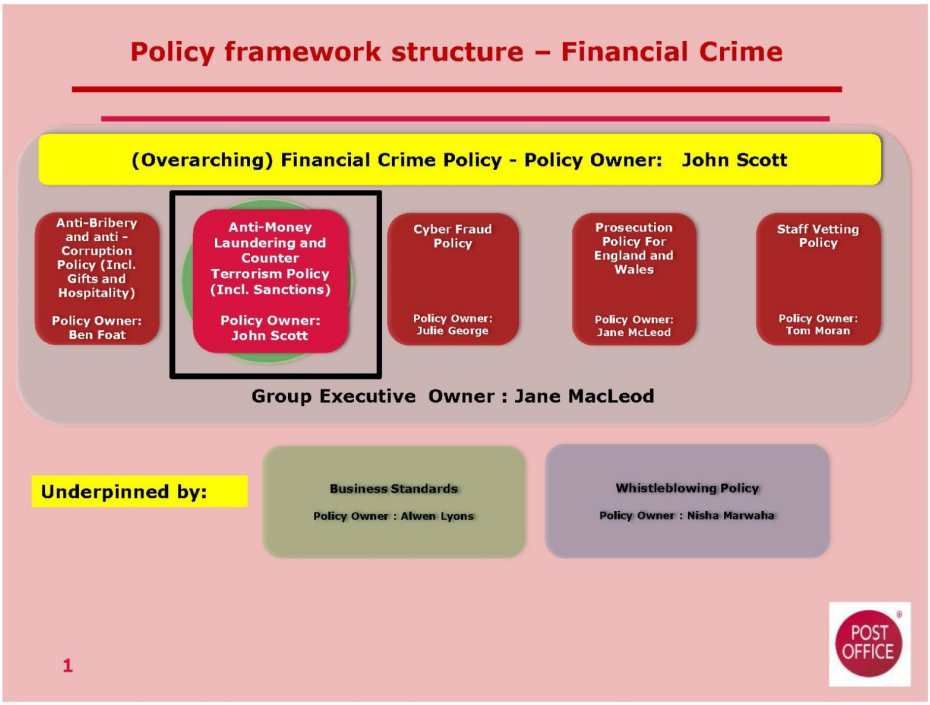
suspicious activity, provide appropriate AML/CTF training for relevant individuals, and maintain adequate transaction records.

Risk Appetite

Post Office has an averse appetite for regulatory and legal risks. This policy reflects this and sets out controls to reduce and/or mitigate AML/CTF 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 Financial Crime through reports to its committees – principally to the Board Audit, Risk & Compliance Committee ('ARC'). The key individuals and their specific responsibilities in relation to this policy are:

POL00423565

- The General Counsel who is a member of the Post Office Executive is the policy Executive Owner and policy Sponsor, accountable to the CEO and to the Post Office Board overall,
- The Head of Security and Financial Crime (MLRO) is the policy Owner who is responsible for the day to day implementation of and compliance with this policy and reports to the General Counsel, and
- The Senior Security Manager, Financial Crime is the policy Implementor who is responsible for and accountable to the policy Owner for the day to day implementation of the policy lifecycle (including monitoring).

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 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 Policy Owner, the Head of Security and Financial Crime.

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.

POL00423565

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.

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 unless he has in place procedures for:

- Obtaining satisfactory evidence that the client is the person he claims to be,
- Keeping records of the identity of those clients and the transactions carried out by them for a least five years,
- Training staff on the firm's preventative procedures and about spotting money laundering; and
- The reporting of suspicions of money laundering and designating a Nominated Officer to whom internal reports may be made.

Failure to put such procedures in place 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.

POL00423565

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,
- Screening all direct customers of Post Office and their transactions for potential financial sanctions breaches, and
- Monitoring regulated transactions and periodically 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 at all times a relevant policy supported by appropriate procedures 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 paragraph and 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

POL00423565

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 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
  - Identity and source of wealth information will be obtained and verified for any PEPs
  - Post Office will record and validate the business relationship with the customer to be on-boarded including:

POL00423565

- The nature and details of the business
- The source and origin of funds
- The relationship with an ultimate beneficial owner (UBO)
- 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** - Money Laundering Regulations dictate that Post Office monitors all PEP relationships 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

POL00423565

- **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 and is are able to delay it for seven working days without arousing the suspicion of the customer

- **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

  Records relating to customers with whom a business relationship exists should be retained for 5 years after the business relationship ceased.

  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

POL00423565

- **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.

POL00423565

Section D. 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. In addition, Internal Audit will periodically test compliance with 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 0845 6034004.

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 GRO

POL00423565

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)

POL00423565

Post Office

Business Continuity Management Policy

POL00423565

Contents Page

Contents Page 2
Document Control Sheet 3
Section A. Introduction 4
Section B. Context 5
About this Policy 5
What is Business Continuity? 5
Risk Appetite 5
How we organise Business Continuity Management 5
Who is responsible 7
Who must comply and how 7
Section C. Policy Details 8
Information 8
Our controls and arrangements 8
1. Baseline and on-going Business Continuity objectives 8
2. Satisfying BCMP Requirements 9
3. Approach to Managing Risk & Audit Requirements 10
4. Continual Service Improvement 11
Section D. Governance 12
How we monitor compliance 12
How to raise a concern 12
Contact us and more information 12
Section E. Key Terms and References 13
Key Terms 13
References 13

POL00423565

Document Control Sheet

POLICY SUMMARY			
GE Policy Sponsor	Policy Owner	Policy Implementor	Policy Approver(s)
General Counsel **Jane MacLeod**	Business Continuity Manager **Jonathan Waples**	Business Continuity Manager **Jonathan Waples**	Post Office **RCC and ARC Committees**
Version and Status:	Policy Review Period	Effective from :	Policy location:
Final - V0.7	Annually from policy effective date	19th May 2016	Z:\NEW COMPLIANCE\New Policy Framework 2015\Refreshed Policies 2016

DOCUMENT REVISION HISTORY			
Version	**Date**	**Author**	**Reason For Change**
Draft v0.6	21/03/2016	**Mike Morley-Fletcher**	Head of Risk sign – off /readiness Review
Final v0.7	30/03/2016	**Jane MacLeod**	Final review, sponsor sign off

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)**	5 May 2016
Board Committee	**Post Office Audit, Risk and Compliance Committee (ARC)**	19 May 2016

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.	No later than 19th May 2017

POL00423565

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 is directly related to this code ensuring the highest standards of business continuity 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 Business Continuity Manager, 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 business continuity management framework to the Board of Directors. Post Office's Audit, Risk and Compliance Committee considers business continuity as a standing agenda item and the Board is updated on a regular and timely basis.

POL00423565

Section B. Context

About this Policy

The purpose of this document is to define Post Office's policy with regard to business continuity management that is appropriate to the aims and objectives of Post Office. This includes:

- A framework for:
  - setting business continuity objectives;
  - satisfying appropriate requirements;
  - continual improvement of the Business Continuity Management Programme; and
- A high level statement of our key controls in respect of business continuity.

The Policy is consistent with business continuity "ISO22301", which are the Business Continuity Institute's Good Practice Guidelines.

Policy Scope: It is important to understand which areas of the business currently fall under the protection of the policy, and which do not. The boundaries of the Post Office business continuity framework are detailed within a separate document, "Business Continuity Context, Requirements and Scope", and these documents should be reviewed together when assessing a BC response requirement.

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

What is Business Continuity?

Post Office adopts the Business Continuity Institute's Good Practice Guidelines definition of business continuity as: *"A holistic management process that identifies potential threats to an organisation, and the impacts to business operation those threats, if realised, might cause, and provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities."*

Risk Appetite

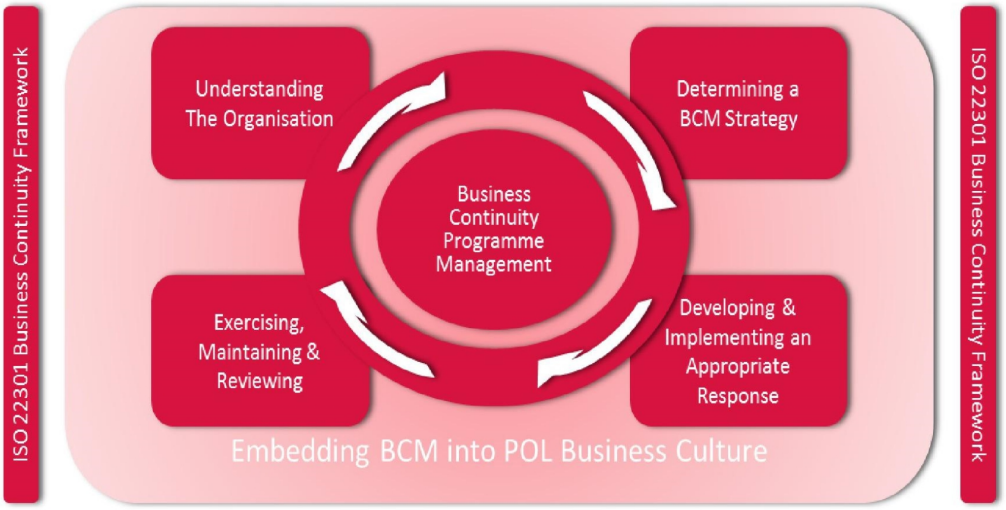
Post Office has an averse appetite for business continuity risk. Post Office recognises that it cannot completely eliminate this risk. However, this policy sets out controls to reduce and/ or mitigate such risks.

How we organise Business Continuity Management

This policy describes Post Office's Business Continuity Management policy and should be read in conjunction with other Post Office resilience, health & safety, and physical security related policies and procedures.

POL00423565

The BCM Framework



This Business Continuity Management Policy is stored electronically, and is available to all relevant stakeholders within the organisation.

POL00423565

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 business continuity by reports from its committees including its ARC Committee. The key individuals and their specific responsibilities in relation to this policy are:

- The General Counsel is a member of the Post Office Executive team and is the Group Executive Owner and policy Sponsor, accountable to the Board.
- The Group Business Continuity Manager is the Policy Owner who is responsible for the day to day implementation of and compliance with this policy and is accountable in this regard 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. 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 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 Investigations Policy. If the cause is found to be due to wilful disregard or negligence, it will be treated as a disciplinary offence.

POL00423565

Section C. Policy Details

Information

Post Office recognises the need to ensure that our business operates safely, smoothly and without interruption for the benefit of our colleagues, customers, shareholders and other stakeholders.

To ensure such levels of safe, continuous operation, Post Office has implemented a Business Continuity Framework consistent with "ISO 22301".

The operation of a Business Continuity Framework has many benefits for Post Office, including:

- The safe-guarding of colleagues at times of duress;
- Ensuring the supply of goods and services to our customer; Protection of revenue streams and business profitability;
- Maintenance and enhancement of shareholder / stakeholder value; and
- Compliance with legal and regulatory requirements.

In addition, our Business Continuity Framework is a commitment to the development, maintenance, improvement and socialisation of a Business Continuity Management Programme within and across the organisation.

Our controls and arrangements

1. Baseline and on-going Business Continuity objectives

The baseline objectives for business continuity within Post Office are defined within the "Business Continuity Context, Requirements and Scope" document. These are fundamental steps required which are led by business areas and are not subject to frequent change.

These baseline objectives guide the setting of lower level detail for short-term objectives for business continuity planning arrangements within an annual cycle. They coincide with the organisational budget planning. This ensures that adequate funding is obtained for necessary activities identified in the previous cycle.

These business continuity objectives will be documented in the Business Continuity Management Plan ("BCM Plan"), produced each financial year, which will also identify how objectives will be achieved, over what estimated period, and at what level of estimated cost. Once the annual BCM Plan is approved by the Post Office Risk and Compliance Committee it will be subject to regular management review to ensure that its objectives remain valid.

Amendments to objectives will be managed through the standard Post Office change management process.

POL00423565

2. Satisfying BCMP Requirements

Senior Managers commit to the provision of the appropriate resources to establish and develop the Business Continuity Management Programme ("BCMP").

Systematic performance review of the programme. This is conducted by the Business Continuity Manager on a regular basis, ensuring that quality objectives are being met. Qualitative evaluation is undertaken and any issues identified through the audit programme and management processes. Management review includes departmental and other management meetings.

Business Continuity Management Quality System. The Business Continuity Manager has overall authority and responsibility for this and implements and manages the system carrying out the following:

- The identification, documentation and fulfilment of applicable requirements;
- Assigning authorities and responsibilities for the implementation, management and improvement of the BCMP;
- Integration of business processes with the BCMP;
- Compliance with statutory, regulatory and contractual requirements in the management of assets used to deliver products and services; and
- Reporting to senior management on performance and improvement of the BCMP

Role definition and responsibilities are reviewed by the Business Continuity Manager to ensure that colleagues understand the roles they are required to fulfil, and that they have the appropriate skills and competences to do so. These controls are necessary to ensure the continued BCMP success and to mitigate risk.

Post Office will ensure that colleagues involved with the BCMP are competent on the basis of appropriate education, training, skills and experience. The skills are required to ensure business continuity will be determined and reviewed on a regular basis, together with an assessment of existing skill levels within Post Office. Training needs will be identified and executed via individual's training plans maintained to ensure that competences are in place.

Full details of the business continuity responsibilities associated with each of the required roles, and how they are associated within Post Office are given in a separate document, "Roles, Responsibilities and Authorities".

Use of third parties. Post Office uses third parties, both internal and external, in the delivery of products and services. Where this involves the operation of a business process, or part of such process, that falls within the scope of the BCMP, then this should be identified by the Business Continuity Manager within the annual Business Continuity Management Plan.

Post Office retains governance of the relevant business continuity management processes for third parties by demonstrating:

- Accountability for the process;

POL00423565

- Control of the definition of, and interface to, the process;
- Performance and compliance monitoring; and
- Control over process improvements.

This will be evidenced by documentation and records, including contracts, meeting minutes and performance reports.

Third party agreement contractual business continuity terms. Specific, high level, requirements for new and existing relationships will be made available to associated third parties by the relevant third party relationship manager. These requirements set out minimum expectations for service continuity provision (as appropriate to the contractual service level terms). For further information see "Supplier Business Continuity Evaluation Process".

3. Approach to Managing Risk & Audit Requirements

The risk management strategy defined under ISO 22301 requires that relevant assets are identified and the following considerations made:

- Threats;
- Vulnerabilities;
- Impact & likelihood before risk treatment;
- Risk treatment (e.g. reduction, removal, transfer);
- Function responsible/ owner; and
- Timescale and review frequency.

Risk management will occur at multiple levels within the BCMP, including but not restricted to:

- Business continuity management planning – risks to the achievement of objectives;
- Business Continuity risk assessment;
- Assessment of the risk of changes under the established business change model; and
- At the project level as part of the management of significant business change.

High level risk assessments will be reviewed annually, or upon significant change to the business environment. More detail on the approach to risk assessment can be found in the document "Risk Assessment Process".

Regular reviews must take place concerning how well business continuity management processes and procedures are being observed. These occur at two levels:

- Structured regular management review of conformity to policies & procedures within Post Office; and
- Internal audit reviews against the ISO 22301 standard by the Post Office Internal Audit Team.

POL00423565

Certification auditing. Additionally, should certification to ISO 22301 be sought and attained, a third audit level applies:

- External audit against the standard in order to gain and maintain certification to ISO 22301.

Details on the process for internal audits can be found in the document "Procedure for Business Continuity Audits".

4. Continual Service Improvement

The approach to continual improvement of the BCMP is to:

- Consider effectiveness across all business areas and end to end systems, processes within scope;
- Enhance current processes to bring them in to line with best practice (as defined within ISO 22301);
- increase the level of proactivity (and the business perception of proactivity) with regard to the on-going management of business continuity;
- Achieve an enhanced understanding of and relationship with the business units to which the BCMP applies;
- Review relevant metrics on an annual basis to assess their appropriateness, or to make changes to them based on collected historical data and feedback;
- Obtain ideas for improvement via regular review meetings with stakeholders, documenting them in the "Procedure for Continual Improvement"; and
- Review the "Procedure for Continual Improvement" document at regular management meetings in order to prioritise and assess timescales and benefits.

Ideas for improvement may be obtained from any source, including but not restricted to: Customers; Suppliers; Colleagues; Risk Assessments & Audits.

In order to evaluate any proposed improvements to the BCMP, the following criteria would be applied:

- Cost;
- Business benefit;
- Risk;
- Implementation timescale; and
- Resource requirement.

Accepted improvement proposals will be prioritised, and planned according to standard project management principals. Additional information on continual improvement methodology can be found in "Procedure for Continual Improvement".

POL00423565

Section D. Governance

How we monitor compliance

The Business Continuity Manager will ensure that this policy is implemented, reviewed and remains effective. Post Office's internal systems of business continuity risk control ensure that controls are regularly independently assessed for effectiveness, suitability and adequacy. In addition, Internal Audit will periodically test compliance with this policy.

Review and assessment of compliance with this policy is done on a timely basis and regular gap analysis is undertaken by the Business Continuity Manager and reported to the Risk and Compliance Committee.

Business continuity testing is planned and pre-determined. See further information in the "Business Continuity Exercising and Testing Schedule". Post Office's capability to maintain business operation will be subjected to exercise, and the results of these exercises will also be made available to the Risk and Compliance Committee.

We require third parties who do business with Post Office to have at least equivalent arrangements, systems and controls to this policy, and these should be demonstrable on request.

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 Jon Waples – Business Continuity Manager on GRO or by email at GRO

POL00423565

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 (POMS)
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
ISO 22301	The International Standard for Societal Security (Business Continuity).

References

References	Description
Business Continuity Context, Requirements and Scope	The purpose of this document is to describe the way the business operates, internal and external factors influencing it and to highlight in general terms the potential consequences of a business interruption. This will allow the most appropriate level of measures to be put in place to reduce the level of risk and to ensure that plans are available and tested to manage the impact of any interruptions that do occur.
Roles, Responsibilities and Authorities	The purpose of this document is to set out the organisation structure in terms of job roles, management and numbers of resources in each area and then to define how responsibility for each of the processes within the Business Continuity Management System (BCMS) is allocated within that structure.
Supplier Business Continuity Evaluation Process	This document sets out a process for the evaluation of the business continuity arrangements of our suppliers so that a degree of confidence may be gained that

POL00423565

	they possess sufficient resilience to support our requirements.
Risk Assessment Process	It is important that Post Office has an effective risk assessment process in place to ensure that potential impacts do not become real, or if they do, that contingencies are in place to deal with them. The starting point for risk assessment is the list of key business activities documented in the most recent business impact analysis.
Procedure for Business Continuity Audits	The purpose of this document is to set out how the Business Continuity Management Quality system will be audited internally.
Continual Improvement Action Log	Management of BCMP improvements can become unwieldy if they are spread across multiple reports, action plans and meeting minutes. The idea of this spreadsheet is to act as a focal point to record, assess and track all such improvement items in a common manner.
Procedure for Continual Improvement	In general Post Office will use the Plan-Do-Check-Act method (the Deming Cycle) for managing improvements as defined in the ISO 22301 standard
Business Continuity Exercising and Testing Schedule	The purpose of this document is to set out a schedule for testing / exercising activities.
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: 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

POL00423565

Post Office IT Disaster Recovery Policy

POL00423565

Contents Page

Contents Page 2
Document Control Sheet 3
Section A. Introduction 4
Section B. Context 5
About this Policy 5
What is IT Disaster Recovery? 5
Risk Appetite 5
How we organise IT Disaster Recovery 6
Who is responsible 6
Who must comply and how 6
Section C. Policy Details 8
Information 8
Our policy aims, controls and arrangements 8
Section D. Governance 11
..... 11
How do we monitor compliance 11
How to raise a concern 11
Contact us and more information 11
Section E. Key Terms and References 12
Key Terms 12
References 12

POL00423565

Document Control Sheet

POLICY SUMMARY			
GE Policy Sponsor	**Policy Owner**	**Policy Implementor**	**Policy Approver(s)**
Chief Financial Officer **Alisdair Cameron**	Head of IT Service Management **Stephen Hayes**	Head of IT Service Management **Stephen Hayes**	Post Office **RCC and ARC Committees**
Version and Status:	**Policy Review Period**	**Effective from :**	**Policy location:**
Final V6.0	Annually from policy effective date	19th May 2016	Z:\NEW COMPLIANCE\New Policy Framework 2015\Refreshed Policies 2016

DOCUMENT REVISION HISTORY			
Version	**Date**	**Author**	**Reason For Change**
Draft V5.0	31st March 2016	**SH/GB**	Policy Owner review & QA
Final V6.0	19th April 2016	**Stephen Hayes/Alisdair cameron**	Owners final review and sign-off

POLICY APPROVAL		
Role/Forum	**Name**	**Date**
Executive Owner and Sponsor	Chief Financial Officer (Alisdair Cameron)	15 April 2016
Executive Committee	Post Office Risk and Compliance Committee (RCC)	5 May 2016
Board Committee	Post Office Audit, Risk and Compliance Committee (ARC)	19 May 2016

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.	No later than 19th May 2017

POL00423565

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 is directly related to this code ensuring the highest standards of disaster recovery management are maintained.

This policy sets out what is and what is not acceptable but if you have any doubts or questions, these should be referred in the first instance to the Head of IT Service Management who oversees compliance with this policy. It is essential that you read this policy.

Introduction by the Group Executive Policy Owner: Chief Financial Officer

As Post Office's Chief Financial Officer and the Group Executive Policy Owner and Sponsor, I have overall accountability for IT Disaster Recovery to the Board of Directors. Post Office's Audit, Risk and Compliance Committee ("ARC") considers IT Disaster Recovery risks as an agenda item and the Board is updated on a regular basis.

POL00423565

Section B. Context

About this Policy

The purpose of this document is to define Post Office's policy with regard to IT disaster recovery and to demonstrate that it is appropriate for the aims and objectives of Post Office. This includes a framework as follows:

- The documentation of specific policy statements;
- A methodology for recording compliance with the IT Service Continuity policy;
- Management processes and procedures managed by the Post Office Service Integrator under their Service Integration Service Desk (SISD) agreement;
- Reporting the tests conducted within each IT supplier's Business Continuity Plan; and
- The recording of the Post Office IT eco-system resilience and disaster recovery tests that have been completed, the risks identified and service improvements to be implemented to the various service provider deliverables within their agreements.

The policy complies with the relevant provisions of the following standards ISO/ IEC17799:200, BS15000.

This policy sets out what we must all do to ensure Post Office complies with its IT disaster recovery obligations in its client and partner contracts and that Post Office follows a robust process to ensure the IT eco-system supplier's resilience and fail over solutions are regularly tested to ensure Post Office service continuity is maintained. This policy's effective date is 19th May 2016.

What is IT Disaster Recovery?

The Post Office IT disaster recovery policy sets out a mechanism whereby specific IT eco-system supplier processes, procedures and controls are effectively followed and test outputs measured with service improvements qualified to mitigate any risks identified during testing.

On the condition that the policy and processes are rigorously applied and measured, Post Office will have an effective audit trail of documentation and will have a high degree of confidence that the IT eco-system suppliers have the correct level of resilience within their IT architectural solutions to deliver high quality products and services as defined in their contractual obligations to Post Office.

Risk Appetite

Post Office has an adverse risk appetite for IT disaster recovery risk. Post Office recognises that whilst it cannot completely eliminate this risk, this policy sets out controls to reduce and/ or mitigate such risks.

POL00423565

How we organise IT Disaster Recovery

The Post Office IT Service Integrator provides an IT Service Continuity Management service within the IT service delivery model, based on a Service Integration and Management (SIAM) framework and works as a Managing Agent for the IT incumbent providers. Post Office procures these services through its SISD agreement with the Post Office IT Service Integrator.

For each IT supplier within the eco-system that has business continuity/ disaster recovery obligations within their direct contracts with Post Office, the Post Office IT Service Integrator will manage these supplier obligations on Post Office's behalf within the provision of the ITIL IT Service Continuity Management service.

The IT Service Continuity Management service is detailed within the following separate documentation; SIAM ITSCM Policy.v1b, SIAM ITSCM Process.v1a, POL-17645-HLD001-3.5 Operations_Manual_IT_Service_Continuity_Mgmt.v1c. These documents are pending Post Office final approval.

Who is responsible

Post Office's Board of Directors have overall responsibility for ensuring that Post Office has a framework to ensure compliance by (i) Post Office with its contractual obligations, and by (ii) 3rd party suppliers with Post Office's IT Disaster recovery obligations as set out in the relevant contractual agreements. The Board is kept abreast of relevant matters relating to the management of IT Disaster Recovery by reports from its committees, including the Audit, Risk and Compliance Committee. The key individuals and their specific responsibilities in relation to this policy are:

- The Chief Financial Officer, who is a member of the Post Office Group Executive team, is the policy Executive Owner and policy Sponsor, accountable to the Post Office Board overall;
- The Head of IT Service Management is the policy Owner, who is responsible for the day to day implementation of and compliance with this policy; and
- The Head of IT Service Management is also the policy Implementer, who is responsible for and accountable for the day to day implementation of the policy (including monitoring and reporting).

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.

POL00423565

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 Policy Owner.

If non-compliance is identified the matter must be referred to the Head of IT Service Management for investigation. 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.

POL00423565

Section C. Policy Details

Information

Post Office recognises the need to ensure that our business operates safely, smoothly and without interruption for the benefit of our colleagues, customers, shareholders and other stakeholders. To ensure such levels of safe, continuous operation, Post Office has implemented a Business Continuity Framework consistent with "ISO 22301".

The operation of a Business Continuity Framework has many benefits for Post Office, including:

- The safe-guarding of colleagues at times of duress;
- Ensuring the supply of goods and services to our customers;
- Protection of revenue streams and business profitability;
- Maintenance and enhancement of shareholder/ stakeholder value; and
- Compliance with legal and regulatory requirements.

Post Office is committed to the development, maintenance, improvement and socialisation of a Business Continuity Management Programme within and across the organisation.

As part of the Post Office Business Continuity Framework, this IT Disaster Recovery policy outlines the IT approach to delivering continuity of services under a Disaster Recovery event within the Post Office.

Our policy aims, controls and arrangements

Aims of the policy

- Maintain an acceptable level of service during a service invocation;
- Ensure plans and alternative service options are in place to meet the organisation's needs in the event of a significant business outage or disruption;
- Support Business Continuity Management ensuring the appropriate communication and management plans are in place and available to support business critical needs;
- Reduce the likelihood of a disruption occurring through the identification and mitigation of risks;
- Ensure each IT eco-system supplier will have processes and plans supporting the delivery of their contracted services. End to end delivery must underpin the recovery of business systems based on the business needs; and
- Comply with relevant provisions of ISO / IEC17799:200, BS15000 (as amended) and all other industry standards in force.

POL00423565

Analyse the IT Landscape, define responsibilities and prepare plans

- Analyse threats and estimate the probability of having an effect on Business Service Continuity;
- Maintain an overall business criticality matrix of services using the baselines provided by Supply Chain and Customer;
- Detect and report the most vulnerable points of infrastructure;
- Ensure all continuity team members have an in depth knowledge of the IT infrastructure and of the items involved in providing each IT service that underpins business services;
- Identify areas of the IT service model where there are constraints and to define the process to manage and mitigate the risk;
- Identify the responsibilities of all parties in the event of an invocation;
- Detail in recovery plans all necessary information required by the customer in order to invoke a successful continuity plan and maintain service;
- Ensure that any plans designed by the key stakeholders are within the authority matrix.
- Establish processes to plan for, respond to and recover from, disruptive events.

Develop and Test and Report on the Recovery Procedures

- Develop and maintain the recovery procedures for specific business services delivered through the IT eco-system supplier network.
- Test and improve recovery procedures, working with IT eco-system supplier.
- Ensure each IT eco-system supplier has processes and plans supporting the delivery of their contracted services.
- Validate a working continuity programme by evidencing that recovery plans are in place and that they are being tested in line with the requirements set out in the contract.
- Receive all IT eco-system supplier written reports following their Continuity testing.
- Provide written reports within agreed timescales following Continuity Exercises to the key stakeholders within the authority matrix.

Manage invocations

- Inform key stakeholders within the authority matrix of any invocation of IT Continuity plans.
- Provide for the restoration and ongoing performance of the services following disaster, or a failure in or disruption to services.
- Conduct a post supply chain disaster review following any invocation of IT service continuity, business continuity or supply chain members disaster Recovery plans to understand the cause of the supply chain disaster and plan for the restoration of the IT Services to the pre- supply chain disaster state and implement actions to eliminate or mitigate future occurrences.

POL00423565

Continuous improvement

- Continually review all IT eco-system supplier continuity plans where applicable, to ensure they meet continue to meet the business requirements and amend where appropriate through the contractual process.

Co-ordination of the IT Disaster Recovery plan with the Business Continuity Plan

- Ensure a business continuity plan is made and includes the planning for non-IT related aspects such as key personnel, facilities, crisis, communication and reputation protection, and that it refers to the IT Service Continuity Plan for IT related infrastructure recovery/ continuity.

POL00423565

Section D. Governance

How do we monitor compliance

The Head of IT Service Management will ensure that this policy is implemented, reviewed and remains effective. Post Office internal systems of risk control ensure that disaster recovery controls in this policy are regularly independently assessed for effectiveness, suitability and adequacy. In addition, Internal Audit will periodically test compliance with this policy.

We assess compliance with this policy on a regular basis and regular Disaster Recovery reports will be issued by Head of IT Service Management to the IT Supplier and Service Committee.

We require our subsidiaries and third parties to have at least equivalent arrangements, systems and controls to this policy, and these should be demonstrable on request.

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 **Stephen Hayes, Head of Service Management** GRO **or by email** GRO

POL00423565

Section E. Key Terms and References

Key Terms

Term or Acronym	Description

References

References	Description
1. Post Office Group	Post Office Limited and all subsidiaries and entities within the Post Office Group which includes Post Office Management Services (POMS).
2. 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: GRO or by telephone on: GRO 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

POL00423565

Post Office

Pre-Employment Vetting Requirements

POL00423565

Contents

Contents 2
Document Control Sheet 3
Section A. Introduction 4
Section B. Context 5
About this Policy 5
What is pre-employment vetting? 5
Risk Appetite 5
How we manage pre-employment vetting 6
Who is responsible 6
Who must comply 6
Section C. Policy Details 8
How you comply 8
Our Records 8
Section D. Governance 9
How do we monitor compliance 9
How to raise a concern 9
Contact us and more information 9
Section E. Key Terms and References 10
Key Terms 10
References 10
Appendix. Further Guidance on how vetting will be conducted 11
Proof of Qualifications 13
Money Laundering Regulations (MLR) 14

POL00423565

Document Control Sheet

SUMMARY			
GE Policy Sponsor	**Policy Owner**	**Policy Implementor**	**Policy Approver**
Group People Director **Neil Hayward**	Head of Human Resources **Sean Leahy**	Head of Human Resources **Sean Leahy/Andrew Lewis**	Post Office **RCC and ARC Committees**
Version and Policy Status:	**Document Review Period**	**Policy – effective date :**	**Policy location:**
Draft V5.0	Annually from policy effective date	19th May 2016	Z:\NEW COMPLIANCE\New Policy Framework 2015\Refreshed Policies 2016

REVISION HISTORY			
Version	**Date**	**Author**	**Reason For Change**
Draft v4.1	18th April 2016	**Jane MacLeod**	Legal Team Final Review
Draft v5.0	21st April 2016	**Andrew Lewis/Sean Leahy**	Policy Owner final review
Draft v5.0	25th April 2016	**Neil Hayward**	Policy Sponsor sign-off

POLICY APPROVAL		
Role/Forum	**Name**	**Date**
Executive Owner and Sponsor	Group People Director (Neil Hayward)	30th April 2016
Executive Committee	Post Office Risk and Compliance Committee (RCC)	5th May 2016
Board Committee	Post Office Audit, Risk and Compliance Committee (ARC)	19th May 2016

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.	No later than 19th May 2017

POL00423565

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 is directly related to this code ensuring the highest standards of employment vetting 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 who oversees compliance with this policy. It is essential that you read this policy.

Introduction by the Group Executive Policy Owner: Group People Director

As Post Office's Group People Director and the Executive Policy Owner I have overall accountability for vetting to the Post Office's Board of Directors. Post Office's Audit, Risk and Compliance Committee considers HR (see section E for the definition of "HR") legal and compliance risks as a standing agenda item and the Post Office Board is updated on a regular basis.

POL00423565

Section B. Context

About this Policy

This policy supersedes and replaces all previous policies relating to employment vetting for and on behalf of Post Office.

The purpose of this policy is to set out a framework for the employment vetting of all roles within Post Office, and within contract partners offering products and services as any part of Post Office Group, which meet our legal, regulatory and contractual obligations and therefore reduces risks of human error, theft, fraud and/ or misuse of facilities. This policy is effective from 19th May 2016.

What is pre-employment vetting?

Vetting is the process of performing a background check on someone before offering them employment or conferring a contract of work.

This policy addresses and minimises any potential security risks that are posed as a result of recruiting new employees as well as those recruited as a result of redeployment of employees into roles with different vetting requirements. The policy also applies to contract partners offering products and services under any part of Post Office Group branding, such as Sub-Postmasters and their employees (Referred to as Partners in this policy). Successful deployment will reduce and minimise security risks to the business, our customers, our Partners and employees.

This policy re-iterates the terms set out in Condition 8 of the January 2006 postal operators' licence; Protecting the Integrity of the Mail, which specifies the vetting standards that Post Office is obliged to meet under the Mails Integrity Code of Practice (2006). This policy meets Post Office regulatory obligations of Ofcom, the Financial Conduct Authority (FCA) and Security Industry Authority (SIA); which encompass all recruitment - employees, agents and assistants. Failure to adhere to this vetting policy may put trading licences at risk and, as a result, Post Office Groups ability to operate in key business markets (including but not limited to; postal services and financial services) could be withdrawn or fines applied.

This policy ensures all legal (Right to Work) documents are collected and verified as required in accordance with Post Office's duty to prevent illegal working. Other requirements addressed by this policy include the need to adhere to the legal, regulatory and contractual requirements for certain roles, such as obtaining relevant security clearance or evidencing required qualifications.

Risk Appetite

Post Office has an averse risk appetite for regulatory and legal risks. This policy reflects this and sets out controls to reduce and/ or mitigate risks associated with offering employment or conferring contracts for work.

POL00423565

How we manage pre-employment vetting

Post Office HR Service Centre commences pre-employment vetting process once all relevant documentation has been received; vetting must be completed prior to a prospective employee's or Partner's start date. A contract will only be issued once the vetting process is complete.

Exceptional Circumstances:
In exceptional circumstances (for example, to deal with industrial action, Christmas pressure outside of planned engagement of Christmas casuals or an outbreak of a serious contagious disease) different and possibly reduced levels of vetting may be applied. However only with the prior authorisation of, and to the specific requirements determined by and agreed with the Head of Human Resources for the business area the candidates will be joining.

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 vetting by reports from its committees including its ARC Committee. The key individuals and their specific responsibilities in relation to this policy are:

- The Group People Director is a member of the Post Office Executive team, and is Group Executive policy owner and policy Sponsor, accountable to the Post Office Board;
- The Policy Owner, the Head of Human Resources, is responsible for the day to day implementation of and compliance with this policy, and is accountable to the Group People Director; and
- The Policy Implementor is responsible for the day to day implementation of the policy lifecycle (including monitoring) and is responsible for and accountable to the policy Owner for reporting all policy matters.

Who must comply

Compliance with this policy is mandatory. This policy will apply to the recruitment approval process for all Post Office employees, officers, contractors, casual workers, and Partners. 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 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

POL00423565

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 HR Vetting 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 Investigations Policy. If the cause is found to be due to wilful disregard or negligence, it will be treated as a disciplinary offence.

POL00423565

Section C. Policy Details

How you comply

It is the policy of the Post Office that all applicants agree to undergo a pre-employment vetting process. The nature of this process will include verifying eligibility to work in the United Kingdom or Northern Ireland, and electronic searches of information already available in the public domain. Such information may include the following: sanction lists, criminal records, lists of politically exposed persons, FCA Register Search, embargo lists, Companies Office records, etc.

All successful applicants based in the United Kingdom and Northern Ireland will be subject to a basic financial check (sometimes referred to as Credit and Voters Checks). This will provide us with information including data from the electoral register to verify date of birth, where appropriate publicly available data to reveal any adverse information, including County Court Judgments, Bankruptcies, Voluntary Arrangements etc.

Pre-employment vetting guidelines may be updated to reflect current best practice and/ or required legislation or other Post Office change of policy.

It is the policy of Post Office that all non-payroll contractors complete pre-employment vetting prior to gaining access to systems and work locations. For details of non-payroll contractor pre-employment vetting requirements contact the HR Service Centre.

HR Service Centre will commence the pre-employment vetting process once all the relevant documentation has been received; the vetting must be completed prior to the employees start date. A contract will be issued once the vetting process is complete.

Our Records

This policy document must be maintained and be available for review at all times. The policy will be kept in the resourcing section of the HR, Advice and Guidance intranet site. Other policy related records created as a result of vetting activity must be kept in accordance with Post Office retention of records policy and must comply with legal and regulatory record keeping requirements.

In all cases, records must be maintained to show:

- that the verification process was properly carried out and all documentation retained in the personal file including the pre-employment checklist (except for where data protection rules prohibit the retention of the data); and
- the candidate's personal file and all documentation therein must be retained throughout the period of employment and for 7 years post-employment.

POL00423565

Section D. Governance

How do we monitor compliance

The Head of Human Resources will ensure that this policy is implemented and reviewed, vetting controls in this policy are regularly independently assessed for effectiveness, suitability and adequacy. In addition, Internal Audit will periodically test compliance with this policy.

HR assess compliance with this policy on a regular basis and reports will be issued by the Group People Director to Post Office's RCC and to the Board ARC Committee.

We require third parties who do business with Post Office 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, contact the policy Owner, the Head of Resourcing Manager.

POL00423565

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 (POMS) and FRES
Executive Policy Owner	As defined by the Post Office Policy Framework-Roles and responsibilities Matrix document V0.5
FCA	Financial Conduct Authority
HR	Post Office Human Resources team
Partner	Any contract partner or their employees who offer products or services under the branding of Post Office Group or its subsidiaries. Such as Agents, Sub-Postmasters and their Assistants.
Policy Owner	As defined by the Post Office Policy Framework-Roles and responsibilities Matrix document V0.5
SIA	Security Industry Authority

References

References	Description
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: 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

POL00423565

Appendix. Further Guidance on how vetting will be conducted

Application Form Declaration: Each candidate must complete an application form either online or hard copy. The application form must be signed or the candidate must declare online that the information is correct.

A copy of the application form must be kept. This can either be stored securely within the recruitment system or in the candidate's personal file.

Criminal Convictions Declarations: The candidate must declare any unspent criminal convictions, impending prosecutions and cautions. Also any military Martials must be declared.

Proof of Identity: All candidates are required to produce one document which has photographic proof of the person's identity. (Refer to Document Checklist for Candidates at Appendix2).

Proof of Right to Work in the UK: The candidate's Right to Work documents are checked against the Home Office guidelines to ensure that these documents constitute a valid Right to Work (see Appendix 2).

Proof of Address: All candidates are required to provide documentary evidence of their address/place of residence (refer to Document Checklist for Candidates Appendix 2)

Proof of National Insurance Number: A check must be made to ensure the number is in the format of an official National Insurance (NI) number i.e. 2 Letters, 6 numbers and a single letter

In addition to the official NI number card and official notification of the NI number from the Inland Revenue, P60's and payslips may be used. These documents must not be handwritten.

Health Consent Form: For Post Office employees this consent is required should an offer of employment be made. The employee will be asked further screening questions against a matrix provided by the POL Employee Health Service (EHS) providers ATOS Origin. Where further medical advice is required, candidates are referred to ATOS Origin.

Personal Declaration to Post Office Ltd. (P13 form): In part this goes toward satisfying the condition of the operating licence issued to Post Office Ltd.

The P13 form should be read, signed and dated by all candidates at the document checking part of the interview process and by agency staff or contractors at the registration session.

The candidate's signature should be witnessed, countersigned and dated by an appointed Post Office Ltd Representative, (this can be the hiring manager or a member of the HR team).

POL00423565

The P13 form must be retained within the candidate's personal file and a copy supplied to the candidate

The requirements are specific to roles which are deemed "Fit and Proper" (F&P) and in line with the FCA.

Fitness and Propriety Form: The Fitness and Propriety (F&P) declaration form will be sent to successful candidates for completion by the Recruitment Team.

It is a mandatory element that all successful candidates (internal and external) for the roles within scope fully complete a F&P declaration form and answer **all** questions **honestly**. For the avoidance of doubt, honesty at all times when completing the F&P form is a crucial factor in considering whether a successful candidate is deemed to be "Fit and Proper."

Post Office can request that the F&P declaration form to be completed by employees within scope on an on-going basis and those members of staff that change their role into a role that fall within the F&P scope.

Directorship Search: The Directorship Search requires the successful candidate to answer specific questions, which are: - have they **ever** been a director, secretary or LLP of a company (Yes or No) or **ever** been disqualified from acting as a director (Yes or No)

If the successful candidate answers yes to either or both questions they must list the company name, country of registration, company number, dates of position held, country in which disqualified, reason for disqualification and dates when disqualified.

A search will be carried out irrespective of yes or no answers directly with Companies House to verify what the successful candidate has stated on the consent form.

FCA Register Search: The FCA Register Search requires the successful candidate to answer specific questions which are; - Are you currently or have you **ever** previously been approved by the FCA to carry out a controlled function (Yes or No). If yes, then the candidate will need to supply their individual reference number (if known)

Irrespective of the answers, a search will be run directly with the FCA to verify what the successful candidate has stated on the consent form. In the case of employees, this search will be conducted by Post Office Ltd.

In the case of agency staff/contractors, this search will be conducted by the relevant supplier.

The relevant supplier will verify all information and report on any discrepancies indicating the risk of severity of the discrepancy

Globex Criminality Database Search (By Exception): The Global Criminality Database Search will only be undertaken **by exception** in circumstances when amber/red flag issues have arisen primarily within the Directorship search area.

POL00423565

A "global" database search may be run, using the candidates name and previous names to identify any crime or information relating to,

- Bribery
- Corruption
- Counterfeiting
- Falsifying information on official documents
- Fraud
- Embezzlement
- Theft
- Tax evasion
- Money laundering
- Insider trading and market manipulation
- Currency counterfeiting
- Securities fraud

Proof of Qualifications

Where appropriate for the role, proof of valid and up to date qualifications must be obtained.

Specific roles and Supply Chain staff: Valid Driving License (where relevant to the role). A check is required to ensure that the candidate has a valid and acceptable driving licence suitable for the role.

- If the individual is required to drive a vehicle above 3.5t then they will need to have a C1 on their licence. For drivers who passed their test before January 1997 they should have this as an acquired right, for any drivers who passed their test after this date then they would not have this as a part of passing their car test, and are required to undertake an additional driving test to drive rigid vehicles above 3.5t.
- In the case of agency staff/contractors, the relevant supplier will be made aware by Post Office as to which type of licence is required.

SIA Licence Check: Where a candidate has an SIA licence the licence number must be checked against the Home Office register.

POL00423565

References (5, 6 or 10 years)

- The candidate is required to give consent for references to be requested by completing the Multi Consent Form or equivalent for agency staff and contractors.
- This consent allows Post Office and approved agencies to apply to the following in order to gather reference information prior to employment;
    - Previous employers;
    - Accountants;
    - Education establishments
    - DWP and HMRC
    - The consent also gives Post Office permission to disclose any reference information with auditors from a third party.
- Where the role is a regulated role such Financial Services Area Manager or Mortgage Specialist or the candidate is required to complete a F&P declaration, written confirmation shall be sought from all the former employers, educational establishments, etc., listed by the applicant that the dates given are accurate and that there is nothing in their experience of the applicant which suggests a lack of integrity or otherwise adversely reflects upon his/her suitability for the employment in question.
- Confirmation of periods of registered unemployment must be sought from the Employment service or other government agencies.
- Employment cannot be offered until all relevant information has been received.
- Where any lack of integrity is indicated and a clear decision not to employ cannot be made, any decision of employment must be referred to the Head of Resourcing in Post Office.

Money Laundering Regulations (MLR)

Successful candidates will be required to make an application to HM Revenue and Customs for a "fit and proper test" in line with the Money Laundering Regulations 2007.

Once the application is completed it will be sent by the HR Service Centre (HRSC) Recruitment Team to the Vetting Team who will then process the application.

POL00423565

Conflicts of Interest Form: In accordance with section 175 of the UK Companies Act 2006, it is the duty of a director of a company who is in any way, directly or indirectly, interested in a contract or proposed contract with the company to declare the nature of his interest at a meeting of the directors of the company.

A director has a duty to make a section 175 declaration at each board meeting if appropriate, and a questionnaire on conflicts of interests will be circulated to Directors on appointment. If any conflicts are disclosed in the questionnaire they should be discussed with the Company Secretary.

A Conflicts of Interest Form will be presented to the successful candidate to complete.

Companies House Application: In accordance with Section 167 of the Companies Act 2006, the successful candidate must be registered with Companies House. The application will be the responsibility of the Company Secretary via the on line an APO1 form.

More information on appointments of Directors and the requirement to register can be found at www.gov.uk/government/publications/appoint-a-director-ap01

POL00423565

Post Office Whistleblowing Policy

POL00423565

Contents Page

Contents Page 2
Document Control Sheet 3
Section A. Introduction 4
Section B. Context 5
About this Policy 5
What is Whistleblowing 5
Section C. Policy details 7
How to raise a concern 7
Whistleblowing Officer and 'Speak Up' details 7
Confidentiality and anonymous reporting 7
Investigating concerns 8
Outcomes and Reports 9
External Disclosures 9
Protecting the Whistleblower 10
Contact us 10
Who is responsible for this policy 11
How we monitor compliance 11
Section D. Key Terms and References 12
Key Terms 12
References 12

POL00423565

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 **RCC and ARC Committees**
Version and Policy Status:	**Policy Review Period**	**Effective from:**	**Policy location:**
Final V1.4	Annual Review (from Effective date)	19th May 2016	Z:\NEW COMPLIANCE\New Policy Framework 2015\Refreshed Policies 2016

REVISION HISTORY			
Version	**Date**	**Author**	**Reason For Change**
Draft v1.3	18/04/16	**Nisha Marwaha**	Policy Owner review
Final v1.4	27/04/16	**Jane MacLeod**	Sponsors review and sign-off

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)	5 May 2016
Board Committee	Post Office Audit, Risk and Compliance Committee (ARC)	19 May 2016

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.	No later than 19th May 2017

POL00423565

Section A. Introduction

Chief Executive's Note

Post Office is committed to conducting business with the highest standards of honesty, integrity and openness in order to create a workplace where workers feel able to raise concerns. A culture of openness and accountability is essential in order to prevent illegal, improper or unethical conduct and an effective Whistleblowing Policy helps us to identify and address situations when they occur.

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 Whistleblowing obligations. Post Office's Audit, Risk and Compliance Committee ("ARC") considers Whistleblowing as an agenda item and the Post Office Board is updated on a regular basis.

POL00423565

Section B. Context

About this Policy

The purpose of this policy is to encourage the reporting of suspected wrongdoing and/or dangerous practices, (see section entitled What is Whistleblowing below), within Post Office, to make it easier for management to address those concerns and therefore avoid serious accidents, fraud, regulatory breaches, financial impropriety and/or reputational damage.

The aims are:

(1) to encourage staff to report matters as soon as possible in the knowledge that their concerns will be taken seriously and investigated, and that confidentiality will be respected,
(2) to provide staff with guidance as to how to raise those concerns, and
(3) to reassure staff that they should be able to raise concerns without fear of reprisals, even if they turn out to be mistaken.

This policy enables Post Office to comply with its Whistleblowing obligations under applicable legislation and to be in line with regulatory requirements. This Policy is effective as at 19th May 2016.

What is Whistleblowing

"Whistleblowing" refers to the act of exposing wrongdoing and/or dangerous practices by reporting it either internally within an organisation, or externally, for example to a regulator. The law on Whistleblowing is contained in the Employment Rights Act 1996 as amended by the Public Interest Disclosure Act 1998. Wrongdoing includes criminal activity, civil offences (including negligence, breach of contract, breach of administrative law), miscarriages of justice, dangers to health and safety or to the environment and the cover up of any of these.

Workers should raise a concern if they are aware of, or suspect, wrongdoing which affects others (e.g. customers, members of the public, colleagues or the Post Office). Some examples (this is a non-exhaustive list) of situations where a worker may raise a concern are:

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

POL00423565

A Whistleblower is a person who raises a genuine concern relating to any wrongdoing including any of the above. If a worker has any genuine concerns related to suspected wrongdoing, they should report it under this Policy.

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

POL00423565

Section C. Policy details

How to raise a concern

In the first instance, workers should raise concerns with their line manager, or a senior HR manager in Post Office. Alternatively workers can notify the Whistleblowing Officer directly, using the contact details provided in this Policy.

It is recognised that sometimes raising a concern directly with the business may not be possible, for example, if the worker considers that the line managers may be involved in the issue or if they have a concern about confidentiality.

In such instances workers should contact the **"Speak Up"** confidential reporting service which is run by InTouch MCS Ltd, an independent company (see section below entitled Whistleblowing Officer and Speak Up details for more information).

InTouch will treat concerns in complete confidence and the worker does not have to provide contact details. **Post Office treats all concerns raised under this Policy very seriously.**

Whistleblowing Officer and 'Speak Up'

The Whistleblowing Officer for the Post Office Group is Post Office's General Counsel, currently Jane MacLeod who can be contacted by telephone on: GRO or by email on: GRO

The Speak Up service is available on GRO or via a secure on-line web portal http://www.intouchfeedback.com/postoffice.

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

Confidentiality and anonymous reporting

Post Office hopes that workers will feel able to voice Whistleblowing concerns openly under this Policy. However, if a worker wants to raise a concern confidentially, Post Office will make every effort to keep their identity secret. If it is necessary for anyone investigating a concern to know the worker's identity, the investigator will discuss it with that individual.

When reports are made anonymously via Speak Up, there is no requirement to provide contact details. However, not providing details may reduce Post Office's ability to undertake a thorough investigation into the concerns raised.

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

POL00423565

Investigating concerns

All concerns (including those raised via Speak Up) will be passed to the Whistleblowing Officer who will carry out an initial assessment of the issue to determine the scope of any investigation.

The Whistleblowing Officer will decide whether an investigation is appropriate and what form the investigation should take. The type of investigation will depend on the nature of the concern and may be:

- investigated internally (or the Whistleblowing Officer may decide to appoint an external investigator if there are good reasons),
- resolved by agreed action as determined by the Whistleblowing Officer without the need for investigation,
- referred to the police, and
- referred to a regulatory authority.

If an investigation is appropriate, the Whistleblowing Officer will appoint an investigator. The appointed investigator should be an individual at an appropriate level for the matter under investigation and they must not have any conflict of interest with the individuals or issues concerned.

In some cases an investigator or team of investigators may be appointed including staff with relevant experience of investigations or specialist knowledge of the subject matter.

The Whistleblowing Officer may determine that the matter should be investigated under the terms of other more appropriate Post Office Group policies, such as those covering grievance or bullying and harassment matters, in which case the process described in the applicable policy will apply. The Whistleblowing Officer can also decide to take no action if the complaint appears to be without a reasonable basis.

During an investigation under the Whistleblowing Policy, the investigator may wish to contact the worker directly to request additional information. Where the worker's identity is known, this will be done only where the worker has consented to a representative from Post Office speaking to them directly. Where the worker's identity is anonymous, questions or requests for information can be raised anonymously either through the Speak Up service, or via secure voicemail or messaging on the web portal.

Subject to concerns about confidentiality, the worker may be required to attend meetings to provide further information. Workers can bring a colleague or union representative to any meetings under this Policy. The companion must respect the confidentiality of the worker and any subsequent investigation.

POL00423565

Investigators should consider the principles set out in Post Office's internal Investigations Policy and adhere to those wherever possible when undertaking the investigation.

Outcomes and Reports

The investigator should aim to keep the Whistleblower informed of the progress of the investigation and its likely timescale.

The investigator must write a report containing the findings of the investigation, including conclusions as to the validity of the allegations and recommendations for further action. The report should be submitted to the Whistleblowing Officer.

After the investigation, the investigator will inform the Whistleblower of the outcome of the investigation and what action, if any, has been taken. Sometimes the need for confidentiality may prevent Post Office disclosing specific details of the investigation or any disciplinary action taken as a result. If it is determined that no action will be taken, then the individual concerned should be informed of the reason for this.

The Whistleblowing Officer will determine what further action is required. If Post Office concludes that a Whistleblower has made false allegations maliciously or with a view to personal gain, the Whistleblower will be subject to disciplinary action.

Post Office cannot always guarantee the outcome the Whistleblower is seeking, but will aim to deal with concerns fairly and in an appropriate way. If a worker is unhappy with the way in which their concern has been handled, they should raise it with the Whistleblowing Officer or if that is not appropriate for any reason, the Chairman of the Post Office Board Audit and Risk Committee.

The investigator will share any reports with the Whistleblowing Officer. In all cases a report of the outcomes of any investigation will also be made to the Audit Committee as a means of allowing the committee to monitor the effectiveness of the Policy.

Copies of such reports should be held in accordance with Post Office's document retention policies.

External Disclosures

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

However, the law recognises that in some circumstances it may be appropriate for workers to report their concerns to an external body such as a regulator. It will very rarely, if ever, be appropriate to alert the media.

POL00423565

The independent Whistleblowing charity, Public Concern at Work, have a list of prescribed regulators for reporting certain types of concern. Their contact details are as follows:

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

Public Concern at Work operates free, confidential advice to people concerned about crime, danger or wrongdoing in the workplace. We strongly encourage you to seek advice from them before reporting a concern to external parties.

Protecting the Whistleblower

It is understandable that Whistleblowers are sometimes worried about possible repercussions. Post Office has a statutory obligation to protect Whistleblowers and will support workers who raise genuine concerns under this Policy, even if they turn out to be mistaken.

Post Office will take all reasonable steps to ensure that Whistleblowers do not suffer any detrimental treatment as a result of raising a concern. Detrimental treatment includes disciplinary action, dismissal, threats or other unfavourable treatment connected with raising a concern.

Workers must not threaten or retaliate against Whistleblowers in any way. If anyone is involved in any such conduct, it will be taken seriously and they will be subject to disciplinary action.

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

Training will be provided to managers to make them aware of the rights of Whistleblowers.

Contact us

If you need further information about this Policy or wish to report an issue in relation to this Policy , contact Nisha Marwaha – Employment Lawyer on GRO or by email : GRO

POL00423565

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 Whistleblowing by reports from its committees including its ARC Committee.

- 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.

How we monitor compliance

The Principal Employment Lawyer will ensure that this policy is 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 and Compliance Committee.

The General Counsel provides an annual summary of reports made via the Speak Up line and other known instances of Whistleblowing to (i) the Post Office Board and the Post Office Management Services Board as appropriate, and (ii) the Post Office Board Audit and Risk Committee. In making these reports, the confidentiality of Whistleblowers will be respected.

Any serious concerns reported by Whistleblowing will be escalated by the Whistleblowing Officer to the Chairman of the Post Office Board Audit and Risk Committee.

POL00423565

Section D. Key Terms and References

Key Terms

Term or Acronym	Description
HR team	Post Office Human Resources team

References

References	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 (POMS)
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

POL00423565

6) Oversight of Post Office FCA regulated activities - RCC

Author: Jonathan Hill Sponsor: Kevin Gilliland Date: April 2016

Executive Summary

Context

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.

Post Office is an Appointed Representative 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 (AR) allows Post Office to be exempt from authorisation under FSMA to undertake FCA regulated activities provided certain conditions are met, including that BoI and POMS will take regulatory responsibility for Post Office in respect of such activities. 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 Distribution Agreement (DA) which includes a Regulatory Governance Manual (RGM) to govern the conduct of regulated activity.

The questions addressed in this paper:

1. What are Post Office's obligations under the AR, DA and RGM?
2. What framework is in place to ensure compliance with these obligations?
3. What assurance is provided to Post Office and its Principals to demonstrate compliance?
4. What would the consequences be if Post Office failed to comply?
5. What further actions should Post Office take to ensure compliance?

Conclusion

BoI and POMS take the ultimate responsibility for regulatory compliance through their FCA authorisation and under the Appointed Representative agreements. The obligations in place with our regulatory Principals require Post Office to comply with the relevant FCA handbook requirements and Post Office's CEO is the FCA Approved Person for the AR responsibilities.

There is an established framework in place for providing regulated financial services for compliance through the BoI relationship and reporting of compliance

POL00423565

risks and issues to the Principal. It is however recognised by both Principals that there are gaps and there are areas that need to be improved, particularly through 1st line ownership of controls in the network. The key areas for improvement have been identified with action plans and are outlined in this paper.

The Network lead team fully support this activity. It is our assessment that both the introductory and sales activities in our network should continue pending further work on controls and oversight. Planned Internal Audit oversight activity in network sales this year will further test the adequacy of the control environment across the key risk areas identified in this report.

Background

All Post Office FS distribution can be conducted online, via call centres or through the branch network. The exception to this are loans which are conducted by call centre or internet only. All contact centres and website fulfilment is managed directly by the Principals and/or their third party providers.

Internet

The customer interaction will be on an 'execution only' basis. The relevant web sites and on line journeys and are all reviewed and signed off directly by the regulatory principals in respect of the sales and service journeys. There are established 'sign off' processes in place between sales teams and Principal compliance teams for this approval.

So for example for credit card internet journeys the Post Office/BOI product teams and the Post Office digital team may construct the website and the journey. But BOI compliance are then responsible for reviewing and approving the site from a compliance perspective.

Call Centres

The customer interaction will be on a non-advised basis, with the exception of mortgage sales. The sales and service call centres for Post Office's FS products are operated by third parties operating on behalf of Post Office Money.

Post Office has a general help line for customers (POEX), Post Office call centre staff will not fulfil financial services sales or service calls from this call centre but are trained to direct these calls to the financial services firms.

Post Office Branch Network

The Post Office branch network provides different levels of distribution with customers' dependant on product and who engages with the customer (see below).

POL00423565

Table 1: Insurance Distribution in the Post Office Network-POMS

	Motor and home insurance	Life term assurance	Over 50s Life	Travel Insurance	Other insurance products e.g., pet, business
Financial and Mortgage specialists	Can complete sales on non-advised basis (use 3rd party insurer website for sale)	Can complete sales on non-advised basis (use 3rd party insurer website for sale)	Can complete sales on non-advised basis (use 3rd party insurer website for sale)	Can complete sales on non-advised basis (sales captured through Horizon platform)	Introduction only
Customer Relationship managers	Introduction only	Introduction only	Can complete sales on non-advised basis (sales captured through Horizon platform)	Can complete sales on non-advised basis (sales captured through Horizon platform)	Introduction only
Counter colleagues in Crown and Agency	Introduction only	Introduction only	Can complete sales on non-advised basis (sales captured through Horizon platform)	Can complete sales on non-advised basis (sales captured through Horizon platform)	Introduction only

Banking distribution in the Post Office Network-BOI

	Mortgages	Credit Card	Savings Products including Pre paid funeral
Mortgage specialists	Fully Advised sales process	Can complete sales on non- advised basis	Can complete sales on non- advised basis
Financial specialists	Capture leads only	Can complete sales on non- advised basis	Can complete sales on non- advised basis
Customer Relationship managers	Capture leads only	Introduction only	Introduction only
Counter colleagues in Crown and Agency	Capture leads only	Introduction only	Introduction only

POL00423565

Financial and Mortgage Specialists ("FSs and MSs") in Crown branches

The scope of FSs/MSs activities extend beyond insurance products. For example, all mortgage specialists are qualified mortgage advisors and all specialists can arrange the sale of a variety of Post Office Money products. These specialists will have customer appointments where customers can discuss their needs and specialists provide information for customers to facilitate them making an informed decision on whether to take out a product.

Customer Relationship Managers ("CRMs") in agency branches

Postmasters or agency approved staff are trained by Post Office to undertake a more engaging introductory sales journey with the customer using sales aids and scripted conversations. The journeys remain introductory-only except for Over 50s Life and Travel Insurance where CRMs can complete the sale on the Horizon platform. For the other insurance products the CRM can introduce the product and signpost to the customer options on how to complete the sale; typically online or through a contact centre.

Counter Colleagues

Counter colleagues can complete sales for Over 50s Life and Travel Insurance using the Horizon platform. This capability is available in 9,600 branches for Over 50s Life and 7,500 branches for Travel Insurance, providing immediate cover to the customer. For Travel insurance this includes requesting the customer to declare any medical issues via the contact centre where medical screening may be required.

The remaining activity is composed of product introductions to customers in Crown and Agency branches. This is where the customer is provided with limited oral 'introductory' information about a product (either in response to a customer's request or introduced to the customer) and, if the customer is interested in finding out more or wants to apply, he/she is either provided with an application pack to complete, invited to contact the relevant contact centre go online or bring the completed application pack in to branch for a counter colleague to send.

1. What are Post Office's obligations under the RGM?

The regulatory Principals have appointed Post Office as its agent to carry out the regulatory activities as outlined contractually in (a) and (b) below and Post Office is required to carry out its business in accordance with the requirements of the FCA handbook. In this respect the CEO of Post Office is the Approved Person for these purposes and has been approved as such by the FCA.

a) The Regulatory Governance Manual (RGM)
b) The Distribution Agreement
c) and the FCA Handbook

The RGM outlines the compliance requirements to be followed in key areas covering the FCA handbook together with relevant product related schedules.

POL00423565

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 insurance products

Post Office is required to have in place systems and controls to meet the requirements identified above.

e.g., for Training and Competence the RGM requires staff to be competent, to be adequately supervised and regularly trained. It also requires that Post Office must establish, maintain and communicate to Post Office staff such systems and controls as are necessary for it to ensure that Post Office staff:

(a) involved, either directly or indirectly, in the sale or promotion of the Products; or

(b) responsible for the supervision of those involved in the sale or promotion of the Products,

are 'fit and proper' persons for the role they perform including confirming financial soundness, honesty, integrity and reputation.

For Financial Promotions the regulatory requirements are that these promotions should be 'clear, fair and not misleading'. Post Office is required to establish, maintain and communicate to staff such systems and controls as are necessary for it to ensure that the promotional material it uses, displays and distributes in relation to the Products is:

a) Approved for use by POMS and BoI;
b) Current and up-to-date; and
c) Withdrawn in accordance with any instructions provided for this purpose

2. What framework is in place to ensure compliance with these obligations?

Governance

Post Office

POL00423565

In Post Office, FS and network risks are overseen by regular reporting into the Risk and Compliance Committee and the Audit and Risk Committee. The Post Office CEO is the FCA Approved Person, the General Counsel is responsible for ensuring we have the appropriate framework in place to ensure compliance and the Network and Sales Director is responsible for ensuring compliant branch sales.

Post Office/BoI

PO risk report into the monthly Sales Oversight Compliance Forum (SOCF) which reports into the monthly Customer and Conduct Risk Committee (CCRC). As well as the respective teams from risk and compliance the CCRC has business representation from the Director of FS, the Network and Sales Director, senior business representation from BoI and the Chief Risk Officer of BoI.

PO/POMS

POMS has a monthly Risk & Compliance Committee. This is attended by the Post Office Head of FS risk and POMS Head of Risk and Compliance and their respective teams. This forum will report into the POMS ARC.

Management Information

The current focus of the MI is Post Office branch distribution as the Principals receive directly and oversee themselves compliance management information in respect of call centre and internet distribution directly.

The MI reported into these forums is currently being reviewed as part of the network conduct risk action plan to ensure that that there is adequate information to mitigate risk and to better assess the sources of assurance that are available in the first line.

The typical MI reviewed includes.

- Training and Competence reports
- Risk registers
- Regulatory Horizon scanning
- Reports into incident breaches
- Complaints reporting
- Compliance monitoring reports and planned activity

In addition to this, both teams will meet regularly to discuss compliance risks and issues as they arise.

There is also a Post Office/POMS/Bank of Ireland tripartite meeting. This does not report into a formal reporting 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.

POL00423565

Risk Management

Post Office FS has a comprehensive bottom up risk register across its product areas that are owned by each business/product area together with a Post Office FS 'top risks' register.

FS Risk requires that material new business initiatives (such as the CRM programme) are formally risk assessed. These business risk assessments are shared with the POMS risk team to review progress and understand compliance risks.

POMS also has risk management processes in place and risk registers that are shared and reviewed. Both POMS and Post Office registers are broadly aligned with a similar risk register structure building on best practice from group risk.

Post Office follows the incident reporting processes of 'group' and reports any relevant incidents and breaches into the POMS risk team.

Compliance

The POMS RGM and approach to compliance was largely adopted from that used by the Bank of Ireland. This is helpful in ensuring a consistency of framework across Post Office bearing in mind that the Bank has a higher risk portfolio of activities to oversee across the network. The FS risk team work together with BOI and POMS to ensure compliance, such activities include:-

- Working with the wider business to ensure compliance of business initiatives
- Following up on monitoring reviews
- Investigating compliance breaches and undertaking root cause analysis
- Working with the Principal on the design and approval of incentive schemes
- Design approval and oversight of T&C schemes
- Agreeing updates to policies and procedures including the RGM

3. What assurance is provided to Post Office and our Principals to demonstrate compliance?

The reporting referred to in section 2 above is the pre-dominant source of assurance provided to the Post Office. This has provided assurance to BoI since it became Post Office Principal in 2004. The risk approach agreed has been to prioritise focus on mitigating the distribution areas of greatest risk.

Therefore, mortgage specialists, who give mortgage advice and are subject to professional qualification requirements have the most extensive control and monitoring framework in place. This is followed by the focus on Financial Specialists who have customer appointments with customers and carry out a wider scope of assisted sales. Then more recently the CRM programme with its higher level of introductory customer engagement has had controls designed to manage these particular risks.

POL00423565

It is, recognised that more widely across the network further work needs to be done to improve appropriate local management ownership of compliance risks and to improve the MI and assurance in the first line.

However, this is set in the context of the sales processes and literature all being approved and re-approved by the regulatory Principal. For example, this would include Principal approval of all incentive schemes used in the network and the scripts and sales journeys for over 50s Life and travel insurance are all reviewed and approved by the regulatory Principal.

In the agency network, the move to CRM branches has put greater first line control around the sales process. This is because the enhanced introductory process has been backed up with dedicated line management reviewing compliance MI, the obligations of the dedicated Training and Competence scheme and line management reviewing monitoring MI such as video mystery shopping and customer validation calls. The programme currently stands at 400 branches but is expected to extend to up to 1,000 of our most active branches in the next 18 months.

Financial and Mortgage Specialists and CRMs

The assurance sources available for specialists and CRMs include detailed monthly MI reporting on compliance covering conduct risk. These reports cover accreditation, product knowledge testing, product sales, product mix, cancellations, complaints and the results of monitoring activity which includes video mystery shopping, customer validation calls and one off reviews such as T&C file audits.

There are, however, some gaps in this reporting that need to be filled such as not all products are currently covered by video mystery shopping. Complaints MI and processing also needs to be improved.

Counter colleague introductions and sales

The sources of assurance in the network include;-

- Network quality of sales MI. This is a report on network activity covering, sales broken down by branch covering product line, cancellations and complaints. This MI can be used to review spikes in activity or trends to investigate in the network.
- Product provider management information on sales, lapses, cancellations and complaints and any customer surveys conducted by them
- BoI team individual branch reviews, whilst they are now 'banking' focussed they provide key data on branch conformance. This includes non- accredited activity (branch staff acting beyond their remit such as offering advice), data protection, AML procedures and inspections for non-compliant brochures and financial promotions. This branch review activity has recently begun in POMS to supplement the oversight given by BoI.
- Intelligence reports received from BoI network coaching and development managers (CDMs). The 40 CDMs in the network provide to the risk team regular updates on any breaches uncovered in the network
- Social media monitoring tools. The social media team reviews the network using key word searches to pick up on non- compliant activity.

POL00423565

The conduct risk action plan identifies that further work should be done to identify the adequacy of current MI as well as the current use and first line oversight of the MI that is currently available.

4. What would the consequences be if Post Office failed to comply?

It is important to note that the MI reviewed to date by Post Office and the regulatory Principals has identified past and current control failures in the network that have led to appropriate mitigating action. For example, recent social media monitoring had identified unapproved financial services promotions on agency branch websites in breach of Post Office requirements. As a result rapid mitigating action was taken to close the sites down and social media training has been given to area managers to ensure that good and poor practices are communicated across the network, together with enhanced monitoring.

There have been no systemic or significant risks (eg mis-selling resulting in customer detriment) under the current POMS or BoI principal relationships that have led to regulatory action. Nevertheless section 5 below (further actions) does outline a number of improvements to the controls in the network that are being deployed.

The RGMs states that Post Office must establish, implement and maintain systems and controls to ensure that the Principals are notified of any material or significant breach of the RGM or any regulation, law or voluntary Code of Practice applicable to Post Office in relation to the distribution of the Products for which they are responsible.

Post Office has systems in place to report any breaches to BoI and for POMS it uses the 'Group incident reporting' processes. The consequences of any breach would depend on its nature and if it was reportable to the regulator based on an assessment of materiality by the Principal. A significant breach as well as having regulatory consequences could lead to reputational damage to Post Office as well as any regulatory fines or censure that was imposed.

Under the AR agreements the Principals ultimately would be entitled to suspend any or all relevant Post Office activities that are not compliant with the AR agreement, the RGM or other regulatory rules.

Whilst the FCA senior managers' regime does not currently apply to Post Office, the direction of travel clearly is to make directors/senior managers personally responsible for systems and controls breaches in areas they control or are responsible for.

5. What further actions should Post Office take to ensure compliance?

As reported above the FS Risk team has undertaken a comprehensive risk assessment of the wider 'network risks', reviewing FCA best practice guidance including the FCA's performance management guidance FG 15/10. The action plan has been shared and agreed with the network lead team and is reported to both POMS and BoI on a monthly basis. Both Post Office and POMS risk registers have

POL00423565

compliance and conduct risks as key areas that require on-going actions to mitigate.

The systems and controls surrounding a) FSs, MSs and b) CRMs, are established. The FS risk team has driven risk management disciplines around these sales structures and oversee, training and competence regimes that are regularly tested, together with regular compliance monitoring tools and accompanying reporting MI that is reviewed.

We have developed plans to ensure that as these sales models evolve (for example the CRM population is expected to increase) the control environment is maintained commensurate with the scope and size of future activity.

There are however identified gaps and risk areas where further improvement is being implemented, many of these are captured in the Post Office conduct risk action plan. The conduct risk plan was put in place in February and is broadly on track. However, it is recognised that this is a significant programme of change to implement.

This action programme is fully supported by the network lead team and covers further work to improve controls in the following thematic areas.

- Sales Model risk assessment and external review of conduct risks in sales model *(This is a key area to assess whether the sales model could drive conduct risk, internal assessment by Q1, external review Q2).*
- Training and Awareness of conduct risk and regulation for all relevant staff from the General Executive downwards.(*This work has begun with training of GE, specialists and FS trainers, a plan is in place to extend training coverage across FS and the network split into two stages 'conduct risk awareness' and 'conduct risk application' to be complete by December 2016)*
- Performance management communications and incentives (*Performance management and communication form part of the training work above and includes ongoing monitoring of communications. Recent work has been completed to strengthen and regularise the existing incentive schemes, FS risk needs to oversee the performance of scheme governance in Q1 and Q2).*
- Review of staff performance processes (*this has been reviewed and completed and found to be appropriate)*
- Process to review exit interviews for conduct risk issues (*alert to FS risk team now in place)*
- Enhanced whistleblowing policy and communication plan (*Policy review complete, awaiting update on communication plan Q2)*
- Staff assessment and vetting (*This will be a significant piece of project work driven by HR completion date Dec 2016*)

POL00423565

- Comprehensive review of MI, quality and quantity and first line review and oversight (*This will review the MI available, whether this is appropriate, who should review it and how action is taken as a result Q2*)

The 2015 PWC Internal Audit review on Post Office FS conduct risk also reported that further action should be taken in this regard:

Priority recommendation
Post Office to perform further work in the identification and assessment of conduct risks across the financial services business in order that a complete conduct risk universe is captured and monitored going forward.

This action was completed in 2015 with a detailed risk assessment performed in partnership with BoI who were Post Office's sole Principal at the time. The outcome of the risk assessment was the conduct risk action plan outlined above.

Priority recommendation
…, we are supportive of the recommendation for a more detailed assessment of the adequacy of the current regulatory and conduct risk controls in place to manage and monitor the individuals employed by Sub-postmasters and Multiples. If not already done so, we recommend that Post Office conducts the more detailed assessment as soon as possible and where inadequate controls are identified, introduces an action plan to address.

The risk assessment conducted in 2015 and the resulting action plan covers this area of risk. This encompasses the training, vetting, management information and oversight work streams.

<u>Facilitating evidence of controls and oversight for Over 50s Life and Travel Insurance sales</u>

Over 50s Life and Travel Insurance sales now have updated and approved training and sales processes in place and MI for Post Office/POMS to review activity (such as sales trends, cancellations and complaints). The gaps are around being able to improve the oversight of the efficacy of these arrangements. For example, for CRMs and specialists we undertake video mystery shopping to assess competence, compliance and customer experience. This is not undertaken in the wider network and as part of the conduct risk action plan we are reviewing what other assurance can be put in place. For example, there are action points, for Post Office Risk and both Principals to:-

- *Review existing monitoring programme with BoI/POMS to identify areas of risk and significant gaps by* 31/5/2016
- *To review the key data that is available or can be obtained on a cost effective basis to oversee conduct risk by* 31/05/2016.

POL00423565

Staff vetting

Post Office is reviewing its vetting policies and procedures to ensure that they reflect industry recognised practice. Whilst there are detailed policies and procedures in place for Mortgage Specialists and their managers, the wider policies and procedures need improving to reflect best practice (e.g., current practice includes criminal record checking but does not, for most staff, cover credit checking)

FS Risk and POMS and have given HR feedback on what the minimum regulatory standards should be for vetting and progress on this is being tracked with HR.

Third Line reviews (Internal Audit) reviews 2016/17

Internal Audit supported by PWC are conducting three further relevant reviews this year. These are:

- FS-Branch network sales Training and Competence Review, reporting to Post Office ARC Sep 2016
- FS-Branch network sales process review, reporting to Post Office ARC Jan 2017
- FS-Branch Network sales quality review, reporting to Post Office ARC Mar 2017

The scope of the audits will be reviewing the systems and controls for specialists, CRMs and counter colleagues. This will be an important 'third line of defence' review to benchmark Post Office's assessment of the control environment.

Jonathan Hill
Head of FS Risk
Post Office

POL00423565

7) Annual report on operation of gifts and hospitality procedure

Author: Georgina Blair Sponsor: Jane MacLeod Meeting date: 05 May 2016

Executive Summary

Context

Post Office has had a Gifts and Hospitality procedure in place as part of its anti-bribery procedures since June 2011. The purpose of this paper is to update the Risk & Compliance Committee on the operation of the Gifts and Hospitality procedure in Post Office over the past year.

Questions this paper addresses

1. How many reports of gifts and hospitality were made in in the year to 28 February 2016 and by which business units?

2. How does this compare to last year?

3. Is the gifts and hospitality procedure operating properly as part of our anti-bribery procedures?

Conclusion

1. 305 reports were received in the year to 28 February 2016. The highest number of reports were from Financial Services; some business units reported very little gifts and hospitality.

2. Overall this is more than last year but reporting patterns are similar to last year.

3. There is evidence that most lead teams understand the need to report and ask for authorisation when offered gifts and hospitality, but that these reports are not always passed on to the Central Risk Team to record on the central register. Instead reports are held at local level. The gifts and hospitality reporting procedure needs to be better publicised as it forms a key part of our anti-bribery procedures. Awareness and compliance will be improved by:

- Including the gifts and hospitality procedure in Anti-Bribery training which is currently overdue given our contractual arrangements under the MDA.
- Updating the presentation of the gifts and hospitality procedure on the intranet to make it easier to find
- Working with HR to ensure the procedure is included in an improved induction process.

Input Sought

The Committee is asked to review the report and approve the proposed actions. ARC will be updated on the operation of the procedure as part of an annual anti-bribery update in March.

POL00423565

Appendix 1

Summary of reports to the Gifts and Hospitality register in the year to 28 February 2016 and a comparison for the year to 28 February 2015

Area	**1 March 2015 to 28 Feb 2016**				**1 March 2014 to 28 Feb 2015**			
Business Unit	Total reports of gifts received	Total reports of hospitality received	Reports of gifts received by GE members**	Reports of hospitality received by GE members**	Total reports of gifts received	Total reports of hospitality received	Reports of gifts received by GE members**	Reports of hospitality received by GE members**
Business Transformation	0	1	0	1	0	0	0	0
Commercial	0	33	0	0	0	3	0	0
Corporate Services	1	28	0	2	0	27	0	2
Finance	0	3	0	3	1	13	3	4
Financial Services	3	203	3	26	3	85	1	29
Operations*	0	14	0	7	2	25	2	14
Network and Sales	3	10	0	1	7	18	0	3
Office of the Chief Executive	0	4	0	4	0	19	0	19
People & Engagement	0	2	0	0	1	0	0	0
Total	**7**	**298**	**3**	**43**	**14**	**190**	**6**	**71**

* Operations includes POL IT, Supply Chain and Procurement

**Reports of gifts and hospitality received by GE members are included in the totals for each business unit.

POL00423565

POST OFFICE
RISK AND COMPLIANCE COMMITEE

DECISION PAPER

8) Review of whistleblowing procedures in 2015/16

Author: Georgina Blair Sponsor: Jane MacLeod Meeting date: 05 May 2016

Executive Summary

Context

The purpose of this paper is to update the Risk & Compliance Committee on the operation of the whistleblowing procedures in Post Office over the past year.

Questions this paper addresses

1. Is the whistleblowing policy fit for purpose?
2. Has the policy been complied with in the year?
3. How many reports of whistleblowing reports were made in the year to 31 March 2016 and how does this compare to last year?
4. What else needs to be done?

Conclusion

1. The whistleblowing policy has been updated and needs to be approved (see agenda item 5).
2. The whistleblowing procedure is operating but needs to be publicised more.
3. Seven reports were received (see Appendix 1 for summary). This is more than last year, when a total of three reports were received, but still a low number given the total number of employees in Post Office. A large number of calls are made annually to the Security reporting line 'Grapevine' and it is likely that some of these calls could be classed as whistleblowing reports, but there is currently no mechanism to distinguish them.
4. Implementation of the updated whistleblowing policy will require training and awareness activities. ARC will be updated on the operation of the policy and procedures annually in March.

Input Sought

The Committee is asked to review the report and approve the proposed actions.

POL00423565

The Report

Is the whistleblowing policy fit for purpose?

1. The whistleblowing policy has been revised and updated. As part of the process our external auditors reviewed it for compliance with the new whistleblowing regulations for the financial services sector.

Has the policy been complied with in the year?

2. The previous version of the whistleblowing policy was complied with during the year, but awareness of the whistleblowing line among employees is low.

How many reports of whistleblowing reports were made in in the year to 31 March 2016 and how does this compare to last year?

3. Seven whistleblowing reports were received in the year to 31 March 2016 (see Appendix 1). This is an increase on the previous year, when a total of three calls were received. This is still a low number given the total number of employees within Post Office.

What else needs to be done?

4. The updated policy needs to be implemented. As part of this awareness of the policy, the correct method of dealing with whistleblowing reports and the availability of the Speak Up line and other methods to report whistleblowing will be communicated to all employees.

POL00423565

Appendix 1

Summary of whistleblowing reports in the year 2015/16

Number	Date	Subject of report	Mode of contact	Action	Result
1	September 2015	Behaviour of senior management	Verbally to GC	Investigated – insufficient evidence to support allegation	Closed
2	November 2015	Activity of postmaster	Speak Up Line	Investigated – no evidence found	Closed
3	December 2015	Procurement process	Verbal to Legal team	Further information requested	Closed
4	January 2016	Relating to Sparrow investigation	E-mail forwarded from Lord Arbuthnot	Investigation to confirm whether matters have been addressed	Closed
5	January 2016	Activity of postmaster	Speak Up Line	Investigated – no evidence found	Closed
6	January 2016	Employment matters within third party	E-mail to Paula Vennells	Referred to third party and investigated in conjunction with them. No evidence of misconduct.	Closed
7	March 2016	Activity of colleague in branch	Speak Up Line	Investigated and matter resolved without intervention.	Closed

POL00423565

POST OFFICE
RISK AND COMPLIANCE COMMITTEE

9) AML and CTF Risk Update

Author: Tom Basquille Sponsor: Jane MacLeod Meeting date: 5th May 2016

Executive Summary

Context

This paper updates the Risk and Compliance Committee on progress with the HMRC Regulatory Activity project which has been established to manage both the HMRC's Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) audit, and to progress the recommendations set out on 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. A steering group has been convened to oversee the assessment and implementation of the Promontory recommendations, and to manage the HMRC compliance audit activity. The Steering Group includes representatives from key impacted areas such as Network (inc. Supply Chain), People & Engagement, and Financial Services. External financial crime legal specialists have also been engaged.

HMRC Audit

2. POL continues to work closely with HMRC through the current 'Discovery' phase of the Audit. Following requests for information from HMRC, we have provided a significant amount of information covering areas such as Branch Registration, FRES Data and Sub-Postmaster On-boarding processes.
3. HMRC has also requested transactional information on the regulated services provided by POL and documents such as the current Bureau workbook have been supplied. In addition, HMRC's lead representative, Lee Simpson has been hosted in Model Office at Finsbury Dials to observe operational processes and procedures for these transactions.
4. In relation to branch audits, HMRC have indicated that they propose to conduct hosted visits at two Crown Offices and at one WH Smith branch, and a visit to one branch of each of the next three largest agents – all within close proximity to Finsbury Dials. We have notified WH Smith and the other multiples of the fact of the audit and that a visit is likely. These visits will be used as an 'educational tool' for the main audit comprising scheduled visits by HMRC only to circa. 150

POL00423565

independent branches. We will have the opportunity to comment on the proposed list of branches to be visited and agreed communications will be issued to each branch at least a week prior to the visit.

5. As the HMRC's approach to the audit emerges and the links to Promontory Report's recommendations are established, we will develop the engagement plan for external stakeholders including Treasury, BIS, FCA and Bank of Ireland.

AML training

6. AML compliance training was rolled out to all staff during March and was released to the Network in the week commencing 25th April. Agents will be able to access the training via Horizon On-line and the mandatory test though Horizon itself. A communications framework is in place to promote this regulatory training, including a Message Broadcast on the launch date.

Promontory Report Recommendations

7. Recruitment is underway for 2 roles required to implement the recommendations arising from the Promontory Repot. These roles are (i) an AML analyst to be based in Chesterfield supporting activity such as the Suspicious Activity Reporting and transaction monitoring; and (ii) an AML Manager Role to be based in London, focussing initially on priority tasks such as the AML/CTF Risk Assessment. The Risk Assessment is itself a key recommendation and the output of that work will inform our approach to many of the other recommendations.

8. Many of the recommendations made in the Promontory Report relate to improvements in current processes and procedures such as implementing product risk assessment tool, transitioning to electronic suspicion reports and increasing training and awareness, and the viability of these will be assessed during the project.

9. A breakdown of the areas of focus within the Promontory Report is provided below. Further detail of these recommendations and progress against them will be provided at the next RCC update.

	Priority		
Area	**Level 1**	**Level 2**	**Totals**
Governance and Culture	2	1	3
Risk Assessment	7	4	11
Policies & Procedures	7	7	14
Monitoring Arrangements	3	1	4
Operation of relevant systems and processes	0	4	4
Training, Awareness and Testing	4	2	6
Suspicion Reporting	4	2	6
MSB	5	2	7
Resourcing	3	1	4
	35	**24**	**59**

POL00423565

10) Property compliance update

Author: Steve Norris Sponsor: Thomas Moran Meeting date: 05 May 2016

Executive Summary

Context

This paper addresses the request made by the Audit and Risk Committee (ARC) on the 17th of March to receive an update on Property Compliance Governance.

Questions this paper addresses:

1. What improvements have been made to property compliance governance?
2. What progress has been made to address the other property compliance issues raised in the March audit report?
3. What remains to be done?

Conclusion

1. The Property team, assisted by the Post Office Legal and Risk and Audit teams and Property experts from BNP Paribas, has completed the assessment of the key risks and the prioritisation of any remedial projects.

The Property team has assessed its operating model and specific monitoring controls over Property regulatory including environmental and H&S risks have been clearly assigned within the Property Team and service suppliers. Engagement and co-ordination processes have been established with stakeholders from other business units.

2. There has been significant progress towards achieving full property regulatory compliance since the last update. Work to remedy identified high risk items has been completed and plans have been developed and included in our 2016/17 budget for dealing with identified medium risk remedial works.

3. Further work is needed to improve the culture of prioritising the identification and reduction of property and health and safety risks at operational sites, including the prevention of fire hazards. This will be achieved by closer working between the Property (Steve Norris), Health and Safety (Martin Hopcroft) and Network Operational teams (Steve Blampied) and branch manager training by the H&S Team which will be completed by June.

POL00423565

4. The future stability of the Property and Health and Safety team members is a key component of successful property compliance and must be addressed.

Input Sought

The Risk and Compliance Committee is asked to approve this report for submission to the Audit and Risk Committee.

POL00423565

The Report

What improvements have been made to property compliance governance?

1. The Property team is implementing improvements against five pillars of good governance processes:

(1) Leadership, accountability and culture

a. The desired risk appetite has been discussed with all property and facilities management suppliers (H&S team is aware of the business risk appetite).
b. The scope and responsibilities for service suppliers and Facilities Managers have been reviewed and H&S responsibilities have been clearly assigned to them.
c. Representatives from Network and Health and Safety teams will attend the monthly Property Compliance Forum which provide oversight of all the key property related H&S risks and incidents.

(2) Structure, processes and performance oversight

a. We have re-prioritised the role of Facility Managers to focus on identifying and minimising the higher risks within the property estate and the suppliers' operations. -We have recruited a senior Facilities and Compliance Manager, additionally we are training an existing employee as an assistant Facilities Manager. "Duty holders" and "Responsible Persons" roles have now assigned to POL staff, but Duty Holders will need changing from Kevin Seller as a result of Post Office restructuring.
b. Training for the Post Office property team, Duty Holders and Responsible Persons on key statutory compliance areas is ongoing and will be completed by the end of June.
c. Facilities Management suppliers' competency has been self-assured against best standard.
d. Relevant policies and handbook have been reviewed and will be signed off shortly.

(3) Risk Monitoring

a. Assessment of the key risks and the prioritisation of any remedial projects have been completed.

POL00423565

b. The development of the compliance controls framework, which defines the ongoing compliance controls across the property estate for all the key stakeholders, has been almost completed, pending update on Person in Control ("PiCs") and Facilities Managers new responsibilities.
c. Facilities management contractors' polices, compliance regimes have been checked and approved by the Post Office Property team.
d. Relevant policies and handbook have been reviewed and will be signed off shortly.

(4) Engagement with stakeholders

a. Continue integration and co-ordination with other key H&S team has improved and we are now attending each other's planning meetings and report jointly.
b. Compliance communication and planning with facility management suppliers has improved with visibility of their performance via attendance to the Property Compliance Forum and formal monthly supplier operational meetings.

(5) Management of information

a. Regular incidents/near miss reports are being produced by facility/estate management suppliers and discussed at the Property Compliance Forum.
b. Board/Committee papers: a joint monthly report including H&S and Property will be issued to the Group Executive team on property compliance issues from April onwards

What progress has been made to address the other property compliance issues raised in the March audit report and what remains to be done?

1. Regulatory risk progress

There has been significant progress towards achieving full property regulatory compliance including reducing the risk of breaches of health and safety and environmental law since the last update.

2. Property regulatory compliance risk assessments

Risk assessments have now nearly all been completed by our suppliers (see Appendix 1). There has been some slippage owing to practical difficulties encountered by our suppliers e.g. difficulties gaining access and reliable information. Work to remedy identified high risk items has been completed and plans have been developed and

POL00423565

included in our 2016/17 budget for dealing with identified medium risk remedial requirements; mainly electrics, asbestos, building fabric and legionella.

3. Electrical testing

Electrical testing is now 91% complete. There has been a 1 month slippage due to access issues, but these assessments will be 100% complete in May.

4. Residential risk assessments

Residential risk assessments for fire and fixed wire testing are ongoing due to be completed by the end of May and lower risk water risk assessments (which are not a statutory responsibility) by the end of May. Remedial works such as fitting smoke alarms and carbon monoxide should all have be fitted by the end of April. External fabric of residential properties has been assessed. Internal inspections have only highlighted damp issues at one property. Gas inspections are also complete.

5. Environmental law

There has been significant focus on waste management across the POL estate to avoid fixed penalties and other enforcement being taken against POL. Regulation concerning the management of waste is restrictive and easy to breach. POL is reliant upon Servest and our PiCs to ensure compliance. Servest have retrained and communicated with their staff the need for strict compliance and POL has sent communications to PICs followed up by phone calls to ensure their responsibilities are understood. This is an area of ongoing concern as breaches are still occurring. We have an action plan in place now with Servest to address this. While the most usual enforcement is by small fixed penalty fines £50 to £100 we have faced prosecution for abandonment of waste outside our own premises (successfully defended) where the fine could have been within a range of £7K to £25K.

POL's annual Carbon Reduction Submission was completed and submitted to the Environment Agency in September last year for the year 2014/15. The Environment agency additionally carried out an audit on the previous year's submission in 2013/14 which was also found to be satisfactory.

.

POL00423565

6. Fire risk and housekeeping

The most significant area to improve is in housekeeping to manage fire risk. This was reported by CBRE to the Property Compliance Forum as a finding from their risk assessments, currently carried out over 93% of the estate.

PiCs are being issued with the results of the fire risk assessment audits from CBRE and requested to address any areas identified. We are defining a process which will provide assurance that all steps to address risk have been actioned.

Many PiCs are Managers who have relocated, are new in post or are simply overdue a refresh of their original training. A H&S led PiC training programme has also started and due for completion in June. This is outlined in Appendix 3.

We are engaging with Network Operations to propose the implementation of:

a) Peer to peer compliance review in accordance to industry best practices or an equivalent alternative process. This will be actioned in May.
b) Regular reviews and appraisal of PiCs Property compliance performance by their line managers.
c) Clear audit trail of compliance actions identified and resolved.
d) Improve communications processes between Property, Network Operations and H&S teams.

7. Leadership, accountability and culture

Work is ongoing to ensure that the culture of health and safety across the business is aligned to the 'risk averse' appetite for the areas where opportunities to improve have been noted. The plan in summary is as follows:

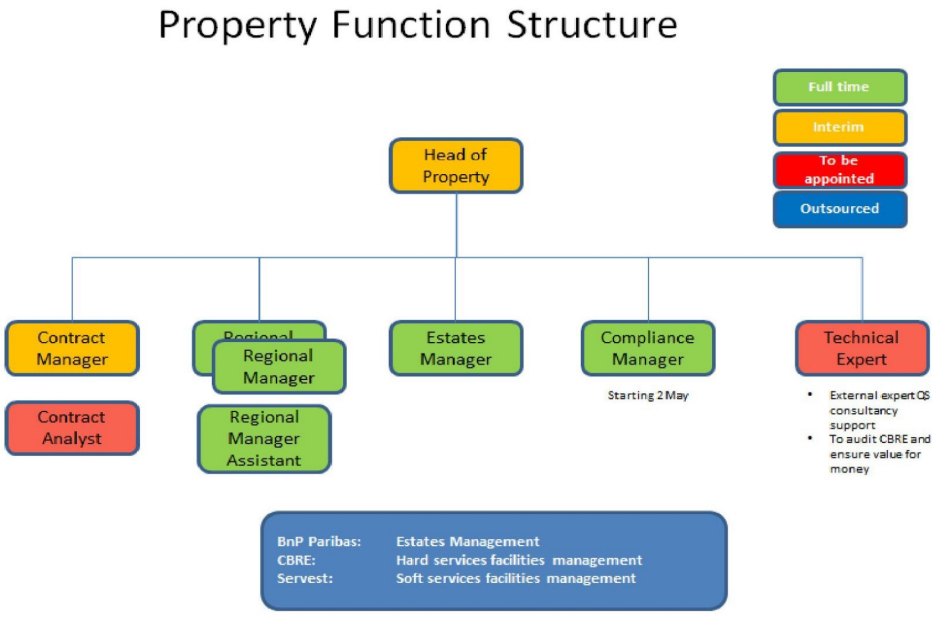
7.1 Compliance programmes addressing the risk assessments as set out in Appendix 1 will be completed in the financial year 2016/17. The Compliance Forum, chaired by Steven Norris, is the entity which will manage completion of this programme of work. The delivery of compliance works will be undertaken by CBRE.
7.2 Site by site risk assessments will be produced by CBRE, who manage the high risk areas and enhanced with insights from Servest and the H&S team. This will be live from April onwards for consideration by the Compliance Forum. This risk based view will be used to prioritise site visit audits by POL's Facilities Managers to ensure high risk areas are continually identified and addressed either through the PiCs, CBRE, BNP the H&S teams or Servest. This will be an ongoing process in perpetuity and key risks will be escalated up to the RCC and POLs Exec through monthly reporting from the Compliance Forum.

POL00423565

The role and responsibilities of the PiCs and training needs are being reviewed by the H&S and property teams in May. The Network Operations Team has been engaged and they will attend the Compliance Forum to ensure that PiCs responsibilities get implemented and monitoring mechanisms of their activities are established by June.

8. Structure, processes and performance oversight

The future stability of the Property and Health and Safety teams must be assured in order to enable the implementation of the new operating model and ensure that appropriate property regulatory compliance including health and safety matters are properly addressed and monitored going forward. The structure of the Property Team is shown below:



(Note: the above structure exclude: Crown Transformation and NT and Equipment teams. These teams have a different reporting line)

There are additional statutory roles of Duty Holders and Competent persons required under environmental law, health and safety law and other statutory compliance, for each of the 14 areas of compliance. These roles have all been defined and individuals appointed within the Post Office. The table at Appendix 2 explains these roles and the appointee. In addition the role of Competent Person is fulfilled by our suppliers, Servest and CBRE and their competency has been

POL00423565

recently checked. Due to internal restructuring, the Duty Holder will have to be re-appointed from Kevin Seller.

The business should be aware that in the event of enforcement, the relevant authority may look to enforce against Group Executive Members and Directors.

The compliance controls activities for PiCs and H&S teams are to be finalised and integrated with the activities of the Property Team and a final meeting to implement this is planned on 25th May.

There is ongoing work to improve the management of risks across the estate and risk reporting. Particular focus will be given to shared premises and third party occupied properties where obligation may be shared especially between Royal Mail Group (RMG) and POL. A programme of work covering these risks is being prepared by CBRE which will then need to be for action to by RMG.

9. Risk Monitoring

The compliance control framework has been developed which has addressed critical areas. Other priority areas are now being addressed. Amended policies will be signed off and implemented.

The Property Compliance Forum recommended that once the new operating model and compliance governance framework has reached business as usual, an operating benchmark exercise is carried out to ensure that structure and processes in place are designed and operating as expected for an organisation of this size and complexity. We anticipate this to be around August.

10. ARC and RCC support

Continued support is required from the ARC and RCC to ensure all involved give these objectives the high priority they demand and that behaviours are fostered and appropriate decision are taken to fully support these objectives.

POL00423565

Appendix 1

Status of compliance risk assessments

Planned Maintenance	% inspected	Risk	Completion date	Next steps
Fire Risk Assessments	93%	M-H	End May	13 sites remaining. Cultural improvements still needed at sites
Asbestos	99%	M	30 April	All high risk items access controlled while containment is completed. Huyton CO (Vacant) is still outstanding due to difficulties in obtaining access
Radon	100%	L	Complete	No risk areas identified nor unlikely to be in phase 2 assessments
TM44	100%	L	Complete	Highly inefficient boilers, coolers and lighting systems being replaced in 2016
Lift Insurance Inspections	100%	L	Complete	Minor defects remedials actioned to Lift service contractor
PAT Testing	100%	L	Complete	Minor issues. All have been addressed
Fixed Wire	91%	M	End May	All high risk areas addressed. Medium risks will be addressed in 16/17
Pressure	100%	L	Compete	No issues
Energy Certificates	100%	L	30 April	Minimal issues. Reports now being received
Legionella	91%	M	End May	43 remaining, these are being planned to be completed within May
Building fabric	100%	M	Complete	Mainly security and access risks which will be addressed in 16/17

Note: This table explains the recovery of the backlog of overdue risk assessments over the last 6 months. Going forwards risk assessments will be undertake on a rolling programme as they become due.

POL00423565

Appendix 2

Duty holder and Responsible Persons roles and appointed person

STATUTORY RESPONSIBILITIES					
TOPIC	**LEGISLATION**	**Main Regulatory Bodies** (provided by Ashfords- legal firm) other bodies may regulate some aspects of these topics, e.g. Food Standard Agency, FinancIAL Conduct Authority)	**RESPONSIBLE PERSON**	**JOB TITLE**	**DUTY HOLDER**
1. Electricity	Electricity at Work 1989 (Regulation 3)	Health and Safety Executive Local Authority	**Steve Norris**	Interim Head of Property	**Kevin Seller**
2. Legionella Management	The Control of Legionella Bacteria in Water Systems (AcoP L8) & The Notification of Cooling Towers and Evaporative Condensers Regulations (1992)	Environmental Agency	**Kevin Harris**	Facility Manager	**Kevin Seller**
3. Waste	Environmental Protection Act 1990, Section 34.	Environmental Agency	**Cherly Hurd**	Facility Manager	**Kevin Seller**
4. Asbestos	The Control of Asbestos Regulations 2012, Regulation 4	Health and Safety Executive Local Authority	**Andy Mason**	Equipment, Facilities and Deployment Manager, Service Delivery	**Kevin Seller**
5. Health & Safety	The Health and Safety at Work Act 1974, Section 4 COSHH regulation Environmental Liability Directive	Health and Safety Executive Local Authority Natural England (i.e. Environmental Liability Directive)	**Martin hopcroft**	National Safety, Environment & Wellbeing Manager	**Martin Hopcroft**
6. Pressure Systems	Pressure Systems Regulations 2000	Health and Safety Executive	**Steve Norris**	Interim Head of Property	**Kevin Seller**

POL00423565

STATUTORY RESPONSIBILITIES					
TOPIC	LEGISLATION	Main Regulatory Bodies (provided by Ashfords- legal firm) other bodies may regulate some aspects of these topics, e.g. Food Standard Agency, FinancIAL Conduct Authority)	RESPONSIBLE PERSON	JOB TITLE	DUTY HOLDER
7. Lifts & Lifting Equipment	Lifting Operations and Lifting Equipment Regulations 2008	Health and Safety Executive Local Authority	Kevin Parkin	North Network Change Manager, Property	Kevin Seller
8. Fire	Regulatory Reform (Fire Safety Order) 2005 & Part 3 of the Fire (Scotland) Act 2005, supported by the Fire Safety (Scotland) Regulations 2006.	Health and Safety Executiv	Martin Hopcroft	National Safety, Environment & Wellbeing Manager	Kevin Seller
9. Natural Gas Systems	Gas Safety (Installation and Use) Regulations 1998	Health and Safety Executiv	Steve Norris	Interim Head of Property	Kevin Seller
10. Construction/Projects	Construction (Design & Management) Regulations 2015	Environmental Agency Health and Safety Local Authority	Andy Mason	Equipment, Facilities and Deployment Manager, Service Delivery	Kevin Seller
11. Ionising Radiation	Ionising Radiation Regulations 1999		Steve Norris	Interim Head of Property	Kevin Seller
12. Carbon	Carbon Reduction Commitment		Kevin Harris	Interim Head of Property	Kevin Seller
13. Environmental & Sustainability		Environmental Agency Health and Safety	Kevin Harris	Facility Manager	Kevin Seller
14. F-Gas		Health and Safety	Steve Norris	Interim Head of Property	Kevin Seller

Note: The Duty Holder Kevin Seller needs to be re-appointed as a result of internal restructuring at Post Office. Deputy Responsible Persons are covered by the property team.

POL00423565

Appendix 3

PiC training approach

Context - There was a requirement to refresh the content of the online Person in Charge training product and make available to all PiCs across the Post Office Estate. Although this was recognised by the Health & Safety Team, this was also a recommendation through the Property Compliance Risk Review.

Reason - Many PiCs are Managers who have relocated, are new in post or are simply overdue a refresh of their original training. Due to IT issues, it has been difficult to update the previous version of the PiC Training and therefore a new product has been created and is currently being tested by our external provider and H&S Business Partners.

Topics – The PiC training covers the general PiC duties and areas of responsibility including Health & Safety Duties, undertaking risk assessments, hazard surveys, ensuring Site Log Books are maintained, keeping H&S training records, fire risk assessments and training, evacuation plans, testing fire alarms and emergency lighting, knowledge of RIDDOR and control of contractors including signing in logs.

Assurance – The H&S Business Partners will have access to Certificates of Compliance with dates that PiC training has been completed and these will be supported by a central view of certification of PiC training module completion via the Training team. There is a requirement for PiC Training to be refreshed every 3 years.

Inspections – These are undertaken by Trade Union rep Inspections (2 per year) and H&S BP Audits at high risk sites. Facilities Managers will also be auditing high risk sites and undertaking property audits. At all inspections and audits the question will be asked whether the PiC training has been undertaken and certificate in date.

Timescales – The new product has been returned to the H&S Team for final review and it is expected that the PiC Training will be launched across POL be the end of May 2016. Local Risk Assessments will be completed in May / June 2016 at all sites and the Certificates of Compliance collated and checked in June 2016.

POL00423565

11) Modern Slavery Act - update

Author: Nisha Marwaha Sponsor: Jane MacLeod Meeting date: 5 May 2016

Executive Summary

Context

The Modern Slavery Act 2015 (the Act) challenges slavery, domestic servitude, forced and compulsory labour and human trafficking. Post Office is required to produce an annual slavery and human trafficking statement (Statement) setting out what steps have been taken to ensure its business and supply chains are slavery free. This paper attaches the Statement which must be approved by the Post Office Board and signed by a Director.

Questions this paper addresses

1. What specific risks should the board be aware of?
2. What action have we taken so far?
3. What are other businesses doing and how do we compare?

Conclusion

- Post Office has been undertaking due diligence on its business and supply chains to identify any risk areas.
- Post Office has prepared a Statement which must be published within 6 months of year end.
- A steering group appointed in January 2016 is responsible for creating a project plan and undertaking due diligence on Post Office's and POMS supply chains.
- The steering group has identified that the highest level of risk is within our Agency network. We will be taking action to address this risk including amending our contracts with our Postmasters to require compliance with the Act.
- Post Office's Statement has been prepared using Home Office guidance and in consideration of other available Statements by UK and international companies.
- Post Office will have to take ongoing action to meet the requirements under the Act.

Input Sought

The Committee is asked to note the contents of the Statement and provide any comments before it is submitted to the Board for approval.

POL00423565

The Report

What specific risks should the board be aware of?

- The requirement to publish a Statement applies to "commercial organisations" which (a) supply goods or services and (b) have a total turnover of not less than £36,000,000. It will therefore not apply directly to Postmasters if their turnover is less than £36 million per year.
  → However, Postmasters are part of the Post Office supply chain. Post Office must state what steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business.

- To date we have not identified any direct relationship with an individual or company registered in a high risk country.

- The due diligence that we have undertaken so far indicates that there is a potential risk on non-compliance within our agency Network:
  → The reason for this is that there are a large number of people employed by Postmasters (including multiple partners) but who are not employees of Post Office or POMS. They work directly for the Postmasters (including multiple partners). We will be taking action to address this risk (see below) including working to amend our contracts with our Postmasters to require compliance with the Act and we will be delivering training to Postmasters as and where it is appropriate.

What action have we taken so far?

1. GE member Neil Hayward delegated responsibility for our Modern Slavery initiatives to a steering group lead by Hannah Dalton (Head of HR). The steering group was appointed in January 2016.

2. The steering group has developed a project plan to carry out due diligence of our business and implement change. Our ongoing work involves a risk analysis of our core business and its related supply chains.

What are other businesses doing and how do we compare?

1. We looked at statements for international companies with complex supply chains to get a flavour for content and examples of initiatives.

   ➢ For example: **Ford**
   - They have published a statement which is approx. 2 pages long.
   - Ford recognise their supply chain is extensive and complicated and that it presents challenges.
   - Some of Ford's initiatives are similar to ours - this is encouraging given that Post Office's business and supply chains are not as extensive as Ford.

POL00423565

2. Many companies have not yet published their Statements, but we have looked at a variety to ensure that our approach is consistent. We are confident that the detail in our Statement and our project plan is appropriate at this stage, but we will monitor developments and keep the adequacy of the Statement under review.

3. We also looked at what some of our partners are doing:

WH Smiths

- Statement not yet published.
- They use the Ethical Trading Code of Conduct and Human Rights Policy. It incorporates the ILO Conventions to scope out the current position on Modern Slavery related matters.
- The policy specifies a person who takes responsibility for the Code.

Bank of Ireland

- Do not currently have a Modern Slavery statement.
- Publish a Responsible Business Report which currently makes no reference to Modern Slavery.
- As a key partner, Post Office should investigate directly with BOI as there appears to be very little in terms of Modern Slavery related matters.

POL00423565

Post Office Limited (Post Office) & Post Office Management Services Limited (POMS)
Modern Slavery Transparency Statement 2015-2016
May 2016

Executive Summary
This statement sets out the steps we have taken during the last financial year to ensure that Modern Slavery is not taking place in any of our supply chains or any part of our business. It is made pursuant to section 54(1) of the Modern Slavery Act 2015 (MSA).

Our business
Post Office is the UK's largest retail network and the largest financial services chain in the UK with more branches than all of the UK's banks and building societies put together. We have provided services for more than 370 years and currently supply more than 170 products and services (mails & retail; financial services; governments services; and telephony) from a Network of more than 11,500 Post Office branches nationwide.

Post Office directly manages currently over 300 of the Network branches. The remainder of the branches are managed on an agency basis by Postmasters and multiple partners.

Our supply chains
We currently operate throughout the UK, however our supply chains connect with suppliers with a global reach.

Banking services
Our banking services are provided through a joint venture with the Bank of Ireland (BoI).

Postmasters
Postmasters can operate one or more branches. As agents they have control on how they run their branches on a day-to-day basis. All those working in an agency Post Office branch are employees of the Postmaster.

Multiple partners
A large proportion of the agency part of our network is run by multiple partners.

Trade Unions
In our Crown network, we work closely with the Communications Workers Union (CWU) and Unite (CMA) Communications Managers Association.

Third Party Suppliers/Procurement
We also procure products and services from a wide range of national and international businesses.

Responsibility and due diligence
Responsibility for our Modern Slavery initiatives currently resides with a steering group which was appointed in January 2016. It is tasked with the development of a project plan to carry out due diligence and implement change. Our ongoing work involves a risk analysis of our core business and its related supply chains.

Where are the risks of Modern Slavery at Post Office/POMS?
To date we have not identified any direct relationship with an individual or company registered in a high risk country. The due diligence that we have undertaken so far indicates that there could be a risk of non-compliance within our agency network because there are a large number

POL00423565

of people employed by Postmasters (including multiple partners) but who are not employees of Post Office or POMS. They work directly for the Postmasters (including multiple partners). We will be taking action to address this risk (see below).

What we have done so far

- Our Whistleblowing Policy has been updated to include references to concerns about Modern Slavery.
- We have adapted the Post Office recruitment policy to address MSA requirements.
- We conducted an assessment of the Post Office procurement process to ensure it aligns with the MSA. As part of this process we conducted a review of the criteria used by Post Office to evaluate whether suppliers meet Post Office's minimum tendering requirements.

Next steps

Our work on Modern Slavery continues and we intend to introduce the following changes in the near future.

- Updating Postmaster's selection and appointment process to address MSA requirements.
- Amending our standard form procurement contracts.
- Developing a communication and training plan to ensure our suppliers, staff and agents are aware of Post Office's obligations in relation to Modern Slaver and informing them about the Modern Slavery Helpline.

Our policies

We currently operate the following policies that describe our approach to Modern Slavery:

- *Code of Business Standards*
- *Whistleblowing Policy*

Further information

If you have any concerns about the issues raised in this statement or if you think you have identified signs of Modern Slavery then please either contact us or call the Government's Modern Slavery Helpline on GRO

Signed: .....
Name: .....
Position: .....
Date: .....

POL00423565

12) 'Horizon Spotting' Report

Author: Jane MacLeod
Meeting 5 May 2016

Executive Summary

Context

As part of its remit, the Risk & Compliance Committee should consider legal, regulatory and other external developments on behalf of Post Office in order to ensure that impacts on Post Office (including its customers, staff, suppliers and stakeholders) are understood and being appropriately managed. This report highlights current developments of relevance to Post Office and the work that is being done to monitor these.

Questions this paper addresses

1. What are the material legal, regulatory and other external risks the Post Office executive and Board should currently be aware of?
2. What work is being undertaken to assess, monitor and mitigate these risks?
3. Who is accountable for this work and how will it be reported through Post Office governance structures?

Conclusion

1. There are a number of material developments which either will or could impact Post Office and details of these are set out in this summary.
2. In each case work is being undertaken to monitor and assess the risks arising from these developments. 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.
4. The status of those developments which have previously been noted to the Committee is set out in the Appendix.

Input Sought

The R&CC is asked to note these developments.

POL00423565

The Report

Gender Pay Gap

1. The government issued its 'Consultation on Draft Regulations' for Mandatory Gender Pay Gap Reporting on 12th February 2016. Responses to the draft regulations were required by 11th March. Post Office responded, primarily to raise limited concerns over some of the proposed definitions of 'pay'.

2. Gender Pay Gap differs from Equal Pay: Gender Pay focuses on the position of women in the workplace, as measured by pay, whilst Equal Pay is concerned with ensuring that employees are paid equally for work of equal value. It is possible to have a Gender Pay Gap without having an Equal Pay issue and vice versa.

3. Subject to parliamentary approval, the legislation will come into force with effect from 1st October 2016. Companies with more than 250 relevant employees will be required to provide information as defined by the legislation.

4. The information should be published on a searchable website accessible to both employees and to the general public. The information will also need to be uploaded onto a government website. In order to monitor progress the information will need to be held for three years. There is currently no intention to impose penalties for failing to publish.

5. Gender Pay will be measured as at April each year. The first year of reporting will be in respect of pay in April 2017 with the deadline for publishing being April 2018. The information will need to contain:

   - the mean gender pay gap;
   - the median gender pay gap;
   - the numbers of men and women in each of the pay quartiles;
   - the difference between the mean bonuses paid in the preceding year; and
   - the proportion of men and women receiving a bonus.

6. The Human Resources Service Centre (HRSC) is currently able to report easily on most of the definitions of pay, the exceptions being the treatment, for these purposes, of clothing, first aider, and fire warden allowances.

7. It is not proposed to begin to rectify these limited shortcomings until the legislation is finalised on 1st October. Keith Murdoch, Head of Reward has attended external meetings with stakeholders and, whilst there is overwhelming support for the intent behind the legislation, there is widespread concern about the quality and clarity of the draft regulations. It is prudent, therefore, to await the final version of the regulations which will likely see improvements in drafting.

POL00423565

Trade Union Bill

1. On 15 July 2015 the government published a new Trade Union Bill 2015-2016 proposing amendments to the Trade Union and Labour Relations (Consolidation) Act 1992. The Bill aims to reform various aspects of the law on industrial action and trade union obligations and activities. The proposed reforms include increasing ballot thresholds, extending the notice of industrial action required to be given to employers and, a new expiry date for action to be taken following a ballot. The Bill would also introduce more stringent requirements for unions to supervise picketing. Key proposals include:
   - Requirement for a 50% turnout, so that a strike would not be able to go ahead unless half of the eligible members cast a vote.
   - In the case of 'essential public services', such as health, education, fire, transport, border security and some nuclear workers, at least 40% of eligible members would have to vote in favour of action for it to be lawful. This is in addition to the 50% above.
   - A four-month time limit to be introduced limiting the period that can pass between a ballot authorising industrial action taking place and the action starting, and unions will have to give employers fourteen days' notice of the commencement of industrial action instead of the current seven.
   - The ballot paper should state the form of intended industrial action, and when it is to take place.
   - Permitting the use of agency workers to provide cover for striking employees.

2. The Bill is now in its 3rd sitting in the House of Lords after which it will move to the Commons for consideration of Lords amendments.
3. For Post Office, like other unionised businesses, the Bill, if passed in its current form, will provide greater notice of impending strike action. In addition the ability to cover strike action using agency workers (if approved) will assist in mitigating the potentially adverse effect of strike actions on Post Office operations.
4. The progress of the Bill through Parliament and the assessment of the impact of the changes is being monitored by the Industrial Relations team reporting into Neil Hayward.

POL00423565

Ofcom Review

1. On 16 June 2015, Ofcom announced a wide ranging review of the regulation of Royal Mail. The scope of the review is to ensure that the regulatory framework within with Royal Mail operates remains appropriate to secure the efficient and financially sustainable provision of the universal postal service (USO) against the backdrop of changes in the competitive profile of the market.

2. In July 2015, Ofcom published a Discussion Paper providing further detail on the context and purpose of the review and asked stakeholders to consider and provide answers to a number of preliminary questions on the appropriateness of its scope and lines of enquiry. Ofcom intends to complete the review during the course of 2016, with any recommendations for changes to the regulatory framework to be implemented in the same time period.

3. Self-evidently, any changes to the regulatory framework for Royal Mail has the potential to impact on our own obligations, particularly under the Mails Distribution Agreement, thorough which POL effectively provides services to enable Royal Mail to discharge the USO.

4. Accordingly, in its response to the Discussion Paper, POL put down a marker of its interest in the work of the review and POL representatives from the Mails and Public Affairs teams also met with Ofcom last autumn to establish an open dialogue. Discussions have also taken place with colleagues in the Regulatory Affairs Team at Royal Mail, in order to develop a shared appreciation of the likely direction of travel and to ensure that POL is kept abreast of developments.

5. No update or progress report has be forthcoming from Ofcom since the publication of the Discussion Paper, but we anticipate that it will come forward with some proposals in the near future, not least if it is to keep to its intended timetable. Any material developments will, of course, be reported as soon as they occur.

POL00423565

STATUS OF PREVIOUSLY REPORTED DEVELOPMENTS

Issue	Brief Description	Update
Money Laundering	Implementation of the recommendations in the Promontory Report HMRC compliance audit	1. POL continues to work closely with HMRC through the current 'Discovery' phase of the Audit and numerous documents have been provided in response to HMRC requests. 2. HMRC's lead representative, Lee Simpson has been hosted in Model Office at Finsbury Dials to observe operational processes and procedures for these transactions. 3. HMRC have indicated that they propose to conduct hosted visits at two Crown Offices and at one WH Smith branch, and a visit to one branch of each of the next three largest agents – all within close proximity to Finsbury Dials. We have notified WH Smith and the other multiples of the fact of the audit and that a visit is likely. We await details of the 150 branches likely to be visited over the summer. **AML training** 4. AML compliance training has been rolled out to all staff and is due to be released to the Network in the week commencing 25th April. 5. Recruitment is underway for 2 roles required to implement the recommendations arising from the Promontory Repot.

POL00423565

Issue	Brief Description	Update
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.
GDPR	New and more onerous EU Data Protection Regulation	Work is about to start on scoping the likely impact of the Regulations and the Directive on PO ahead of commencing activity to implement necessary changes.
Networks and Information Security Directive	New EU Directive to support GDPR	
Modern Slavery Act 2015	New requirements for due diligence and reporting obligations on supply chain	Statement prepared for release subject to Board review. Work will be ongoing to assess and monitor areas of concern.
Enterprise Bill	Proposals to cap termination pay of public sector employees to £95k	The Government has confirmed that the regulations will not come into force before 1 October 2016 and therefore all exits before that date will not be within the scope of the public sector exit payment cap.
Senior Managers' Regime	Statutory accountability of senior management in FCA and PRA regulated firms	No developments at this stage.
Mails – International Data Capture	Information collection requirements to support mails related dangerous goods requirements	No developments reported at this stage.

POL00423565

Post Office RCC 5 May 2016 FOR NOTING Paper 13

RCC 16/20 – 16/28

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

Minutes of an RCCC meeting held at
Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ
on 29th February 2016 at 10am

Present:	Susie Hayward (SH)	Head of Risk and Compliance (Chairman)
	Russ Tavener (RT)	Head of Commercial
	Gerry Barrett (GB)	Head of General Insurance
	Paul Jones (PJ)	Head of Travel
In Attendance:	Karen Oates (KO)	Deputy Head of Compliance
	Michael Brown (MB)	Insurance Operations & Regulatory Manager
	Elizabeth McMenemy (EMM)	Compliance Advisor
	Sanjeeve Thakrar	Risk Manager
Apologies:	Emma McGinn (EMG)	ISAG Representative
	Ryan Griffin (RG)	Head of Protection

RCC 16/20 WELCOME, QUORUM AND CONFLICTS OF INTEREST

(a) The Chairman declared the meeting quorate and open.

(b) SH received apologies from Emma McGinn and Ryan Griffin

RCC 16/21 MINUTES OF THE MEETING HELD ON 9 FEBRUARY 2016

The minutes of the meeting held on 9 January 2016 were approved and the Chairman was authorised to sign them as a true record of the meeting.

RCC 16/22 MATTERS ARISING AND ACTIONS LIST

(a) **Action PRCC 15/47 (m)** – ST to meet with POL BCP representative to discuss alignment of BCP plans and testing

(b) **Action PRCC 15/50 (a)** – GB confirmed that Junction will be responding to the consultation and will share details

(c) **Action RCC 16/08 (d)** – SH updated the meeting on the discussions with MI to produce MI. Action plan in place with POL and we will start to see improvements.

(d) **Action 16/14 (a), 16/15 (b) 16/15 (c), 16/15 (d), –** The meeting considered this action closed

POL00423565

(e) **Action 16/15 (a) –** ST to review and update the incident management process and circulate for the next meeting

(f) **Action 16/16 (e) –** GB noted that information is available and will be included in future MI

(g) **Action 16/16 (h) -** EMM noted that the reasons had been checked and correct

(h) **Action 16/16 (i) –** MB to review travel complaints with PJ

(i) **Action 16/17 (d) –** GB confirmed that Junction had provided an update on the Add-on position and the changes would be implemented with the timeframe

RCC 16/23 **RISK MANAGEMENT**

ACTION ST

(a) SH introduced Sanjeeve Thakrar (ST) as POMS new Risk Manager to the meeting. ST discussed the existing risk management framework and the need to work with each product heads to update the registers particularly controls, actions and dates currently recorded and assist with imbedding the framework. ST will be working through the register to update the scoring to the POL 5x5 table. PJ suggested that the likelihood table be updated to show the likelihood within the 5 year plan.

(b) SH reminded the meeting of the need to ensure the registers are maintained to enable accurate reporting of risk position to ExCo and Board. ST working on a dashboard to assist the reporting structure.

RCC 16/24 **INCIDENT MANAGEMENT**

ACTION MB

(a) The incident register was reviewed however noted that some of the known incidents had not been captured. MB to circulate the incident log again and requested each to ensure incidents are actions are up to date.

(b) New incidents discussed included the Brand Bidding websites and Data incident of data sent to Junction.

ACTION ST

(c) SH noted that the incident management reporting process was in need of refresh and recirculation to all staff. ST to review and update.

RCC 16/25 **1st LINE COMPLIANCE REPORT**

ACTION EMM/PJ

(a) The 1st line QA data was reviewed and discussed. The number of calls monitored by WH has reduced to 4 calls per agent consisting where possible to one sales, renewals, cancellation and MTA however the results were showing high numbers of sales and renewals as these are where the majority of the calls taken. The risk based approach was discussed and how WH are assessing the

POL00423565

risk. It was agreed that EMM would check the criteria and PJ to provide some guidance on areas to assess such as high medical screening and complaints RCA.

(b) Team leaders to provide additional oversight of 20 calls per team commencing on 1st March, training has been completed. Results will be provided to EMM to include in 2nd line reporting.

(c) Claims MI was reviewed with no deviation to trend and no issues identified. Noted that the Travel repudiation numbers had been previously understated and now amended.

(d) Cancellations and NTU's data was reviewed and noted no life data for January. Again, discussed the ability to obtain reasons for cancellations from Aviva and whether the cancellation rate was higher than market

(e) The complaints report was reviewed and noted that complaints had increased 54% since December however seasonally no increase from last January.

(f) Complaints for pet increased 93% relating to renewal costs. Noted that retention rate had remained within the target of 75%, currently running at 78%. Agreed that price increases would be monitored closely with the provider and discussions underway with Pinnacle to proactively manager. RT to check analysis

ACTION RT

(g) The meeting discussed the FOS referrals which are generally low however would be useful to obtain full information of FOS referrals and decision from providers.

(h) The MI received from POL was reviewed at the meeting including the VMW results, Training & Competence Report and CRM Report. The levels of QA available across different areas of the nextwork was discussed and the reasons for POL not being in a position to provide full oversight. The criteria for scoring and incentives were also discussed. It was agreed that as the MI from POL improved, greater value would be obtained.

RCC 16/26 **2ND LINE COMPLIANCE REPORT**

(a) The 2nd line compliance report for Travel was reviewed with commentary from EMM. EMM noted that January had seen a 47% reduction in complaints from last year. However EMM considered redress payments to be high and suggested these be reviewed in line with the review of the Complaints Handling process.

ACTION SH

(b) EMM reminded the meeting of the Add-on review recently conducted and that work had commenced on a vulnerable customer review.

ACTION KO (c) The Regulatory change log was reviewed. KO noted that a meeting was scheduled to review the impact of each area on the business and the log would be updated and circulated accordingly.

POL00423565

(d) The level of Financial Promotions was discussed. As this is currently still outsourced to Thistle, the resource requirements are unknown. A defined marketing plan would be useful to determine anticipated activity in this area.

RCC 16/27 **ISAG REPORT**

As EMG is absent for this meeting, ISAG content was deferred to the next meeting

RCC 16/28 **ANY OTHER BUSINESS**

There being no further business the meeting was closed

The next meeting of the RCC would be held on 14th April 2016 at 1pm.

…….. ……

Chairman **Date**

POL00423565

Post Office Ltd
Risk & Compliance Committee meeting
5 May 2016

Location:

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

ATTENDANCE LIST

ATTENDEES	SIGNATURE
MacLeod, Jane	
Alwen, Lyons	
Cameron, Alisdair	
George, Martin	
Hayward, Neil	
Hussey, David	
Kevin, Gilliland	
Nick, Kennett	
Paula, Vennells	

Also in attendance

CoSec	

Additional access

Wechsler, Tom	

POL00423565

Risk and Compliance Committee Agenda

Date
Thursday, 5 May 2016

Start Time	Finish Time
13.00hrs	16.00hrs

Room
1.19 Wakefield, Finsbury Dials

Present	In Attendance	Apologies
• Jane MacLeod (Chair) • Paula Vennells • Neil Hayward • Nick Kennett • Alwen Lyons • Alisdair Cameron • David Hussey • Kevin Gilliland • Martin George	• Mike Morley-Fletcher • Garry Hooton • Adnan Killedar • John Scott (item 9) • Tom Moran (item 10) • Steve Norris (item 10)	

Agenda Item	Action Needed	ARC?	Purpose	Lead	Timing
GOVERNANCE					
1. RCC minutes and actions	Agree minutes Review actions		Agree minutes of last meeting and review actions	Chair	13:00 – 13:05
2. Review of effectiveness of RCC against TOR	Review paper and agree actions		Review the effectiveness of RCC against its Terms of Reference in 2015/16 and the actions identified	Chair	13.05 – 13.10
INTERNAL AUDIT					
3. Internal audit report	Review report consider appropriateness to go to ARC	✓	Update on progress of audit plan and findings of completed audits	Garry Hooton	13.10 – 13.30
RISK					
4. Risk report **(a) General control framework** **(b) Policy framework** **(c) Business continuity** **(d) Self-assessment** **(e) Risk report in ARA**	Review reports and approve actions; consider appropriateness to go to ARC	✓	Update on progress in implementing the central control framework, policy framework, business continuity management and self-assessment and the draft wording for the risk disclosure in the Annual Report and Accounts.	Mike Morley-Fletcher	13.30 – 14.00

CONFIDENTIAL

POL00423565

Agenda Item		Action Needed	Going to ARC?	Purpose	Lead	Timing
POLICIES						
5.	**Policies for approval**	Approve policies	✓	Approve six policies submitted as part of the Partner Banking Agreement and the revised whistleblowing policy.	Chair	14.00 – 14.10
				BREAK		
COMPLIANCE						
6.	**Financial Services deep dive**	Review appropriateness to go to ARC	✓	Response to ARC request for an explanation of Post Office's oversight of regulatory activity in branch and how issues are escalated.	Kevin Gilliland	14:20 – 14:45
7.	**Gifts and hospitality update**	Review paper and approve actions		Annual review of compliance with gifts and hospitality procedure in 2015/16.	Mike Morley-Fletcher	14:45 - 14:55
8.	**Whistleblowing update**	Review paper and approve actions		Annual review of operation of whistleblowing arrangements in 2015/16	Chair	14:55 – 15.05
9.	**AML update**	Review appropriateness to go to ARC	✓	Response to ARC action requiring a report on AML at every ARC meeting including a stakeholder plan.	John Scott	15:05 – 15:15
10.	**Property compliance update**	Review appropriateness to go to ARC	✓	Response to ARC action requiring update on property compliance to be circulated before next meeting	Steve Norris	15:15 – 15:30
NOTING PAPERS						
11.	**Update on approach to modern slavery**	Note paper	✓	Update on POL's approach to complying with new legislation about modern slavery	Chair	15:30 – 15:35
12.	**Horizon spotting**	Note paper		Update on risks spotted on horizon and reported at last meeting, and any new risks identified.	Chair	15:35 – 15:40
13.	**POMS RCC minutes**	Note minutes		Minutes of most recent POMS RCC	Nick Kennett	15:40 - 15:45
14.	**AOB**			Discuss AOB	Chair	15:45 – 16:00
	CLOSE					16.00

POL00423565

RCC 5 May 2016 Paper 1A

Post Office Ltd – Confidential

Risk and Compliance Committee (R&CC)		**Reference: R&CC March 16**
Date: 02 March 2016	**Venue: Boardroom, Finsbury Dials**	**Time: 13:00 – 16:00**
Attending:		
Jane MacLeod (JM)	General Counsel	Chair
Alistair Cameron (AC)	Chief Finance Officer	Member
Paula Vennells (PV)	Chief Executive Officer	Member
Neil Hayward (NH)	Group People Director	Member
Alwen Lyons (AL)	Company Secretary	Member
Nick Kennett (NK)	Financial Services Director	Member (mid-Item 2 onwards)
David Hussey (DH)	Transformation Director	Member
Kevin Gilliland (KG)	Network and Sales Director	Member (Items 1, 2, 8, 9)
Paul Brown (PB)	Head of Commercial Development	Representing Commercial Director
Tom Wechsler (TW)	Chief of Staff	Supporting CEO
Mike Morley-Fletcher	Head of Risk and Assurance	Report
Garry Hooton (GH)	Head of Internal Audit	Report
Adnan Killedar	Risk Business Partner	Observer
Georgina Blair	Risk Business Partner	Minutes
John Scott (JS)	Head of Security	Report (Items 1, 2, 8, 9)
Jenny Ellwood (JE)	Head of Transformation Risk & Assurance	Report (Item 5)
Julie George (JG)	Head of Information Security	Report (Item 7)
Peter Markey (PM)	Chief Marketing Officer	Report (Item 9)
Apologies:		
Martin George	Commercial Director	

The meeting began at 13.00

The Chair declared the committee quorate and opened the meeting.

JM noted that as well as the papers already marked as going to the ARC in the agenda, the AML risk update (item 8) and the paper on contract management (item 10) were also going to ARC.

JM explained that work is under way to align the pension investment reporting with the schedule of governance meetings. There would be no pension update presented at this meeting, but a pension report would be provided to the next Audit and Risk Committee (ARC) meeting, with the investment advisers present. This report would be circulated to the Committee to discuss by correspondence before the ARC meeting.

Agenda Item 1, RCC minutes and actions

The Committee agreed the minutes of the previous meeting and the attached actions.

JM confirmed that going forward all Group Executive (GE) members would be invited to RCC meetings.

Agenda Item 2, Internal audit report

GH explained the status of the audits on Appendix 1 and 2. The Committee discussed whether the 2015/16 audit plan had been over-ambitious. It was noted that the 2015/16 plan had been signed off by the ARC in March 2015.

Nick Kennett joined the meeting.

The Committee noted that there appeared to be a high number of partially completed and delayed audits in the plan for the current year. MMF explained that the plan had been designed so that

POL00423565

audits conducted in quarter 4 would be presented to the May ARC. The Committee queried whether this would give ARC too many reports to review, and it was clarified that only red rated reports go to ARC in full. Only the high rated actions from other reports get reported to ARC.

The Committee discussed the list of action points in Appendix 3. It was noted that some of the actions had been superseded by recent events and were not up to date. Certain GE members stated that the actions had not been escalated to them. The Committee discussed whether some of the action deadlines were overly optimistic and it was agreed that members would challenge unrealistic deadlines against action plans in the draft audit report. The Committee requested that a process be designed and implemented which allows agreed audit actions to be tracked and escalated to the appropriate GE member as necessary (**Action 1706**).

The Committee discussed how the audit actions would be presented to ARC, and it was requested that only overdue actions should be reported, however the methodology to do this was still being considered. It was noted that there was an ARC action requiring the reporting of high rated actions.

22 January 2016 POLARC 16/04 (a)	Internal Audit Update To include post audit assurance in the ARC report in relation to high rated actions.

[ARC action provided for information]

MMF suggested that a regular schedule of quarterly meetings be set up with each GE member. AC confirmed that he had found his first quarterly meeting useful but that he had not been presented with any overdue actions to review at the meeting.

Referring to Appendix 1, NK commented that the POMS audit shouldn't be on the list of work being completed for POL, as the POMS audit is being completed for the POMS ARC and any relevant findings will be reported by the POMS ARC to the POL ARC.

NK also queried why the FRES audit was listed in Appendix 1, as POL pays for Bank of Ireland (BoI) resource to audit FRES and receives reports via the FRES ARC, and it was unclear why POL was spending scare audit resource on FRES when the BoI resource could be used to provide assurance. JM pointed out that unlike POMS, where an appropriate governance structure has been worked out, the POL Board has no oversight of FRES. It was agreed that JM and NK would consider how POL GE and Board should ensure they have oversight of both FRES and POMS performance. (**Action 1707**)

The Committee discussed the 2016/17 audit plan and queried whether it was overambitious and whether the audits were prioritised against the top risks of the business. MMF explained that the top risks and current priorities had been discussed with individual GE members and their representatives in the course of drawing up the plan. It was agreed that it would be helpful to show which risks the proposed audits related to. GH also undertook to provide details of how long it was proposed each audit should take, to address the concerns about ability to complete the plan with the existing resources. (**Action 1708**)

The Committee requested that the "Top 10" audits be prioritised with other potential audits being listed as optional.

Agenda Item 8, AML risk update

JS summarised the main points from the AML risk update (paper 8) for the Committee. The Committee discussed the forthcoming HMRC Anti Money Laundering/Counter Terrorist Financing (AML/CTF) compliance audit, and asked for further detail on the likely cost of remedying the failure to register newly opened PO branches with HMRC; JS confirmed that this is currently being scoped. The Committee noted that the data comes from Network, the registration is paid for by Financial Services and the registration process is done by the AML team in Security, and it was unclear who would be responsible for any fines levied by HMRC.

POL00423565

The Committee discussed the AML/CFT compliance requirements required when providing cash delivery, collection and processing services for customers who are themselves Money Service Businesses (MSBs).

The Committee requested that the Promontory Report (an external review of POL's AML/CFT framework, concluded in Dec 2015) be circulated to Committee members to help them understand the work required to prepare for the HMRC audit. (**Action 1709**)

JM explained that steering group with representatives from affected parts of the business had been put together to scope the resources needed and that we would need specialist expertise. DH offered to provide project management resource.

Agenda Item 9, Customer vulnerability review

PM joined the meeting to present an update on recent work relating to customer vulnerability (paper 9). The Committee noted the difficulty in defining vulnerable customers, due to the transitory nature of some types of vulnerability, and the associated difficulty in defining appropriate processes and procedures.

The Committee agreed that customer vulnerability should be included as an aspect of a wider Customer Policy to be written by Commercial (**Action 1710a**, but that there should not be a separate policy specifically relating to vulnerable customers. The Committee requested that NK discuss the advantages and disadvantages of joining the British Bankers Association (BBA) Vulnerability Taskforce with PM before a further decision on this was made. (**Action 1710b**)

PM left the meeting.

Break

A ten minute break took place. KG and JS both left the meeting.

Agenda Item 3, Corporate Governance capability and ARA disclosure

MMF presented the paper on Corporate Governance capability and disclosure (paper 3). The Committee discussed the proposed wording for the corporate governance statement in our next Annual Report and Accounts (Conclusion 3 on p.2) and were supportive of the fact that the wording was now focused on the drivers for PO and was as straight forward and succinct as possible. As POL's accounts are closely scrutinised by some observers, this would make clear what we expected to be held to account for.

It was agreed that the option for reference to future changes was self-evident and so was not needed.

Agenda Item 4, Risk update

MMF presented the risk summary paper (paper 4).

MMF presented the Group Risk Profile update which now included suggestions from risk owners of their Key Further Actions (paper 4a). JM noted that the dates given for completion of key further actions (paper 4a, Appendix 2) were nearly all in the next few months, and asked the Committee to consider whether these were accurate or optimistic, or whether other medium or longer term actions were needed. The Committee agreed that currently the actions were in the main short term steps on the way to achieving the longer term desired risk outcome. The Committee noted that at this stage of the business's transformation there were many significant actions that were short term and that once these were completed longer term actions should become more apparent. The Committee agreed that only the key further actions for the red risks should be presented to the ARC, and requested that the red risks be recirculated to GE members for a further review of actions (to add any relevant medium or longer term actions) before the ARC paper is finalised. (**Action 1711**)

POL00423565

MMF presented the risk incident reporting paper (paper 4b). He explained that the purpose of reviewing reported risk incidents was to learn from their occurrence with regard to the appropriateness of our Top Risk, either their descriptions or their evaluation; it was not to discuss the management of specific incidents, which should be handled by respective risk owners. MMF drew the Committee's attention to Tables 2 and 3 in Appendix 1, which showed those incidents reported by business unit Risk Champions since the last RCC meeting mapped against the top risks. NH noted that instances of industrial action could be recorded against Top Risk 1 Industrial Relations as incidents. The Committee requested that the Central Risk Team work with business unit Risk Champions to help them identify other incidents that should be reported and match them to the Top Risks for lessons learnt. (**Action 1712**)

The Committee discussed the Health and Safety risk, noting that while this was currently well controlled it was of such importance that it should appear on the register of top risks. The Committee requested that MMF work with NH to add the Health and Safety risk to the Top Risks and complete a Risk Mitigation Plan. (**Action 1713**)

MMF presented the updates on the General Control Framework (paper 4c) and the Policy Framework (paper 4d). The Committee queried whether a whistleblowing report would be presented to the RCC and ARC and it was confirmed that this was on the agenda for May. The Committee also noted that the identification of policies and policy owners for non-Corporate Services policies (Phase 2 of the Key Policy Framework in Appendix 1) was purely for information and no action had been agreed. Once tools had been developed and lessons learnt from reviewing and remediating the Corporate Services policies, the extension to non-Corporate Services policies would be considered, assisted by benchmarking information on standard policy frameworks to be provided by Ernst & Young, and a proposal would be brought back to the RCC for discussion in May.

MMF presented the update on Business Continuity management (paper 4e). The Committee noted that dealing with business as usual (BAU) activity had taken up some project resource and that buffer in the project plan had been used up, but MMF confirmed that resource had been diverted within the Risk team to address this. Consideration will be given to rebasing the project plan.

MMF presented the paper on the Self-Assurance Regime (paper 4f), explaining the difference between the high-level Executives' Declaration and the more process specific Control Self-Assessment (currently planned solely for Finance Reporting controls). The Committee supported the proposal for both:

- The Committee agreed that an initial Executives' Declaration self-assessment exercise should take place at the end of March 2016 which should be used to identify gaps for a more evidential based dry run at the half year, in preparation for a full roll out at year end, with supporting evidence. (**Action 1714**)

- The further application of CSA at branch level was raised as a possibility for improving conformance with mails segregation requirements. The Committee requested that Mark Siviter, Head of Mails, and KG clarify what would be needed to prove conformance with the mails segregation requirements. (**Action 1715**)

Agenda Item 5, Business Transformation risk report

JE joined the meeting to present the Business Transformation risk report (paper 5). The Committee discussed cost estimation for longer projects. The Committee noted that Project Trinity had changed the risk profile of the business, and reference to this should be made in the ARC papers in the Group Risk Profile presented to the ARC. (**Action 1716)**

POL00423565

RCC 5 May 2016 Paper 1A

Post Office Ltd – Confidential

Agenda Item 7, Cyber Security paper
JG joined the meeting to take any questions on the paper on Cyber Security (paper 7). The Committee queried whether there had been a Distributed Denial of Service (DDOS) attack on the Post Office website in August 2015. JG confirmed that forensic investigation had found no evidence of a DDOS attack.
Agenda Item 10, Contract management
JM presented the paper on contract management (paper 10). The Committee agreed that the detail of the top 30 contracts (Appendix) would not be given to ARC.
Agenda Item 11, Horizon spotting report
JM presented the paper on horizon spotting (paper 11). The Committee agreed that this was very interesting and should be presented to ARC.
Agenda Item 12, Noting papers
JM referred the Committee to the two noting papers. The Committee had no comments.
Agenda Item 13, Any Other Business
No AOB was raised.
The meeting closed at 16.00

Next Meetings – 5 May 2016 Room 1.19 Wakefield 13.00 – 16.00
7 July 2016 Room 1.19 Wakefield 13.00 – 16.00

POL00423565

POL Risk and Compliance Committee
Action List
Status Report as at: 29/04/2016

MEETING DATE	AP REF	ACTION	Action Owner	Due Date	STATUS	Open/Closed
08/15/2015	1674	Provide a regular short update on Vulnerable Customer approach until this work is completed	Martin George	05/05/2016	Last update given at March RCC	Open
02/03/2016	1710a	Create Customer Policy which includes treatment of vulnerable customers	Martin George	tbc	Discussions in progress	Open
02/03/2016	1715	Ask Mark Siviter, Head of Mails, and Kevin Gilliland to clarify what would be needed in terms of controls self assessment to prove conformance with the mails segregation requirements.	Mike Morley-Fletcher	07/07/2016	Discussions in progress	Open
02/03/2016	1712	Central Risk Team to work with business unit Risk Champions to help them identify other incidents that should be reported and match them to the Top Risks for lessons learnt.	Mike Morley-Fletcher	07/07/2016	In progress - discussed in Risk Champions' Forum on 28/04/16	Open
02/03/2016	1707	Consider how POL GE and Board should ensure they have oversight of both FRES and POMS performance.	Jane MacLeod/ Nick Kennett	07/07/2016		Open
02/03/2016	1710b	Discuss the advantages and disadvantages of joining the British Bankers Association (BBA) Vulnerability Taskforce with Pete Markey before deciding whether to join.	Nick Kennett	05/05/2016	FS is currently co-ordinating with both POMS and BoI on addressing customer vulnerability issues. FS has existing working group arrangements in place with BoI to review vulnerability in respect of FCA's recent guidance on this issue. We currently don't anticipate joining the BBA taskforce as the benefits are unclear to PO but we will maintain a watching brief	Closed
02/03/2016	1716	Make reference to the effect of Project Trinity on the risk profile of the business in the Group Risk Profile presented to ARC.	Mike Morley-Fletcher	17/03/2016	Group risk profile updated for effect of Project Trinity before presentation to March ARC.	Closed
02/03/2016	1714	Initial Executives' Declaration self-assessment exercise to take place at the end of March 2016; outputs to be used to identify gaps for a more evidential based dry run at the half year.	Al Cameron/ Mike Morley-Fletcher	31/03/2016	Completed - see May RCC Paper 4d for details.	Closed

POL00423565

MEETING DATE	AP REF	ACTION	Action Owner	Due Date	STATUS	Open/Closed
02/03/2016	1713	Add the Health and Safety risk to the Top Risks and complete a Risk Mitigation Plan	Mike Morley-Fletcher/ Neil Hayward	17/03/2016	Heath and Safety risk was added to the Group Risk Profile presented to the March ARC and a Risk Mitigation Plan drawn up.	Closed
02/03/2016	1711	Recirculate red risks to GE members for a further review of actions (to add any relevant medium or longer term actions) before the ARC paper is finalised	Mike Morley-Fletcher	17/03/2016	Input from GE members gathered and included in group risk profile presented to March ARC.	Closed
02/03/2016	1709	Circulate Promontory Report (an external review of POL's AML/CFT framework, concluded in Dec 2015) to Committee members to help them understand the work required to prepare for the HMRC audit.	Jane MacLeod	05/05/2016	Executive Summary circulated to GE members on 26/04/16.	Closed
02/03/2016	1708	Provide details of how long each audit in the 2016/17 plan is expected to take to address the concerns about ability to complete the plan with the existing resources	Garry Hooton	17/03/2016	Incorporated in update on progress to plan - see May RCC agenda item 3 - Internal audit report.	Closed
02/03/2016	1706	Design and implement a process which allows agreed audit actions to be tracked and escalated to the appropriate GE member as necessary.	Garry Hooton	05/05/2016	Completed.	Closed
12/01/2016	1700b	MMF to investigate an appropriate rewording of GCF 3	Mike Morley-Fletcher	02/03/2016	Included in Paper 4c for March RCC.	Closed
12/01/2016	1700a	Update General Controls Framework based on RCC comments	Mike Morley-Fletcher	02/03/2016	Included in Paper 4c for March RCC and will be included as part of risk report in future meetings.	Closed
12/01/2016	1705	Review coverage of RCC against its Terms of Reference	Georgina Blair	05/05/2016	Completed - see May RCC agenda item 2 - Review of effectiveness of RCC.	Closed
12/01/2016	1704	RCC to review options regarding compliance with UK Corporate Governance Code and present them to the ARC.	Mike Morley-Fletcher	17/03/2016	Presented to March ARC.	Closed
12/01/2016	1703	Pensions update to be presented to the March RCC and ARC meetings and then quarterly going forward.	Harpreet Singh	17/03/2016	Update presented to March ARC & item added to standing agenda for future meetings.	Closed
12/01/2016	1702	Business continuity framework to be presented to the RCC	Mike Morley-Fletcher	02/03/2016	Included in Paper 4e for March RCC, and included as standing item in future meetings until project completed.	Closed
12/01/2016	1701	Update Policy framework based on RCC comments and present updated version to the RCC.	Mike Morley-Fletcher	02/03/2016	Included in Paper 4d for March RCC, and to be included as part of risk report in future meetings.	Closed
12/01/2016	1699	Review group risk profile and present updated profile to RCC	Mike Morley-Fletcher	02/03/2016	Included in Paper 4a for March RCC.	Closed

POL00423565

MEETING DATE	AP REF	ACTION	Action Owner	Due Date	STATUS	Open/Closed
12/01/2016	1698	Inform RCC on the sponsor/requestor of FRES audit. GH will discuss scope of the FRES review with NK directly.	Garry Hooton	02/03/2016	Done - see audit plan.	Closed
12/01/2016	1697	Implement improved audit report sign-off process with greater involvement of GE members	Garry Hooton	05/05/2016	Completed.	Closed
12/01/2016	1696	RCC to be provided with follow-up on implementation of audit recommendations	Garry Hooton	02/03/2016	Included in Paper 4a for March RCC and included as standing item in future meetings.	Closed
26/10/2015	1695	Work with risk report authors to improve risk report format	Mike Morley-Fletcher	02/03/2016	Done in preparation of papers for March RCC.	Closed
26/10/2015	1692	Include update from incident owner on current status in incident reporting table	Mike Morley-Fletcher	02/03/2016	Included in Paper 4b for March RCC/.	Closed
07/09/2015	1687	Clarify how POMS will assure itself that POL is complying with POM's compliance requirements	Susie Hayward	05/05/2016	Completed - see May RCC agenda item 6 - Financial Services Deep Dive.	Closed

POL00423565

2) Review of RCC Terms of Reference

Author: Georgina Blair Sponsor: Jane MacLeod Meeting date: 05 May 2016

Executive Summary

Context

In line with best practice and as recommended by the UK Code of Corporate Governance a clear Terms of Reference ('TOR') for the Risk and Compliance Committee ('RCC') should be in place and reviewed on an annual basis. This year's review was completed in April 2016.

Questions this paper addresses

1. Does the RCC have a clear and agreed TOR?
2. Has the Committee fulfilled the requirements of the TOR over the last year?
3. How will the Committee ensure it uses its time effectively in future and fulfils the requirements set out in its TOR?

Conclusion

1. The requirements specified by the current TOR (see Appendix 1) are clear and approved by the Group Executive (GE). The TOR will be updated before the next RCC (July).
2. The analysis carried out (see Appendix 2) confirms that the RCC has fulfilled the requirements of its TOR with the exception of receiving reports from three sub-committees.
3. The draft RCC timetable set out in Appendix 3 is a proposed forward agenda for RCC meetings which will ensure the RCC fulfils the requirements of its TOR in 2016/17.

Input Sought

The members of the RRC are asked to:

1. Confirm they believe they have fulfilled the requirements of the RCC TOR in 2015/16 as specified by the Group Executive.
2. Feedback to the Chair any comments on the proposed forward agenda for 2016/17.

POL00423565

The Report

1. The RCC is responsible for supporting the Group Executive (GE) in fulfilling their responsibilities in the effective oversight of risk management, internal control and compliance. It was decided in March 2016 that RCC membership should be extended to include all members of the Group Executive (GE). The TOR has not yet been updated to reflect this (see Appendix 1). The TOR will be updated for the changes made during 2015/16. This will be completed for the next RCC (July).

2. The areas of the TOR have be assessed against the Committee agendas, papers and decisions to ensure that the Committee has fulfilled its requirements to the Group Executive (see Appendix 2):
   a) The 'Purpose' of the Committee is clear and agreed by the Group Executive.
   b) The 'Meetings' have been convened in accordance with the TOR, although this review of the effectiveness of the Committee did not take place until after the year end (in April 2016).
   c) The 'Responsibilities' have been discharged, with the exception of:
      i) Review of risk reports from the Health and Safety Committee; instead this committee reports directly to the Board.
      ii) Review of risk reports from Commercial Committee and the Business Continuity Committee. The Commercial Committee doesn't report to RCC and the Business Continuity Committee doesn't currently exist.
      iii) No whistleblowing report was provided in 2015/16. One is being provided in May 2016.

3. Areas of specific risk have been reported throughout the year and key further actions agreed, for example cyber security and anti-money laundering in March.

4. The draft RCC timetable set out in Appendix 3 is a proposed forward agenda for RCC meetings which will ensure the RCC fulfils the requirements of its TOR in 2016/17. The scheduling of the various agenda items is yet to be finalised and will be aligned with the ARC timetable.

POL00423565

Appendix 1

RISK AND COMPLIANCE COMMITTEE
TERMS OF REFERENCE
(March 2015)

1. Overview

The purpose of the Risk & Compliance Committee (R&CC) is to support the Executive Team (ET) in fulfilling their responsibilities in the effective oversight of risk management, internal control and compliance.

2. Responsibilities

The responsibilities of the Risk & Compliance Committee include, but are not limited to:

- Reviewing the effectiveness of the risk management framework and risk policy and the oversight of the development and implementation of the risk management framework;
- Oversight of the current risk exposures of the business and advising on the future risk strategy;
- Oversight of the identification and effective management of current key risks and regular reviews of emerging risks;
- Oversight of the key operational risks facing the business including the effectiveness of internal controls;
- Monitoring the implementation of key recommendations and management action plans;
- Monitoring compliance with legal and regulatory obligations, including any significant breaches;
- Receiving and reviewing risk reports from the R&CC Sub-Committees:
  - Health & Safety
  - Commercial
  - Transformation

POL00423565

- Information Security
- Security
- Business Continuity

- Receiving and reviewing reports related to
  - Anti-Money Laundering
  - Bribery / Gifts & Hospitality
  - Whistleblowing
  - Internal Audit activity;

- Receiving and reviewing the draft annual internal audit plan for onward reporting to the Audit and Risk Committee (ARC);

- Receiving and reviewing of the draft annual risk management plan for onward reporting to the Audit and Risk Committee (ARC), and;

- Reviewing the adequacy of policy governance and recommending changes.

3. Authority

The Risk & Compliance Committee is authorised to:

- Seek any information it requires from anyone in the organisation in order to perform its duties including calling anyone to the meeting to be questioned as required; and

- Obtain outside legal or other professional advice on any matter within its terms of reference.

4. Meetings

- The R&CC shall meet at least six times a year and otherwise as required;

- The quorum shall be two members which will be deemed competent to exercise all or any of the authorities and powers vested in or exercisable by the committee;

- The committee will arrange for an annual review of its own performance to ensure it is operating effectively and recommend any changes it considers necessary to ET for approval; and

POL00423565

- The committee will ensure its terms of reference and membership are reviewed on an annual basis and updated as required

5. Reporting

- The committee shall report to Executive Team on its proceedings on all matters within its purpose and responsibilities highlighting significant risk and compliance matters for their attention;

- The committee shall report to the Board and Audit, Risk and Compliance Committee as requested; and

- The committee shall input to the Post Office annual reporting as appropriate.

6. Membership

Members	
General Counsel (Chair)	Jane MacLeod
Chief Executive Officer	Paula Vennells
Chief Finance Officer	Alisdair Cameron
Group People Director	Neil Hayward
Financial Services Director	Nick Kennett
Company Secretary	Alwen Lyons

Other attendees	
Head of Risk & Assurance	Arnout van der Veer
Head of Internal Audit	Garry Hooton
Chief of Staff	Gavin Lambert
Secretariat	Georgina Blair

POL00423565

Appendix 2

Analysis of performance of RCC against requirements

Verbatim Extracts from TOR		Meeting Dates					
Responsibilities -		**May-15**	**Aug-15**	**Sep-15**	**Oct-15**	**Jan-15**	**Mar-16**
Reviewing the effectiveness of the risk management framework and risk policy and the oversight of the development and implementation of the risk management framework	✓	Approved principles of RM and implementation plan and reviewed effectiveness of risk and internal controls framework	Received update on BCP & incident management process	Reviewed interim incident management process	Received update on risk framework implementation timetable	Received update on general control framework	Received update on general control framework and self-assurance regime
Oversight of the current risk exposures of the business and advising on the future risk strategy	✓	Reviewed principal risks	Reviewed group risk profile	Reviewed group risk profile		Reviewed group risk profile	Reviewed group risk profile
Oversight of the identification and effective management of current key risks and regular reviews of emerging risks	✓		As part of review of updated group risk profile	As part of review of updated group risk profile		As part of review of updated group risk profile	
Oversight of the key operational risks facing the business including the effectiveness of internal controls	✓		As part of review of group risk profile	As part of review of group risk profile		As part of review of group risk profile	As part of review of group risk profile
Monitoring the implementation of key recommendations and management action plans	✓						Reviewed key further actions for red risks in group risk profile

POL00423565

		May-15	Aug-15	Sep-15	Oct-15	Jan-15	Mar-16
Receiving and reviewing risk reports from the R&CC Sub-Committees:							
Health & Safety	X						
Commercial	X						
Transformation	✓				✓	✓	✓
Information Security	✓				Annual deep dive on risk profile		Cyber security update
Security	✓				Annual deep dive on risk profile		AML update
Business Continuity	X						
Receiving and reviewing reports related to							
Anti-Money Laundering	✓		AML annual report				AML risk update
Bribery/ Gifts & Hospitality	✓	G&H annual report					
Whistleblowing	X						
Internal Audit activity							
Receiving and reviewing the draft annual internal audit plan for onward reporting to the Audit and Risk Committee (ARC)	✓						Reviewed 2016/17 Internal Audit plan
Receiving and reviewing of the draft annual risk management plan for onward reporting to the Audit and Risk Committee (ARC)	✓				Reviewed plan to March 2017 (presented to ARC in September)		
Reviewing the adequacy of policy governance and recommending changes	✓	Reviewed policy approvals process			Reviewed approach to POL-wide policy framework	Received update on implementation of policy framework	Received update on implementation of policy framework

POL00423565

Appendix 3

RCC Forward planner – proposed topics (assuming 6 meetings per year) – scheduling to be confirmed

Items		Proposed				
	1) Jan	2) Mar	3) May	4) July	5) Sep	6) Nov
1. Standing Agenda Items						
• Minutes and actions from previous RRC meetings	√	√	√	√	√	√
• Minutes from POMS RCC meetings	√	√	√	√	√	√
2. Governance Items						
• Review of RCC Terms of Reference		√				
• RCC effectiveness against ToR self-assessment		√				
3. Risk Management, Internal Control and Assurance						
• Group Risk Profile		√			√	
• Key Further Actions & Risk Incidents	√	√		√	√	
• Internal Audit update	√	√	√	√	√	√
• Internal Audit – approval of the upcoming plan		√				
• Business Continuity – approval of annual plan		√				
4. Financial Reporting and Disclosure						
• Risk disclosures for annual report and accounts			√		√	
• Board Annual Assessment (including Executives Declaration, Key Policies and Control Self Assessment)			√			
• Corporate Governance Statements			√			
5. Compliance						
• Regulation						
▪ Anti Money Laundering	√	√	√		√	√
▪ Anti Bribery & Corruption	√					
▪ Competition Law	√					
▪ Data Protection	√					
• Conduct/ People						
▪ Customers (e.g. Vulnerable, Conduct issues)		√				

POL00423565

Items		Proposed				
	1) Jan	2) Mar	3) May	4) July	5) Sep	6) Nov
▪ Ethics and Code of Conduct		√				
▪ Fraud and Theft		√				
▪ Whistleblowing		√				
6. **Deep Dives**						
▪ FS Deep Dives on specific issues	√		√			
▪ Pensions		√			√	
▪ Health and Safety					√	
▪ Incident Management, Disaster Recovery & Crisis Management					√	
▪ Transformation Risk	√				√	
▪ Cyber / IT Security					√	

POL00423565

Internal Audit Report

Author: Garry Hooton Meeting date: 05 May 16

Executive Summary

Context

The purpose of this paper is to update the Committee on the PO Internal Audit and Business Transformation Assurance activity and key outcomes. This includes details of the work completed since the last Risk and Compliance Committee (RCC) in March and the closing out of the 2015/16 Internal Audit Plan. We have agreed the plan for 2016/17 with ARC and have commenced work on Q1 reviews.

Questions this paper addresses

1. What progress has been made since the March meeting?
2. Is the Internal Audit Plan on track for completion of 2015/16 audit plan?
3. Do we have the resources we need to deliver the plan and actions arising going forwards?
4. Have any significant issues arisen that the committee should be aware of?

Conclusion

1. During the period seven audits, four Internal Audit and three Business Transformation Assurance (BTA) have been completed, with actions agreed with management. These have been finalised with GE Sponsors and five (three IA and two BTA), are nearing completion. The team have also continued to contribute in a business assistance capacity to the Property Compliance Forum, we are intending to cease this in 2016/17 once the Property team have assumed full responsibility for their compliance activity. Work on the 2016/17 plan has commenced. Work has continued on the General Controls Framework, Executives' Declaration processes and developing our Controls Self-Assessment capability (subject of separate papers). We have been working closely with GE sponsors to remediate the overdue audit actions and have made very good progress. BTA replanning will take place following the upcoming second phase of boot camps.
2. The audits remaining for 2015/16 are now either completed or going through final clearance with senior management. The completion of the Agents Remuneration audit has been significantly delayed by the "Agents payments issue", work will resume once the business has completed recovery work. (see **Appendix 1**).

POL00423565

3. We remain one team member short as we continue to try to obtain appropriate temporary maternity cover for the IT audit manager role. Another team member who has been on long term sick leave has returned to the business, initially on a phased basis.
4. There are no significant issues that we believe the committee should be made aware of.

Input Sought

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

POL00423565

4) Risk & Control Report

Author: Mike Morley-Fletcher

Meeting date: 5 May 2016

Executive Summary

Context

This paper updates the RCC on progress against the project plan for developing POL's Risk Framework, in particular how we have been developing POL's Group Risk Profile, Internal Control Environment, Assurance mechanisms and Corporate Governance capability. Please note, our Risk Profile is NOT reviewed at this RCC as it is covered at the other four meetings.

Questions

1. Is implementation of the Risk Framework on target?
2. What has been the primary focus?
3. What else has been progressed?

Conclusion

1. The plan is mostly on schedule (see appendix 1), despite some resource shortages (through illnesses and recruitment holds). However, we have had to reschedule developing the Route Map to Corporate Governance Compliance until September. This will map out our plan over the next 2 to 3 years. Many of our initiatives will contribute to greater compliance and so it was felt that formalisation of the plan could wait until the next RCC/ ARC. A summary of Work Done since the March ARC and Next Steps is included in appendix 2.

2. This period has been primarily focused on developing our risk, control and assurance disclosure statements for our stakeholders in the Annual Report. We have used our revised position on corporate governance compliance to guide the content and extent of our disclosures, but also compared these with other relevant organisation's reports and discussed them with our external auditors.

3. We have also progressed our work on improving our Internal Control Environment (e.g. dry running/ testing our Internal Control Framework, competing the review and remediation of our Corporate Services key policies, continuing to enhance our Business Continuity capability) and our Assurance Mechanisms (e.g. completing our first Executives' Declaration and starting the control self-assessment of our Financial Reporting controls) – see attached papers.

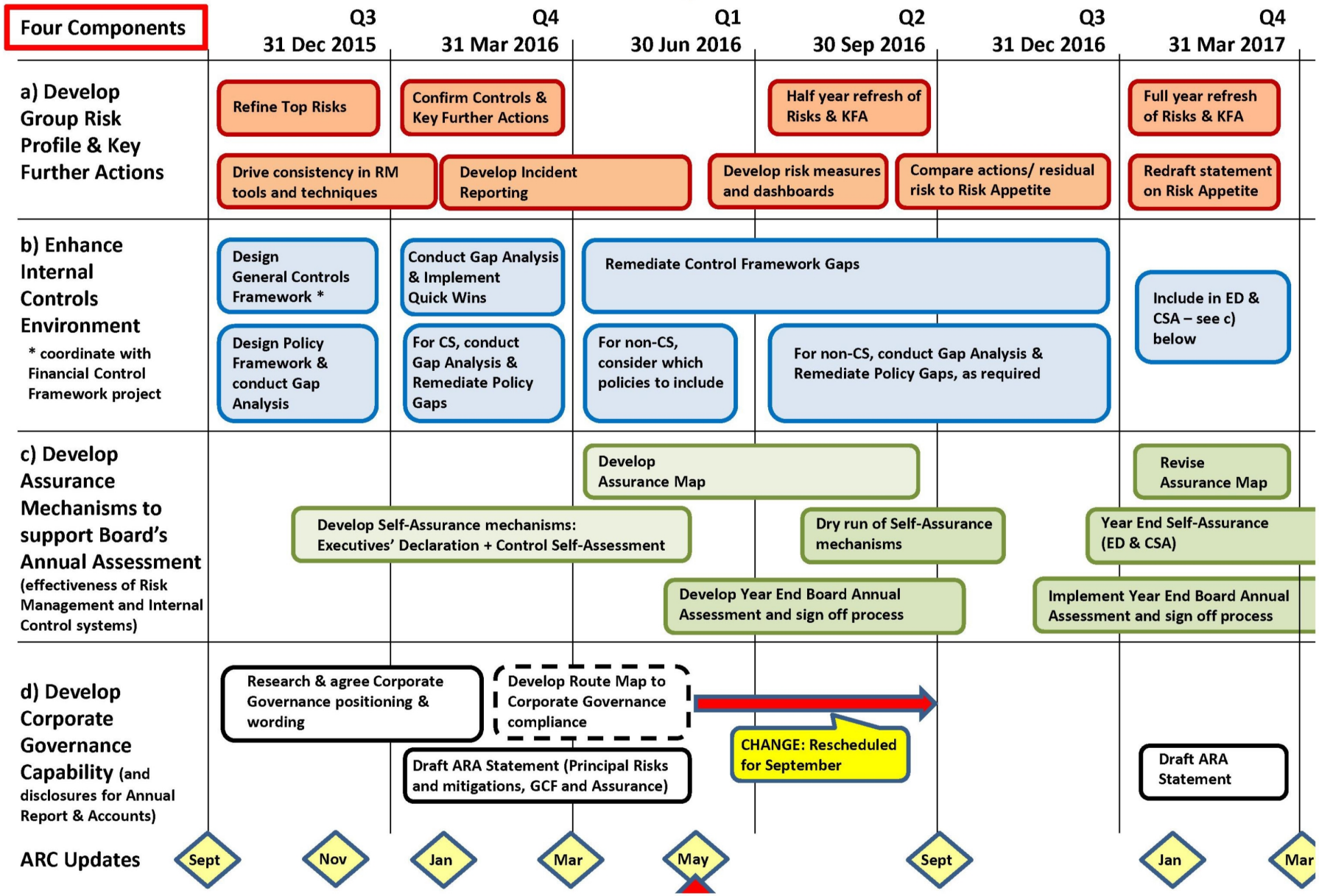
Input Sought

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

POL00423565

Appendix 1: Risk Framework - Project Plan

Version: 25th April 2016



POL00423565

Appendix 2 –Risk and Control Framework: Summary of Work Done and Next Steps

We have completed all key and time-critical components against the four main components of the plan (see Appendix B for a copy of the updated plan). Some of the main achievements have been, and next steps:

Work Done	Next Steps
a) Risk Profile and Actions – no paper provided	
Group Risk Profile: • Details are **NOT** reviewed at this RCC/ ARC. • Drafted Principal Risk and Mitigations for disclosure in Annual Report, per d) below. • Provided information on the Top Risks and Key Further Actions to the Strategy Team for consideration in the Business and Strategy planning process for 2016/ 17.	• Risk owners will review Principal Risks and Key Further Actions for reporting to September RCC/ ARC.
b) Internal Controls Environment	
bi) General Controls Framework (GCF) – see paper 4a): • Reviewed the General Control elements of the Financial Controls Framework project to confirm the design of our GCF, assess its current state, ensure any appropriate remediations have been identified and prepare templates for our subsequent Self-Assessment exercise. • Details of our General Controls have been included in this year's Annual Report in the risk note. • Started to embed risk and control accountabilities into GE objectives (or job profiles)	• Conduct dry run at half year 2016/ 17 and full roll out at year end (to help the Board complete its year-end Annual Assessment of Internal Controls for 2016/ 17). • Ensure risk and control accountabilities are reflected in GE objectives/ or job profiles (June)

POL00423565

Work Done	Next Steps
bii) Policy Framework (key policies) – see paper 4b): • Completed remediation of all Corporate Services policies. • Used EY's benchmarking to develop a list of non-Corporate Services key policies.	• Consider implementation needs of CS policies, ensuring pragmatic and co-ordinated. • Formalise monitoring mechanism to ensure we can evidence compliance with policies. • Complete a current state assessment of non-Corporate Services key policies to steer which polices need remediating and identify any implementation and monitoring needs.
biii) Business Continuity – see paper 4c): • Major Incident Management processes introduced, in conjunction with Crisis Management Team Construct • Initiation of Business Impact Assessments across business units, with aim to develop and test continuity planning.	• Complete phase 1: - Business Protection Team Training & Invocation Test - CMT Exercise • Continue phase 2: - BC Programme Management Structure Development.
c) Assurance Mechanisms (& assessment of effectiveness of Risk Management and Internal Control systems) – see paper 4d)	
• To provide assurance to Management and the Board (via the ARC): 1. Completed a dry run/ test of the Executives' Declaration return, completed by the General Executive (GE), and 2. Implemented Control Self-Assessment (CSA) techniques for the General Control Framework and Financial Reporting processes.	• Use any lessons learnt to improve self-assessment at half year 2016/ 17 • Conduct full roll out at year end 2016/ 17 (to help the Board complete its year-end Annual Assessment of Internal Controls for 2016/ 17).
d) Corporate Governance Capability (& disclosure in the Annual Report & Accounts) – see paper 4e)	
• For this year's disclosures, we reviewed previous declarations and enhanced the risk information in the Strategic Report (our approach to risk, our Internal Control Framework and more details on our principal risks) as well	• Ernst & Young have provided a review of our compliance gaps, which the Central Risk team will analyse to develop a route map to compliance (over the next 2 or 3 years). This will enable RCC and ARC to determine if this is appropriate for our needs and practical.

POL00423565

as in the Governance section (description of internal audit's approach and audits, plus how the Board conducts their assessment of the risk management framework and systems of internal control), in discussion with our external auditors. • In particular, following RCC and ARC suggestion, compliance with the UK Corporate Governance Code is not sought at present and our compliance statement is now, *"PO maintains standards of corporate governance appropriate for our ownership structure, our commitment to our social purpose and our strategy for commercial sustainability"*.	• This was originally estimated for presentation in May, but has been rescheduled to September.

POL00423565

4a) General Control Framework

Author: Deana Herley Sponsor: Mike Morley-Fletcher Meeting date: 5 May 2016

Executive Summary

Context

This paper provides an update on progress made on the General Controls Framework (GCF) project. Successful completion of this activity will give the business confidence over the effectiveness of its General Controls for business as usual operations and when pushing forward with transformation.

The initial focus is in support of the Financial Controls Framework project, but other areas will be considered subsequently.

The General Controls Framework has been included in this year's Annual Report in the risk note. Ultimately, our review of the GCF and the subsequent self-assessment by control owners will help the Board complete its year-end Annual Assessment of Internal Controls for 2016/ 17.

Details of the General Controls Framework:

<table>
<tr><td colspan="5">A) PURPOSE & DIRECTION</td></tr>
<tr><td colspan="2">1) Strategy, objectives and targets</td><td colspan="2">2) Code of Business Standards and Tone from the Top</td><td>3) Social Purpose</td></tr>
<tr><td colspan="5">B) PLANNING & REVIEW</td></tr>
<tr><td>4) 3 Year and Annual Plans</td><td>5) Change is planned and monitored</td><td colspan="2">6) Risk assessments</td><td>7) Performance monitoring</td></tr>
<tr><td colspan="5">C) ORGANISATIONAL DESIGN & DELEGATION</td></tr>
<tr><td rowspan="2">8) Organisational Structure, with Responsibilities and Segregation of Duties</td><td rowspan="2">9) Delegation of Authority, including Capital Investment limits</td><td rowspan="2">10) Staff calibre, experience and qualifications, including personal development and appraisal</td><td rowspan="2">11) Senior Management remuneration</td><td>12) Operational, financial and regulatory policies (and control activities) framework</td></tr>
<tr><td>13) IT policies (and control activities) framework</td></tr>
<tr><td colspan="5">D) GOVERNANCE & FEEDBACK</td></tr>
<tr><td>14) Board and Audit Committee</td><td>15) Assurance capability</td><td colspan="2">16) Whistleblowing and Complaints</td><td>17) External Reporting</td></tr>
</table>

Questions this paper addresses

1. What progress has been made since March? Are we progressing to plan?
2. What is happening to any significant gaps identified?
3. How do we ensure the GCF remains focused on the right areas?

POL00423565

Conclusion

1. During the period, Internal Audit reviewed the General Control elements of the Financial Controls Framework project and used this to confirm the design of our GCF, assess its current state, ensure any appropriate remediations have been identified and prepare templates for our subsequent Self-Assessment exercise.

   The project is progressing per our original project plan (see appendix 1 for details and timing). We aim to complete the full Current State Assessment of the GCF by mid June (ahead of plan). Self-assessment templates will be completed, in preparation for a dry run/ test attestation by GE Owner at next half year and full roll out at the year-end.

2. Where the Finance project team and KPMG have identified gaps or controls that need strengthening, these have been reviewed by Internal Audit. A pragmatic view has been taken on gaps and remediation activities, recognising not everything can be fixed straightway, and effort will be focused on fixing only what is needed.

3. As we progress we continue to review and challenge the GCF to ensure it is focused on the right areas. We believe that an additional element is required to reflect the importance of controlling change (e.g. "**change is planned and monitored"**). This has been added as a separate element under Planning and Review (see appendix 2).

Input Sought

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

POL00423565

Appendix 1 – General Control Framework – Project Plan

Set out below is an overview of our approach and timings to prepare the business for attestation of GCF effectiveness reporting in March 2017, including key activities and reporting milestones.

Overview

Month	Activity	Update to ARC
2016		
January	Design GCF	✓
February	Scope testing and developing tools	✓
March	Current State Assessment preparation	✓
April	Current State Assessment of GCF components	*50% complete*
May		
June		
July	Dry Run Preparation & Engagement	
August	Dry Run Assessment	
September	Dry Run Reporting	ARC
October	Remediations	
November		ARC
December		
2017		
January	Year End Preparation & Engagement	ARC
February	Year End Assessment	
March	Year End Reporting	ARC
April	Lessons Learnt	

POL00423565

Appendix 2 – General Controls Framework – Detail - Revised

Includes additional element "Change" as 5)

A) PURPOSE & DIRECTION
1) The **strategy**, objectives and targets are agreed and communicated, both internally and externally.
2) A **Code of Business Standards** is communicated and understood, and reinforced by the **Tone from the Top**.
3) Our **Social Purpose** is agreed and communicated, both internally and externally.

B) PLANNING & REVIEW
4) **3 Year and Annual Plans** (operating and capital) are prepared and reviewed by Management, before approval by the Board.
5) **Change is planned and monitored** to ensure its meets the business objectives, that risks are managed and appropriately mitigated and that approved benefits are realised.
6) Pre-emptive **risk assessments** of Business Plans, projects and business as usual operations are conducted, with current controls reviewed and additional actions identified where necessary to bring the desired level of control back within an acceptable level of risk taking (our risk appetite).
7) **Performance** is monitored and variances between forecast/ budget and actual are analysed and investigated. Change is planned and monitored to ensure benefits realised and user acceptability.

C) ORGANISATIONAL DESIGN & DELEGATION
8) An **Organisational Structure** has been put in place aligned to strategy, with lines of responsibility and appropriate segregation of duties.
9) Formally defined **Delegation of Authority**, including capital investment limits.
10) **Staff** have been appointed of appropriate calibre to fulfil their allocated responsibilities, with appropriate experience and qualifications checked on entry and monitored, with defined job descriptions. **Personal development** and appraisal procedures are in place to ensure an effective workforce.
11) **Senior Management remuneration** is designed to align personal and business objectives, as well as to discourage dishonest, illegal or unethical acts.
12) **Framework** of appropriate **policies**, standards and procedures **and control activities**, including **operational, financial and regulatory requirements**, are in place, communicated and compliance monitored. Significant changes are reported to the Board and relevance monitored.
13) **Framework** of **IT policies and control activities**, including segregation of duties, are designed and implemented to protect the completeness, integrity and security of our operations and data.

D) GOVERNANCE & FEEDBACK
14) The **Board** and **Audit Committee** have defined Terms of Reference and an effectiveness review process.
15) The Audit & Risk Committee seeks and receives appropriate **assurance** on key risks and controls (specifically including financial control and reporting) from sources such as Management representations, self-assessment and independent assurance functions (Internal Audit).
16) A **Whistleblowing policy** and service is available to all staff and calls are actively followed through and appropriately reported to the Board. Similarly a Complaints procedure is available to customers, suppliers and other external stakeholders.
17) **External reporting procedures** are formalised to present a fair, balanced and understandable assessment of the company's position and prospects to stakeholders, in compliance with the applicable regulations.

POL00423565

4b) Policy Framework Project update

Author: Mark Rodgers Sponsor: Mike Morley-Fletcher Meeting date: 05 May 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 also supports other Post Office initiatives such as the Partnership Banking Agreement work.

The project aims to develop a suite of key policies for Post Office and splits this into two sequential phases: the first is to confirm Corporate Services ("CS") policies, review them and, where necessary re-revise or develop them; the second phase will identify key policies from other areas of the business and ensure these are reviewed, re-drafted or developed and implemented too. Our external auditors have provided benchmark data which has been used to ensure the reasonableness and completeness of the final suite of policies (both CS and non-CS). As policies are developed or revised they will be presented for approval to the RCC/ ARC.

Questions?

PHASE 1

a) Are we still on plan for phase 1?
b) Can RCC ratify the policies we have developed or revised?
c) How will we manage subsequent implementation of the policies from phase 1?

PHASE 2

d) For phase 2, can RCC agree the proposed suite of policies, which have been subject to the benchmarking exercise, from other business areas?
e) What are the next steps?

Conclusion

PHASE 1

a) We are on track with phase 1 work for the seventeen CS policies and lessons learned are being documented. Drafting of the CS policies, review and sponsor/ Executive policy Owner sign off is nearing completion, due at the end of April 16 (see appendix 1). As part of phase 1, the review and remediation of policies for the March 2016 (Partnership Banking Agreement ("PBA") project deadline was met.
b) Seven key policies are presented for RCC approval (five from CS and one from IT and one from HR). A summary of the policies is attached (see appendix 5) and policy documents are included in agenda item 5, were approval will be considered.
c) These policies, once approved, will be rolled out to the business by the policy Owner. A policy implementation process has been developed with implementation owners and a suggested timeline for embedding the CS policies (see appendix 2). These will require agreement by key stakeholders for details and timelines. Arrangements to use a dedicated Sharepoint site as a repository are progressing with support requested from the Communications team.

PHASE 2

d) To establish a full suite of policies, including other business areas, we have developed a strawman list from reviewing other organisations and then used data provided by Ernst & Young to benchmark the list. The resultant set of key policies (see appendix 3) is presented for RCC review and agreement. A summary of the benefits of including and the consequences of not

POL00423565

including the three policies we believe we do not currently have, or do not have in adequate condition is attached (see appendix 4).

e) Once the final suite of policies is agreed by RCC, prioritised remediation will commence and then rolled out to the business.

Input Sought

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

a) the progress to date for the phase 1 CS policies, and

b) the benchmarked suite of policies from other areas of the business for phase 2.

Please note: policies submitted for approval are included in agenda item 5, where approval will be considered.

Appendices

Appendix 1: Corporate Services – progress to date
Appendix 2: Policy Implementation Process
Appendix 3: Key Policy Framework – latest update of strawman
Appendix 4: Key Policy Framework – benefits of including three further policies
Appendix 5: Policy Approval – Summary of policies and rationale

POL00423565

Appendix 1: Corporate Services – Progress to date

We are on track with phase 1 work for the seventeen CS policies and lessons learned are being documented. Drafting of the CS policies and review and sponsor/ Executive policy owner sign off is nearing completion, due at the end of April 16.

Five of these CS policies, highlighted in bold, are being presented for approval by the RCC/ ARC.

Policy	Policy Owner	Existing Policy reviewed	Policy Drafted/ Stakeholder review completed	Target for Policy RCC/ARC approval
Corporate Governance, including				
1) Board Constitution	Alwen Lyons	No existing policy	N/A (*See Note 1)	N/A (*See Note 1)
2) Conflicts of Interest	Alwen Lyons	Yes	ETA:End of April	July 2016
3) Enterprise Risk	Mike Morley-Fletcher	Yes	Completed	Not required, RCC Approved during 2015 (*See Note 2)
4) Internal Audit Charter	Garry Hooton	N/A *(*See Note 3)*	N/A (*See Note 3)	N/A (*See Note 3)
5) Whistleblowing	**Nisha Marwaha**	**Yes**	**Completed**	**May 2016**
6) Investigations	Nisha Marwaha	Yes	Completed	July2016
Security				
7) Physical Security	John Scott	Yes	Completed	July 2016
Information Security, including				
8) Cyber and Information and Security	Julie George	Yes	Not required, RCC Approved during 2015 (*See Note 2)	Not required, RCC Approved during 2015 (*See Note 2)
9) IS - Acceptable Use	Julie George	Yes		
10) Business Information Systems	Julie George	Yes		
11) Information Assurance (incl. Data Protection)	Julie George	Yes		
Financial Crime, including				
12) Financial Crime	**John Scott**	**Yes**	**Completed**	**May 2016**
13) Anti-Bribery and Corruption (incl. Gifts and Hospitality)	**Ben Foat**	**Yes**	**Completed**	**May 2016**
14) Anti-Money Laundering (incl. Counter Terrorism & Sanctions)	**John Scott**	**Yes**	**Completed**	**May 2016**
15) Cyber Fraud (including Forensics)	Julie George	Yes	Not required, RCC Approved during 2015 (*See Note 2)	Not required, RCC Approved during 2015 (*See Note 2)
16) Prosecution (England & Wales)	Rodric Williams	Yes	Completed Feb 2016 (*See Note 4)	Completed Feb 2016 (*See Note 4)
Business Continuity, including				
17) Business Continuity	**Jonathan Waples**	**Yes**	**Completed**	**May 2016**

* Note 1. There is no overarching Board Constitution policy. Direction is provided by the existing Articles of Association, Matters referred to Board, ToRs, Delegation of Authority
* Note 2. These policies have been reviewed and already meet policy standards. RCC approved these policies during 2015 and no remediation is required for these policies. Policies will be reviewed as per the documented policy review cycle in each case.
* Note 3. The Internal Audit Charter is denoted N/A because it is already a compliant document with Internal Audit International Professional Practice Framework Standards which incorporate qualitative documentation standards.
* Note 4. The Group Prosecution Policy (England & Wales) was approved by the Board in February 2016.

POL00423565

Appendix 2: Policy Implementation Process

These are the steps we identified for planning and monitoring implementation of policies. They will be trialled with CS polices before being recommended to other business areas. An estimated timeline of 6 months has been used.

Implementation Steps	Details	Example timeline (estimated at 6 months)
1) Establish accessible storage and maintenance protocols	❑ Publish documents to SharePoint ❑ Update Intranet and links (checking searches) ❑ Define maintenance	By 31/05/16
2) Communicate policy and requirements	❑ Agree audience (for communication and training) ❑ Develop communications policy and messages ❑ Communicate policy and requirements	By 30/06/16
3) Develop and deliver supporting training	❑ Identify resources and compile modules/ materials (Learning Academy) ❑ Coordinate and deliver training ❑ Publish to SharePoint	Develop by 31/07/16, deliver by 31/08/16
4) Identify and develop associated controls	❑ Confirm associated controls framework and catalogue controls library ❑ Create matrix of responsibilities (include RACI if required) ❑ Confirm controls operating as expected	Identify by 30/06/16, develop by 31/08/16
5) Monitor and measure compliance	❑ Identify and define compliance monitoring procedures, systems and controls ❑ Identify measures and test monitoring plans ❑ Commence monitoring routines ❑ Capture results, evaluate, define management information and report to governance committees	By 30/10/16
6) Review policy	❑ Use monitoring results to evaluate current policy controls and continuing appropriateness of policy ❑ Maintain policy review log ❑ Conduct annual/ bi annual policy reviews and report to relevant governance body	By 31/12/16

POL00423565

Appendix 3: Key Policy Framework – Latest update of strawman

Phase 1 is the suite of Corporate Services policies which have been reviewed and remediated.

Phase 2 is a proposed strawman of possible key policies* from other business areas. Through review of other organisation's policy suites and on consideration of our specific needs we have developed a proposed strawman list of key policies. We have then used data provided by Ernst & Young to benchmark this policy suite to produce our recommendations below. In addition to the CS policies already agreed, we are proposing a further fourteen policies. Of these, we already have most in a reasonable state. The three highlighted in yellow and bold either are not formalised policies or are in fragmented form: all have some reference material to help with drafting of a full policy. Suggested benefits of including these three further policies are included in appendix 4.

Key Framework Policy (Big P)	Policy Sponsor (GE Owner)	Policy Owner
PHASE 1 – CORPORATE SERVICES		
Corporate Governance, including 1) Board Constitution (Articles of Association, Matters referred to Board, ToRs, Delegation of Authority)** 2) Conflicts of Interest 3) Enterprise Risk 4) Internal Audit Charter 5) Whistleblowing 6) Investigations	Jane MacLeod	1) Alwen Lyons & Victoria Moss 2) Alwen Lyons & Susie Hayward 3) Mike Morley-Fletcher 4) Garry Hooton 5) Nisha Marwaha 6) Nisha Marwaha
7) Physical Security	Jane MacLeod	7) John Scott
Information Security, including 8) Cyber and Information and Security 9) IS - Acceptable Use 10) Business Information Systems 11) Information Assurance (incl. Data Protection)	Jane MacLeod	8) Julie George 9) Julie George 10)Julie George 11)Julie George
Financial Crime, including 12) Financial Crime 13) Anti-Bribery and Corruption (incl. Gifts Policy) 14) Anti-Money Laundering (incl. Counter Terrorism, Sanctions) 15) Cyber Fraud *(same as 8)* 16) Prosecution (England and Wales)	Jane MacLeod	12) John Scott 13) Ben Foat 14) John Scott 15) Julie George 16) Rodric Williams
17) Business Continuity	Jane MacLeod	17)Jonathan Waples
PHASE 2 – NON-CORPORATE SERVICES		
18) Customer Treatment (including Elderly/ Vulnerable)	Martin George	18)To be confirmed
19) Social Purpose - Distribution Network Coverage (Entrustment Letter, Nov 2013)**	Kevin Gilliland	19)Kevin Seller
20) Business Change Management	David Hussey	20)Alison Thompson
Finance, including 21) Accounting and Reporting Manual 22) Treasury Risk Management **23) Procurement** **24) Travel & Expenses** 25) Disaster Recovery	Alisdair Cameron	21) Dave Carter 22) Dave Carter/ Charles Colquhoun 23) Mark Dennis 24) Mark Dennis 25) Stephen Hayes
Human Resources, including 26) Talent and Resourcing 27) Reward and Recognition 28) Learning and Development 29) Performance, Attendance and Behaviour 30) Health & Safety 31) Code of Business Standards	Neil Hayward	26) Tom Moran 27) Tom Moran 28) Tom Moran 29) Tom Moran 30) Martin Hopcroft 31) Colin Stretch

Notes
** 'Big P' or key policies are those which are "materially" important because they provide direction to the content, extent and style of how our Board expects the company and our staff to act and behave in response to "key" needs of our stakeholders.*
*** Where there is no actual policy document, details of alternative documentation which provides the direction of a policy is given in italics. For instance we do not have a Board Constitution policy, but direction is provided by the Articles of Association, Matters referred to Board, Terms of References, Delegation of Authority, which have been approved by the Board.*

POL00423565

Appendix 4: Key Policy Framework – Benefits of including three further policies

We have used data provided by Ernst & Young to benchmark this policy suite to produce our recommendations (see appendix 3). Of the In addition to the CS policies already agreed, we are proposing a further fourteen policies. Of the fourteen, we have eleven already and three we do not have. Below is a view of why we need the three additional policies. The rationale is in terms of the benefits for inclusion and the negative consequences if we do not set policy.

Rationale

Proposed Policy	Benefits of this Policy	Consequences of not having this policy
18) Customer treatment	• Focuses identification of target customers • Supports customer-centric reputation • Enhances social purpose commitments • Supports customer service (e.g. sector NPS, Effort, CSAT, Wait time) • Helps accuracy of management reporting and effectiveness of customer understanding	• Potential censure and sanctions around vulnerable customers by regulators • Raises potential conduct risk challenges • Potential complaints due to uncertainty in standards •
23) Procurement	• Supports consistent contract management dealings with third parties (depending on TOM) • Supports procurement efficiency and cost control • Helps accuracy of management cost information for decision making • Efficient, clear processes make us good to work with	• Additional cost through inefficient and inconsistent procurement • Lack of contract certainty • Potential risk of poor service provision and impaired or failed service levels • Potential FCA SYSC8 censure and sanctions • Increases litigation risk
24) Travel & Expenses	• Supports cost control consistency • Helps accuracy of management cost information for decision making • Clarity for staff on what can/ can't do, should/ shouldn't do	• Additional cost through inefficient travel and inappropriate expenses • Increased potential for financial crime • Reputational risk • Potential accounting standards breaches • Increased complaints from staff

POL00423565

Appendix 5: Policy Approval – Summary of policies (7) and rationale

See agenda item 5 for policy documents, where approval will be considered.

Ref	Key Framework Policy	Sponsor (GE Owner)	Policy Owner	Why is this policy needed?	Approved by?	How will the policy be implemented?	How will policy compliance be monitored?
12) (PBA)	Financial Crime	Jane MacLeod	John Scott	To help Post Office meet legal and regulatory obligations within appetite, and to manage financial crime risks reducing actual loss, avoiding potential losses.	RCC and ARC May 2016	Proposal for process to implement policies, including: • where they should be stored • how they should be communicated and supported with training • how they should be controlled, monitored and reviewed. Please refer to appendix 2 for more details.	1. Policy Compliance Manager will coordinate, and ensure QA standards, including compliance monitoring. 2. Policy Owner undertakes compliance, and will identify measures, develop monitoring processes, track results and provide reporting with MI to the relevant governance body.
13) (PBA)	Anti-Bribery and Corruption (incl. Gifts & Hospitality)	Jane MacLeod	Ben Foat	To help Post Office meet its legal and regulatory obligations within appetite, to help manage ABC risks, and support good conduct standards in all dealings.	RCC and ARC May 2016		
14) (PBA)	Anti-Money Laundering (incl. Counter Terrorism, Sanctions)	Jane MacLeod	John Scott	To help Post Office meet its legal and regulatory obligations within appetite, and to help manage AML (CTF and Sanctions) risks whilst reducing actual loss, and avoiding potential losses.	RCC and ARC May 2016		
17) (PBA)	Business Continuity	Jane MacLeod	Jonathan Waples	To embed a framework to identify potential threats to business continuity, and to help manage impacts to business operations. It is a set of standards which support resilience and sets out the capabilities to respond.	RCC and ARC May 2016		
25) (PBA)	Disaster Recovery	Alisdair Cameron	Stephen Hayes	To embed a framework to identify potential threats to disaster recovery, and to help manage impacts to IT/ business operations. It is a set of standards which support resilience and sets out the capabilities to respond.	RCC and ARC May 2016		
26) (PBA)	Talent and Resourcing: HR Vetting	Neil Hayward	Sean Leahy	To ensure Post Office operates vetting processes in a legal, and compliant way. To embed standards to control and reduce the risks of error, theft, fraud or misuse of facilities. To ensure Post Office engages with suitable workers.	RCC and ARC May 2016		
5)	Whistleblowing	Jane MacLeod	Nisha Marwaha	To help Post Office meet its legal and regulatory internal and external obligations. To implement good practice and engender good standards in this context.	RCC and ARC May 2016	As above	As above

POL00423565

4c) Business Continuity & Crisis Management Project update

Author: Jonathan Waples Sponsor: Jane MacLeod Meeting date: 5th May 2016

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 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 and is divided into three phases:

- Phase 1: Gap analysis; Business Continuity policy creation; Crisis Management review; pilot Business Continuity activity
- Phase 2: Expanded BC activity; Business Continuity Management Systems Framework delivery
- Phase 3: Improved BCMS awareness; BCMS integration to BAU.

In addition, the Business Continuity Project Manager is available to assist the business with its ongoing BC and CM support needs.

Questions this paper addresses

1. How have we progressed our plan?
2. How is this bringing us in line with ISO 22301?
3. Can we answer the ARC's request on top suppliers yet?
4. Can we answer the ARC's request on Crisis Management process yet?

Conclusion

1. 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 processes (end of April 2016). Business Impact Assessments for the three priority areas are in progress and

POL00423565

will enable review of BC Plans (for these areas) by the end of May. Phase 1 is near completion and Phase 2 is underway. See Appendix 1 for details.

Planned progress was for 40% of achievement to conformity to ISO 22301 at this stage, which has been achieved. The majority of effort in the opening stages of the project related to discovery and gap analysis of current capability against the agreed standard. From this point, activity is focused on achieving alignment to the best practice principles, and will therefore deliver significant advances in conformity over the coming months.

2. The ARC requested a view on top suppliers and their Business Continuity capabilities, and a reach-out was initiated to request visibility of BC planning, capability & testing regimens. Results have been slow in delivery, despite persistent follow-up by POL relationship managers, and project resources.

3. Additionally, the ARC enquired about how their potential engagement in the Crisis Management process might be managed during an invocation. This is described in sections 5.4 and 5.5 of the Major Incident Response Procedure (Appendix 2). Designed to engage the right stakeholders, at the right time, during any invocation, the procedures state that NED involvement would be requested – by the Gold Team (all GE) - at the height of a Crisis event.

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.

POL00423565

Appendix 1

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	Activity - BPT Invocation Test Publish Major Incident Response Procedure	
- Schedule and begin Business Impact Assessments	Develop BIA Methodology Documentation Business Impact Analysis Process Documentation Business Impact Analysis Workbook	Supply Chain BIA - Sean Farrow Business Impact Assessment: Supply Chain	Financial Services BIA - Business Impact Assessment: Financial Services IT BIA - Andy Garner Business Impact Assessment: IT
- Schedule and begin Business Continuity Plan Development		Supply Chain Business Continuity Plan - Sean Farrow	Business Continuity Plan: Supply Chain Activity: Business Continuity Rehearsal: Supply Chain - Earliest Possible Date
- On-going BCM Planning for priorities (embedding to BAU)			Property Business Continuity Plan - Kevin Seller Business Continuity Plan: Property Activity: Business Continuity Rehearsal: Property - Earliest Possible Date IT Business Continuity Plan - Andy Garner Business Continuity Plan: IT Activity: Business Continuity Rehearsal: IT - Earliest Possible Date
Phase Two: Expanded BC activity; BCMS Framework delivery			**End of July Completion Target**
- BC Management Programme Structure		Procedure for the Management of Non-Conformity	Continuous Service Improvement Process Business Continuity Programme Auditing Process Business Continuity Programme Audit Plan Business Continuity Exercising & Testing Schedule Business Continuity Test Plan Business Continuity Test Report Procedure for the Control of Documents Procedure for the Control of Records Business Continuity Communication Plan BC Risk Assessment Process BC Risk Assessment Report BC Risk Assessment Workbook BC Risk Treatment Plan
- 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

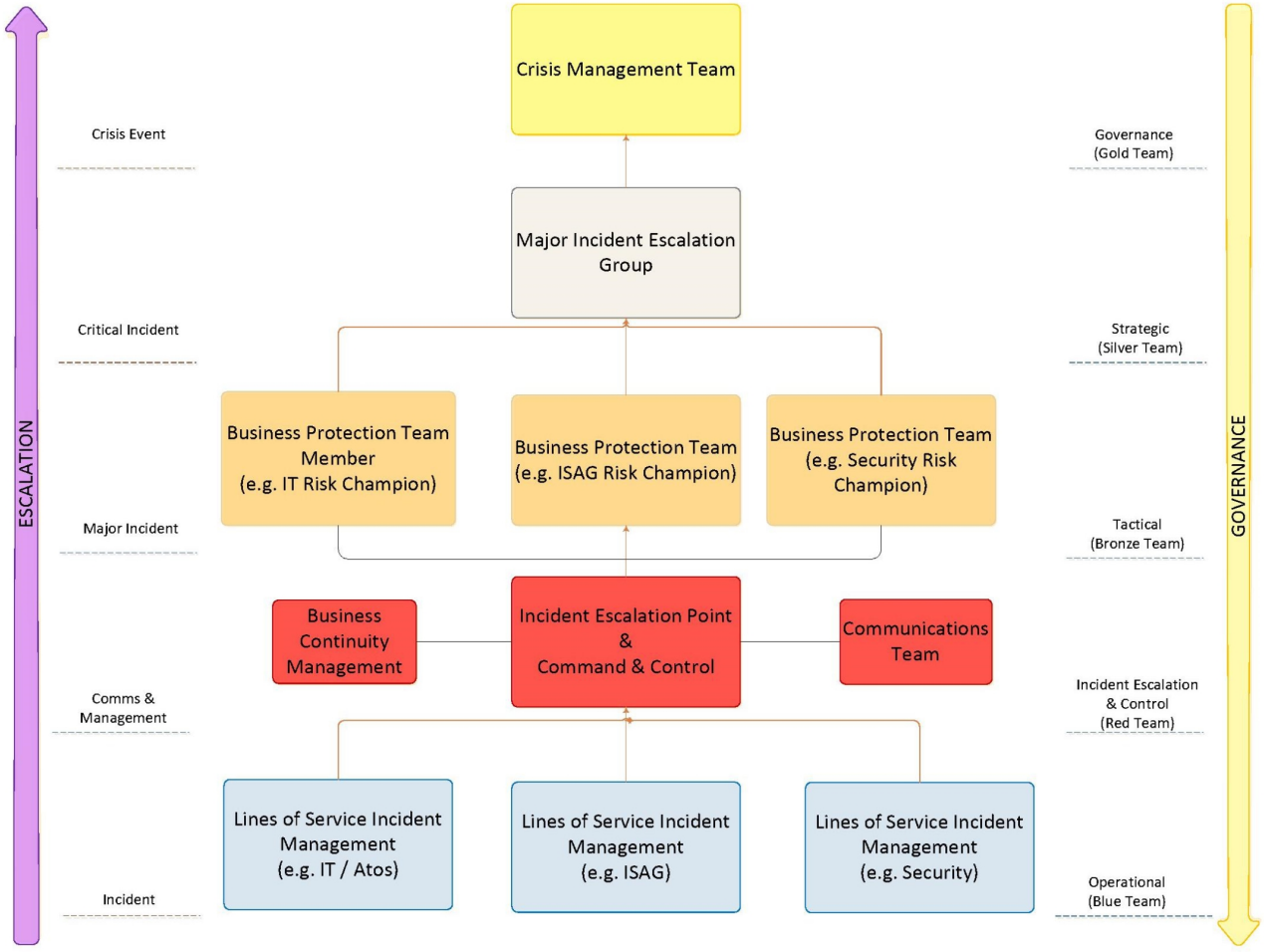
POL00423565

Appendix 2

The following is an extract from sections 5.4 & 5.5 of "Major Incident Response Procedure", detailing the Major Incident Response Teams' construct and each levels roles and responsibilities, including senior stakeholder engagement during a Crisis Management invocation.

Designed on the principle of escalation to the relevant business stakeholders and specialists, the construct swiftly engages appropriate resources efficiently in resolving the incident. In consequence, GE involvement will be on a selective basis if invoked at Silver Team level, or on a full basis at Gold Team level. An invocation of the Gold Team may instigate, the involvement of our major stakeholders, such as the NEDS or ShEx.

5.4 Major Incident Response Teams' Construct



POL00423565

5.5 Major Incident Response Teams' Responsibilities

GOLD TEAM – Crisis Management Team (CMT)

All GE Members (potentially other major stakeholders – NEDs, Ministers, etc.); Instigated at point of high crisis (escalated Major & Critical Incidents; prolonged severe operational disruption across majority of business units; reputational damage or risk; Ministerial or Judicial scrutiny, etc.)

SILVER TEAM – Major Incident Escalation Group (MIEG)

Selected, appropriate, GE membership supported by senior management teams; instigated in response to major incident event (escalated Major incidents; significant operational disruption across multiple business units; major disruption to individual office / operational locations; major disruption to IT service(s) provision across all / majority of network; significant staff abstraction events (snow days, transport strikes etc.). Tactical guidance to BRONZE team, in response to GOLD, as appropriate.

BRONZE TEAM – Business Protection Team (BPT)

Senior management representation from across all business units. Invoked on escalation from any departmentally managed Incident to a Major Incident. Remains in direct control of Operational resources during ALL levels of response above Incident, receiving tactical and strategic guidance from SILVER & GOLD teams respectfully.

RED TEAM – Incident Escalation Point & Command and Control (EIP / C&C)

Permanently assigned resource dedicated to managing incident escalation and communication across the POL network (branch & offices). Single, direct line of communication to Operational Teams. Operates across all levels of Crisis Management Construct from the moment of Incident escalation to the point of closure. Has direct engagement with Business Continuity function and Communications Team, to ensure adherence to CM & BC process and appropriate internal and external comms.

> *Caveat: At this point in time, there is no single capability for this function within POL. Escalation is affected by a call to Atos Service Desk requesting they contact the Business Protection Team and provide a conference call bridge for this group. At that point the central management of incident logging, comms, BC response etc. concludes, and reverts to BPT. This is inefficient, and the recommendation is that this hub activity be brought back in-house, potentially utilising an enhanced, permanent Command & Control Centre.*

BLUE TEAM – Operational Incident Management

Incident Management activities currently controlled within respective business units, either internally or via a third party (e.g. Atos) will need to develop an escalation route into the RED Section in order to engage Major Incident or Crisis Management

POL00423565

4d) Assurance Mechanisms: Executives' Declaration and CSA

Author: Deana Herley Sponsor: Mike Morley-Fletcher Meeting date: 5 May 2016

Executive Summary

Context

The purpose of this paper is to provide an update on the progress made in enhancing our Assurance Mechanisms. In particular, how we have started:

- the **Executives' Declaration** return, completed by the General Executive (GE), and
- **Control Self-Assessment** (CSA) techniques to provide assurance to Management and the Board (via the ARC) over key control areas – we have started with the Financial Reporting processes and then will move to the General Control Framework.

Questions this paper addresses

1. How have we progressed with trialling the Executives' Declaration?
2. What are the results of the Executives' Declaration, are further disclosures required?
3. Is the implementation of CSA on target?

Conclusion

1. **Executives' Declaration**. At the last RCC we launched a new exercise, run by Internal Audit, to support GE members in considering (and attesting) if any additional disclosures were required in our Annual Report as part of our year-end procedures. Against a set of key question areas, this involved GE members consulting with their lead teams and making further enquires with relevant Finance, Risk and Legal representatives to identify any additional issues or concerns that have not been already recorded as a part of normal management processes. Going forward, GE members will be asked to attest twice annually, at half year and year end in support of our Interims and Finals.
2. **Executives' Declaration exceptions.** Outputs have been collated and reviewed for consistency against Internal Audit reviews. **Seventeen exceptions were identified:**
   - six exceptions have already been disclosed
   - one exception (qu 5, item i) requires disclosure but this has not been made yet – re mobile decision
   - nine were considered by the owner, but the decision is that no disclosure is required
   - one exception (qu 8, item o) has been identified which requires further debate over whether we should disclose – re "extent of oversight over levels of compliance of sales of regulated products in the network".

   All items noted are summarised in appendix 1 and exceptions highlighted in yellow.
3. **Control Self-Assessment.** To enable automation of CSA of the Financial Reporting processes, a task management workflow solution has been selected (TrAction hosted by PWC). We will start with **Fixed and Intangible Assets** in May. A phased approach will then be taken to on-board the 11 other financial reporting processes (**Jun-Sept**). Independent testing over the Financial Controls Framework project deliverables by Internal Audit will be planned for June. As noted previously the General Control Framework will also be self-assessed using TrAction.

POL00423565

Input Sought

The Committee is asked to review the information provided in appendix 1 and confirm whether:

- the exception noted should be disclosed
- agree with exceptions where decided is NOT to disclose
- after consideration of these items, any other exceptions should be considered.

POL00423565

Appendix 1 – Exceptions

EXECUTIVES' DECLARATION SUMMARY			
Statement	**Exceptions**	**GE Member**	**Decision**
1) any material **risks** to PO that are not captured in the Group Risk Profile	**None.**	**All**	**N/A**
2) any material **control** failures or breaches, including of the **General Control Framework** and **policies** that I am accountable for	**a) Postmasters' Compensation re-statement,**	**Alisdair Cameron**	**Disclosed already**
	b) General weakness in consistency and transparency of **financial reporting controls.**	**Alisdair Cameron**	**Disclosed already**
	c) The **General Control Framework** ('GCF') is of recent implementation within Post Office and therefore work to assess the level of controls already in place and whether they are fit for purpose, is still at a preliminary stage.	**Jane MacLeod**	**Disclosed already (in Risk note)**
	d) Further, the **policy suite** to support the GCF is not complete and those policies for which I am responsible have not yet been through governance, nor do we yet have a **self-assessment process** against those controls and policies.	**Jane MacLeod**	**Disclosed already (in Risk note)**
3) any material **frauds**, **irregularities or losses** that have come to light, whether carried out by our staff, agents, contractors, suppliers or partners	**None.**	**All**	**N/A**

POL00423565

4) any complex or subjective **accounting judgements, estimates and revenue transactions**	**e) Accounting for Gamma**.* **(see below)** Under the agreement with Bank of Ireland, in 2012 POL received one-off, non-refundable income in lieu of providing distribution for Bank of Ireland products, including insurance products. This income (Gamma) is being recognised over the period of the agreement. Following the Project Hawk acquisition, POL no longer has any obligations to Bank of Ireland in respect of insurance and a paper has been submitted to the external auditors by Group Financial Control setting out the rationale for recognising an appropriate portion of the Gamma income (c£4.5m) in 2015/16.	**Alisdair Cameron & Nick Kennett**	**Disclosed already**
	f) Exceptionalisation of the costs of project Hawk in POL and POMS*: A paper setting out the rationale for this has been submitted to the external auditors by Group Financial Control. Total amount treated as exceptional is £3m.	**Nick Kennett**	**Disclosed already**
	g) Estimation of FRES profit share at year end: The draft financial statements for 2015/16 include income of £35.3m in respect of POL's share of profits of its FRES joint venture. Of this, £2.4m relates to the profit share for March 2016. This amount is consistent with estimates from FRES management but will not be confirmed before POL closes its 2015/16 books.	**Nick Kennett**	**Proposed no disclosure required**
	h) Estimation of Credit Card profit share: The financial statements for 2015/16 include income of £750k in respect of profit share on credit cards under the arrangement with Bank of Ireland. This amount has been confirmed verbally by Bank of Ireland, but the actual amount will not be confirmed before POL closes its 2015/16 books.	**Nick Kennett**	**Proposed no disclosure required**
5) any **provisions or exceptional items** not already recorded	**i)** We are just disclosing the need to provide on the **Mobile decision**.	**Alisdair Cameron**	**Decision to disclose made, but disclosure is currently outstanding**
6) any **liabilities and contingencies**, including those associated with guarantees	**j)** There is a risk that the **RMG Resource Costs and Incentives claim** as a result of delayed IT separation will exceed the estimate. POL received an invoice for £837,783 on 13 November 2015. This was formally disputed with RMG. It is not clear what further	**Jane MacLeod**	**Proposed no disclosure required**

POL00423565

	amounts they may claim for the period through to end of March 2016, but in conversations RMG have made reference to their claim potentially amounting to approximately £3m (and this is similar to the projected costs of this claim identified as approx. **£2.3m** by Roger Middleton).		
7) any material **legal action** being taken by or against PO	**k)** Threat from British Gas in the last couple of days for **unpaid energy bills**.	**Alisdair Cameron**	**Proposed no disclosure required**
	l) On 13 April 2016 we received a letter from Freeths Solicitors advising that they have **lodged a claim in the High Court on behalf of some 91 claimants**. They have not as yet served the claim on us and accordingly as at the date of this declaration we remain unsighted on the grounds of the claim, who it is brought on behalf of, or the remedy they are seeking.	**Jane MacLeod**	**Proposed no disclosure required**
	m) As proceeding against Post Office may be commenced by service on any POL business address (which includes Customer Service Centres and Crown Offices), there is **no guarantee that the relevant documents will be forwarded to the legal team with the consequence that we may not be aware of such proceedings**.	**Jane MacLeod**	**Proposed no disclosure required**
8) any **legislative**, **regulatory or contractual compliance issues** that have come to light	**n)** We are managing **risks around public procurement**, especially the **contract extension with Fujitsu**, which was published in February.	**Alisdair Cameron**	**Proposed no disclosure required**
	o) Post Office Limited as Appointed Representative for POMS has limited **oversight over the levels of compliance of sales of regulated products in the network**, in particular in **relation to over 50s life insurance and travel insurance**. While complaint levels are low, this does not of itself provide **assurance that sales are compliant**.	**Jane MacLeod**	**Debate if this should be disclosed (in the Risk note[1])**

[1] The Risk Note (Control environment: 2016/ 17) has wording to inform the reader of the current state of our ICF and policies (e.g. subtle reference to need for some improvement) and that we plan to progress this next year. In addition, however, we can add the following wording, ***"As part of embedding the risk management framework, we will review the model for oversight of regulatory compliance across the various sales channels to consider whether enhancements are required."***

POL00423565

	p) During 2015-16 I became aware that POL had entered into **network contracts with operators who were at the time, appointed representative of third parties**, giving rise to potential regulatory and contractual breaches.	**Jane MacLeod**	**Proposed no disclosure required**
	q) I am aware that during 2015/16 there were a number of **branches which operated under expired contracts or without a written contract.**	**Jane MacLeod**	**Proposed no disclosure required**
9) any material **new contracts** entered into, and where I have not followed the **contract process**	**Same as n) Fujitsu extension, CSC extension**.	**Alisdair Cameron**	**Refer to question 8, item n**
10) any direct or indirect **personal interest** in any transaction, arrangement or related parties entered into by PO	**None**.	**All**	**N/A**
11) any material events that could **crystallise** before the end of the reporting period above	**Same as j) Mobile decision**.	**Alisdair Cameron**	**Refer to question 5, item i**
12) any **other information** that could have an impact on period (indicated above) when drawing up our annual report.	**Same as b)** I am aware of a review of **POL internal controls** being carried out by KPMG for the CFO and that preliminary findings suggest some potential gaps versus an ideal control environment. However, I am not aware of the conclusions of this work, their implications or their potential materiality in the context of POL group.	**Nick Kennett**	**Refer to question 2, item b**

POL00423565

4e) Disclosure in Annual Report

Author: Mike Morley-Fletcher Sponsor: Jane MacLeod Meeting date: 5 May 2016

Executive Summary

Context

As agreed by RCC and ARC, compliance with the UK Corporate Governance Code is not sought at present, however, we intend to maintain *"standards of corporate governance appropriate for our ownership structure, our commitment to our social purpose and our strategy for commercial sustainability"*. We have used this to guide our disclosure notes.

For this year's risk, control and assurance disclosures, the Risk and Internal Audit team reviewed the previous PO Annual Report, discussed best practice with our external auditors and considered other relevant organisation's reports to ensure we are providing appropriate, up to date and informative disclosures to our stakeholders. Several enhancements have been made and are detailed below. *Please read in conjunction with relevant sections in the draft Annual Report – see appendix 1.*

Questions this paper addresses

1. How have we explained our approach to Corporate Governance compliance and disclosure?
2. What changes have we made to the risk and control disclosures on how we manage risk (as part of the GE note)?
3. What changes have we made to the risk and control disclosures on how we govern risk (as part of the ARC note)?

Conclusion

1. Corporate Governance compliance statement – redrafted by RCC/ ARC:
   - Includes our redrafted Corporate Governance statement, *"PO maintains standards of corporate governance appropriate for our ownership structure, our commitment to our social purpose and our strategy for commercial sustainability"*.
2. Managing Risk – fuller details are provided on how we manage risk and what our principal risks – see appendix 1 and 2:
   - Explains in greater detail our approach to risk, our risk management framework and our risk governance.
   - Includes for the first time a description of our Internal Controls Framework, now that we have defined it, are assessing and remediating it, to explain to stakeholders the key general controls we use to manage the business.
   - Provides more details on our principal risks, disclosing all 14 risks identified by the RCC (8 included last year), with updated details of causes, consequences, mitigations and trends compared with last year.
3. Governing Risk – fuller details are provided on how Internal Audit assures the Board and how the Board conducts its annual assessment of our risk management framework and internal controls:
   - Includes for the first time a description of Internal Audits activity, how the annual plan is developed and details of the types of audits conducted in 2015/ 16.

POL00423565

- Includes for the first time a description of how the Board, via the ARC, assesses the risk management framework and systems of internal control.

Input Sought

The Committee is asked to review the disclosures presented, in particular the details of our Principal Risks and Mitigations in appendix 2, and provide any input or feedback, before they are presented to the ARC for approval.

POL00423565

Appendix 1: Risk Extracts from the draft 2015/ 16 Annual Report - Managing our risks

Points to consider:

- section on Internal Control could be shortened?

Our Approach to Risk

We define risk as anything that can adversely affect our ability to meet the Post Office's objectives, maintain its reputation and comply with regulatory standards.

Risk is not something that we can avoid. It is an inherent part of how the PO seeks to grow and create value. Instead we seek to understand and harness risk in the pursuit of our aims and business plan objectives. As we progress, our aim is to operate within an acceptable level of risk taking, in accordance with risk appetite parameters set by the Board.

All staff are expected to be aware of risks in their areas of responsibility and manage those risk intelligently in their day-to-day activities.

Risk Management Governance

The Board is accountable for the risk management and internal control systems in the Post Office, for reviewing their effectiveness and for determining the nature and extent of the principal risks. Responsibility for day-to-day operations rests with members of the Group Executive. The Risk and Compliance Committee, on behalf of the Group Executive, reviews the operation of the risk management process and management of the principal risks. The committee is chaired by the General Counsel, membership includes all of the Group Executive and the output is reported to the Audit, Risk & Compliance Committee (ARC).

Assurance for the Board over the effectiveness of our risk management and internal controls is provided by the Audit, Risk and Compliance Committee, through review of reports from Management, particularly the Risk And Compliance Committee (RCC), Internal Audit, external advisers and External Audit.

For further details on Governance of our risk management and internal controls see XXX on page YYY.

Our Risk Management Framework

To improve our ability to consistently spot, manage and monitor risks, and take advantage of opportunities we might otherwise miss, we have developed a structured framework for assessing, managing and communicating risk. The framework identifies roles and responsibilities, the policies for how risks are managed, the tools and processes used, a risk appetite statement and the reporting outputs to inform both Management and the ARC.

Material risks are identified by business areas (bottom up analysis) for their own risk management; Group Executive members review these and add further strategic and external perspectives (top down review). The scope of risks to consider is facilitated by a Risk Universe. Impact and likelihood is assessed for evaluating each risk, after consideration of the controls we have in place. Where the resultant, "net", risk profile is considered in excess of our risk appetite, a response will be needed to bring the risk back within an acceptable level of risk taking. For other risks we may want to introduce monitoring procedures. Details of our Principal Risks are included on page ZZZ.

Our Control Framework

Our risk management efforts are underpinned by our internal control framework. The Board has put in place an organisational structure with formally defined lines of responsibility and delegation of authority. Executive Management have established procedures for setting our direction, planning and controlling the operation of our business, and reviewing and monitoring our performance and conduct. These include:

POL00423565

- communication of the Group's strategy, objectives and targets
- expectations of standards of conduct by our colleagues as set out in our Code of Business Standards
- definition and review of our social purpose
- setting by operating divisions of the annual and three-year operating and capital plans and review by Board. This includes the identification and assessment of risks compared to our appetite
- monthly comparisons of operating divisions actual financial performance with budget, with consideration by the Board of year end forecasts
- an organisational structure with lines of responsibility and appropriate segregation of duties
- change management approach, resources and governance are used to manage significant projects
- formally defined delegation of authority, including capital investment limits and a treasury policy
- appointment of employees of the necessary calibre to fulfil their allocated responsibilities, with formal personal development and appraisal procedures
- senior management remuneration designed to align personal and business objectives, as well as to discourage dishonest, illegal or unethical acts
- a framework of operating, financial and IT policies and procedures, communicated and monitored
- a whistleblowing procedure for colleagues to raise concerns in confidence and if required, anonymously; a complaints procedure is available to customers and third parties.

Progress during the year and plans for next year

During the year, we have continued to develop our risk management capability. Highlights of what's been achieved and what is planned for next year include:

Risk assessment: during 2015/ 16, there has been more regular use of the risk management framework in business areas and by RCC, with greater focus on defining further actions required to manage risks and the introduction of longer term horizon scanning	**Risk assessment:** for 2016/ 17, we plan to focus our incident reporting process to provide lessons learnt on our risk assessments and operationalise our risk appetite further
Control environment: during 2015/ 16, we have reviewed the appropriateness of our Internal Control Framework and our key policies and identified appropriate remediations	**Control environment:** for 2016/ 17, we plan to formalise our monitoring mechanisms for both our Internal Control Framework and our key policies

POL00423565

Appendix 2: Risk Extracts from the draft 2015/ 16 Annual Report – Principal Risks

Points to consider:

- descriptions for changes in risk profile
- direction for changes in risk profile.

These are our principal risks, detailed with their potential impact and how the Post Office manages them, plus trends of changes to the risk profile from last year.

Any of these risks could have a material impact on our results, condition and prospects. However, these risks should not be regarded as a complete and comprehensive statement of all potential risks; some risks are not yet known and some that are not considered material could later turn out to be material.

Potential risks **Description of risk and causes**	**Consequences**	**Change in Risk Profile**	**Key Mitigations** **Details of risk management and mitigation**
STRATEGIC RISKS			
Competitive threat Post Office faces both opportunities for and threats to income from our competitive market place. - The Mails and parcels market remains intensely competitive and has seen some high profile failures due to inadequate margins. - Government Services are impacted by increased use of digital channels and reduced public spending. - Financial Services is a challenging market where responding quickly to different strategies, business models, and products is essential to growth.	This could result in not achieving our growth objectives, losing market share and revenues.	Increasing competition across the markets in which Post Office operates leads to an increasing risk profile	• Competitor impact tracked and customer perceptions used to inform our decisions. • Our strategy is focussed on customer requirements, utilising new technology to help us introduce customer centric propositions backed by robust distribution channels. • Each product proposition has a tailored strategy and business diversification provides different response options if there is significant threat to one business area.
Dependency on strategic relationships Post Office has strategic relationships which are key to its product offering and growth, for instance with Royal Mail Group and Bank of Ireland. Misalignment with our strategic partners could result in products that do not support our growth strategy or meet our customer or market requirements.	This could result in not achieving our growth objectives, losing revenue and market share.	Risk profile is unchanged	• Close working relationships established with our strategic relationships. • Scheduled interactions with our strategic partners to improve the product offering and service to drive growth and profitability for us and them. • Contractual arrangements monitored to ensure they provide value and security.
TRANSFORMATION RISKS			

POL00423565

Benefits from business transformation not realised Planned for savings from our transformation programme may be delayed or not achieved, or overall service compromised, due to inadequate capability, capacity and the scale of change.	This could result in not achieving our growth objectives, loss of revenue and cost savings, reduced customer satisfaction and damage to reputation with stakeholders.	Risk profile is unchanged	• Programme management office established, with assurance oversight. • Detailed plans in place to manage the transformation, and identify risks to ensure transformation activities are delivered within budget and on time. • Benefits are tracked from inception to delivery and into business as usual operations through formalised reviews during the lifecycle.
IT transformation not delivered in full Our programme of IT transformation may not be delivered in full due to the level of complexity of replacing legacy IT and simultaneously implementing new integrated service model	This could result in systems and infrastructure that are not fit for purpose, may add costs and lead to business interruption.	Risk profile is unchanged	• Developed and monitoring the implementation of our Strategy and Integrated Service model. • Programme teams and operational business teams work closely to ensure that the objectives of the strategy are delivered. • Transformation assurance and oversight plan in place.
Industrial action Continued progress has been made in industrial relations, however the withdrawal of support from our staff or postmasters to the ongoing implementation of Post Office strategy via industrial action remains a risk.	This could result in business disruption leading to loss of revenue, reduced customer satisfaction and brand damage.	Risk profile is unchanged	• Well defined agreements with relevant unions. • Comprehensive engagement programme in place with staff, unions and postmasters so as to ensure that there is alignment with our vision and strategy around transformation. • Contingency planning in place to minimise the impact of potential industrial action.
OPERATIONAL RISKS			
Lack of appropriate capability The Post Office is dependent on its dedicated work force to meet the expectations of its customers and stakeholders. The ability to continue to attract, motivate, develop and retain people is key to its success.	This could result in not achieving our strategic objectives and loss of staff engagement.	Risk profile is unchanged	• Continue to review our organisational structure to ensure it evolves and supports our requirements. • Operate a capability heatmap to identify key capabilities for our current and future state needs. • Continued investment in developing our people.
Decline in customer experience If we are unable to deliver an attractive customer experience, via our products, service and channels, we risk losing the support of our customers.	This could result in reduced customer satisfaction and brand reputation, with consequential loss of market share and revenues.	Increasing customer expectations and competitive pressures in the market mean the risk profile is increasing	• Our customer strategy is continually monitored to ensure that it meets changing customer product and service expectations and reflects current market and competitor trends. • Our channel strategy ensures we meet the changing customer requirements for access and utilises available and emerging technology to reflect changing customer needs.
Unattractive network proposition	As well as loss of revenue, this	Risk profile is unchanged	

POL00423565

As we transform, there is a risk that the Post Office may not be able to retain, or attract sufficient new, retail partners because of the complexity of our network proposition and lack of profitability for a retail partner.	could result in shrinkage to our network and breach our public purpose commitment.		• Branch level proposition designed to provide appropriate profitability for our retail partners. • New branch model also ensures that we use modern technology to drive efficiency and cost reduction for operators, as well as a better customer experience. • Branch model continually reviewed and updated to ensure we support our retail partners and are attractive to new ones.
Business interruption and cyber threat Post Office is dependent on the continued availability of its information systems and associated infrastructure. These could be threatened, either due to internal issues, external events or cyber attack.	This could result in disruption of service leading to negative customer experience, breach of contractual obligations and brand damage.	Risk profile is unchanged	• Business continuity plans are updated through review, testing and enhancements. • New contracts have provisions covering the security, resilience and availability of our IT systems and infrastructure. • Robust policies are in place to cover information security, with continuous improvements where required. • Rigorous schedule covering penetration testing to assess and improve the security of our systems.
Dependency on third parties Post Office works in partnership with a number of third parties to deliver high quality services. These depend upon us successfully selecting, contracting and monitoring our key in-source or out-source relationships and avoiding any unintentional breaches of contractual terms.	This could lead to business interruption and additional costs through failure to meet contractual obligations.	Post Office actions to deliver separation from Royal Mail and revised partnership structures means risk profile is decreasing	• Contract management framework to monitor our contracts and suppliers. • Assessment of risks and ensure monitoring of mitigating actions. • Defined key policies that we require our suppliers to comply with and attest to compliance.

FINANCIAL RISKS			
Stakeholder funding The cost of delivering the public purpose of the Post Office and meet the expectations of stakeholders may exceed current forecasts.	This could result in not achieving our growth objectives, failing to meet our public purpose commitment and damaging our reputation with stakeholders.	Risk profile is unchanged	• Proactive engagement with stakeholders to ensure there is full understanding of, and alignment with, the strategic goals and the investment case required to deliver them. • Annual and three-year operating and capital plans developed and risk assessed. • Scheduled feedback to stakeholders and review.
Financial reporting and controls failure Our financial controls are fundamental to delivering our fiduciary responsibilities, management information, financial reporting and compliance with accounting and	This could result in loss of revenue, increased costs, financial misstatement and damage to	Increased regulatory requirements across the markets in which the Post Office operates	• Defined and structured delegation of authority which is reviewed and approved by the Board. • A Financial and Accounting manual and a framework of supporting general controls – see Our Control Framework on page SSS. • Documented financial controls, with additional assurance to be provided

POL00423565

governance standards. These may not operate effectively if they are not documented, reviewed and monitored regularly.	reputation with stakeholders.	mean the risk profile is increasing	from a Control Self-Assessment process.
Pension cost increases The cost of servicing the current Defined Benefits scheme could become unbearably onerous as a result of the prolonged low interest rate environment, resulting in substantially increased contributions.	This could result in material increases in required contributions, adversely affecting our ability to achieve commercial sustainability.	Economic conditions relating to the cost of servicing schemes means the risk profile is increasing	• Valuation assumptions and pension funding strategy have regular external and internal monitoring and review. • Working with professional advisors to develop options to minimise the impact of an adverse valuation. • Consultation process is currently underway on options for the future of the Defined Benefit plan. • Alternative de-risking plans can be investigated if required.
LEGAL & REGULATORY RISKS			
Financial regulatory breach	This could result in regulatory censure, fines, litigation or curtailment of trading, which could damage our reputation with customers and suppliers.	Increasing regulatory requirements across the industries in which the Post Office operates means the risk profile is increasing	• Corporate services works closely with the relevant business owners to identify new regulatory obligations. • On-going training to our staff on legal and regulatory matters. • Regular compliance tests and monitoring are conducted. • Programme in place of internal and external assurance (including by our regulatory principals) including in relation to our financial services business, its sales practices and products to ensure that on an ongoing basis these continue to meet regulatory requirements.

POL00423565

5) Policy Approval

Author: Mark Rodgers Sponsor: Mike Morley-Fletcher Meeting date: 05 May 2016

Executive Summary

Context

Policies are a fundamental part of our General Control Framework. We use them to articulate our intent, setting clear rules and expectations, to communicate how we want to standardise and monitor specific activities and behaviours. They also enable us to evidence our intentions to third parties, for instance business partners, suppliers and regulators. We have a Policy Framework to ensure 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.

On a regular basis we review the framework of policies and Policy owners review the content to ensure both are up to date and relevant for our needs. The proposed Framework for our most important policies is included in paper 4b) appendix 3, Key Policy Framework, and review work has been progressing on theses polices. At this stage seven key policies are presented for RCC approval (five from CS and one from IT and one from HR) and subsequent presentation to the ARC.

RCC is asked to review these policies, invited to provide feedback and comments, with the intention of ratifying these seven key policies submitted for approval. Once approved the policies will need to be implemented by the policy Owner, including monitoring of performance and compliance.

Questions?

a) Can RCC ratify the seven policies we have developed or revised?
b) How will we manage subsequent implementation of the policies?
c) What lessons have we learnt so far?

Conclusion

a) Seven policies have been reviewed and where necessary revised. They have been signed off by policy Owner and are ready for approval by RCC and ARC. A summary of the policies is attached (see appendix 1) along with the policy documents (see appendix 3 - 9).
b) Once approved policies will need to be implemented. This will involve deciding where they should be stored, how they should be communicated and supported with training, how they should be controlled, monitored and reviewed. This is the primary responsibility of the policy Owner, but will be supported and monitored by the central Policy Manager. Further details of what this requires is provided in appendix 2, Policy Implementation Process.
c) In addition, we are identifying lessons learnt from our review of phase 1 polices and these will be used to assist policy Owners during phase 2.

Input Sought

RCC is asked to review this paper and invited to provide feedback and comments. In particular to:
a) Ratify the seven key policies submitted for approval, and
b) Consider the requirements for implementation.

Appendices

Appendix 1: Policy Approval – Summary of policies and rationale
Appendix 2: Policy Implementation Process
Appendix 3 - 9: Policy Approval – Copies of documents

POL00423565

Appendix 1: Policy Approval – Summary of policies (7) and rationale

Ref	Key Framework Policy	Sponsor (GE Owner)	Policy Owner	Why is this policy needed?	Approved by?	How will the policy be implemented?	How will policy compliance be monitored?
12) (PBA)	Financial Crime	Jane MacLeod	John Scott	To help Post Office meet legal and regulatory obligations within appetite, and to manage financial crime risks reducing actual loss, avoiding potential losses.	RCC and ARC May 2016	Proposal for process to implement policies, including: • where they should be stored • how they should be communicated and supported with training • how they should be controlled, monitored and reviewed. Please refer to appendix 2 for more details.	1. Policy Compliance Manager will coordinate, and ensure QA standards, including compliance monitoring. 2. Policy Owner undertakes compliance, and will identify measures, develop monitoring processes, track results and provide reporting with MI to the relevant governance body.
13) (PBA)	Anti-Bribery and Corruption (incl. Gifts & Hospitality)	Jane MacLeod	Ben Foat	To help Post Office meet its legal and regulatory obligations within appetite, to help manage ABC risks, and support good conduct standards in all dealings.	RCC and ARC May 2016		
14) (PBA)	Anti-Money Laundering (incl. Counter Terrorism, Sanctions)	Jane MacLeod	John Scott	To help Post Office meet its legal and regulatory obligations within appetite, and to help manage AML (CTF and Sanctions) risks whilst reducing actual loss, and avoiding potential losses.	RCC and ARC May 2016		
17) (PBA)	Business Continuity	Jane MacLeod	Jonathan Waples	To embed a framework to identify potential threats to business continuity, and to help manage impacts to business operations. It is a set of standards which support resilience and sets out the capabilities to respond.	RCC and ARC May 2016		
25) (PBA)	IT Disaster Recovery	Alisdair Cameron	Stephen Hayes	To embed a framework to identify potential threats to disaster recovery, and to help manage impacts to IT/ business operations. It is a set of standards which support resilience and sets out the capabilities to respond.	RCC and ARC May 2016		
26) (PBA)	Talent and Resourcing: HR Vetting	Neil Hayward	Sean Leahy	To ensure Post Office operates vetting processes in a legal, and compliant way. To embed standards to control and reduce the risks of error, theft, fraud or misuse of facilities. To ensure Post Office engages with suitable workers.	RCC and ARC May 2016		

5)	Whistleblowing	Jane MacLeod	Nisha Marwaha	To help Post Office meet its legal and regulatory internal and external obligations. To implement good practice and engender good standards in this context.	RCC and ARC May 2016	As above	As above

POL00423565

Appendix 2: Policy Implementation Process

These are the steps we identified for planning and monitoring implementation of policies. They will be trialled with CS polices before being recommended to other business areas. An estimated timeline of 6 months has been used.

Implementation Steps	Details	Example timeline (estimated at 6 months)
1) Establish accessible storage and maintenance protocols	❑ Publish documents to SharePoint ❑ Update Intranet and links (checking searches) ❑ Define maintenance	By 31/05/16
2) Communicate policy and requirements	❑ Agree audience (for communication and training) ❑ Develop communications policy and messages ❑ Communicate policy and requirements	By 30/06/16
3) Develop and deliver supporting training	❑ Identify resources and compile modules/ materials (Learning Academy) ❑ Coordinate and deliver training ❑ Publish to SharePoint	Develop by 31/07/16, deliver by 31/08/16
4) Identify and develop associated controls	❑ Confirm associated controls framework and catalogue controls library ❑ Create matrix of responsibilities (include RACI if required) ❑ Confirm controls operating as expected	Identify by 30/06/16, develop by 31/08/16
5) Monitor and measure compliance	❑ Identify and define compliance monitoring procedures, systems and controls ❑ Identify measures and test monitoring plans ❑ Commence monitoring routines ❑ Capture results, evaluate, define management information and report to governance committees	By 30/10/16
6) Review policy	❑ Use monitoring results to evaluate current policy controls and continuing appropriateness of policy ❑ Maintain policy review log ❑ Conduct annual/ bi annual policy reviews and report to relevant governance body	By 31/12/16

POL00423565

Appendix 3 - 9: Policy Approval – Copies of documents (7)

These policies have been reviewed and signed off by policy Owners. Six have been provided to the Banking partners and Whistleblowing has been updated. They are presented to the RCC/ ARC for approval.

POL00423565

Post Office Financial Crime Policy

POL00423565

Contents Page

Contents Page 2
Document Control Sheet 3
Section A. Introduction 4
Section B. Context 5
About this Policy 5
What is financial crime? 5
Risk Appetite 6
How we manage financial crime 6
Who is responsible 7
Who must comply and how 7
Section C. Policy Details 8
Information 8
Our Controls 8
Section D. Governance 10
How do we monitor compliance 10
How to raise a concern 10
Contact us and more information 10
Section E Key Terms and References 11
Key Terms 11

POL00423565

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 V0.6	Annually from policy effective date	19th May 2016	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

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)	5 May 2016
Board Committee	Post Office Audit, Risk and Compliance Committee (ARC)	19 May 2016

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.	No later than 19th May 2017

POL00423565

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 is directly related to this code ensuring 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 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 management of financial crime to the Board of Directors. Post Office's Audit, Risk and Compliance Committee considers financial crime as a standing agenda item and the Post Office Board is updated on a regular and timely basis.

POL00423565

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.

Failure to comply with the requirements of this policy by any person 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 refers to permanent staff, temporary including agency staff, contractors and consultants.

Financial crime risks are reviewed with relevant individuals on a regular basis and at least quarterly. This policy's effective date is 19th May 2016.

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.

POL00423565

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:

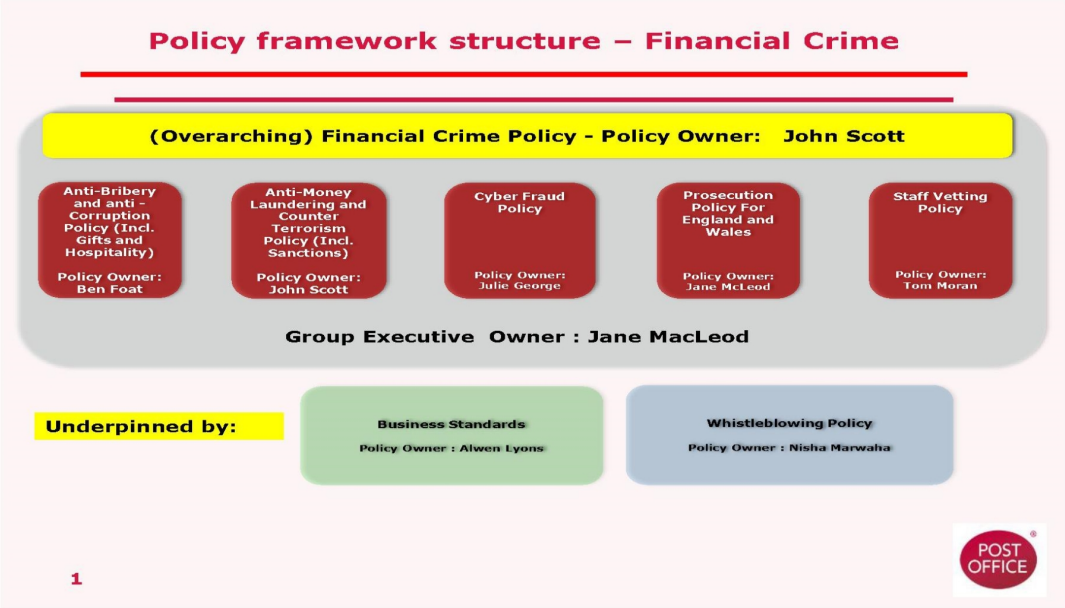
- Any dishonest or fraudulent act,
- Profiteering as a result of insider knowledge of Post Office activities,
- Theft of assets from Post Office or its customers,
- Manipulation of transactional data at Point of Sale,
- False expense or payroll claims,
- Manipulation of Post Office accounts or financial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

Risk Appetite

Post Office has an averse appetite for regulatory and legal risks. This policy reflects this and sets out controls to reduce and/ or mitigate financial crime risks.

How we manage financial crime

This policy is one of Post Offices key policies forming a broad suite of Financial Crime 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. .



POL00423565

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 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 Security and Financial Crime (MLRO) is the policy Owner, who is responsible for the day to day implementation of and compliance with this policy, and is accountable to the General Counsel, and
- The Senior Security Manager, Financial Crime is the policy Implementor who is responsible for the day to day implementation of the policy lifecycle (including monitoring) and is responsible for and accountable to the policy Owner for reporting all policy matters.

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 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 Head of Security and Financial Crime (MLRO).

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.

POL00423565

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
- 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

- All 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 mitigating controls aligned to the inherent risk must be put in place.
- The head of each Business Unit must confirm annually that a formal risk assessment has been undertaken and that adequate controls are in place in accordance with Post Office's central Risk Management Framework.
- Business Units must consider both internal and external risks and past experience (including any litigation), 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 the Head of Security and Financial Crime.

POL00423565

- Each Business Unit must have processes in place for managing and reporting both internal and external financial crime incidents. These processes must be in line with the Post Office's central risk team's reporting requirements.
- 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 will take all reasonable measures to prevent, deter and detect all 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 all third parties, 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. Details of losses and the cause of the loss will be reported regularly to the Post Office ARC by the General Counsel.

POL00423565

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. In addition, Internal Audit will periodically test compliance with 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 Board 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 suspects dishonest or fraudulent activity 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 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 GRO

POL00423565

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: 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

POL00423565

Post Office Anti-Bribery and Anti-Corruption Policy

(Incorporating: Gifts & Hospitality Policy)

POL00423565

Contents Page

Contents Page 2
Document Control Sheet 3
Section A. Introduction 4
Section B. Context 5
About this Policy 5
What is Bribery and Corruption? 5
Risk Appetite 6
How we organise ABC risk management 6
Who is responsible 7
Who must comply and how 7
Section C. Policy Details 9
Information 9
Our Controls 11
Section D. Governance 14
How do we monitor compliance 14
How to raise a concern 14
Contact us and more information 14
Section E. Key Terms and References 15
Key Terms 15
References 15
Appendix 1 – Post Office Gifts & Hospitality Policy 17
Approvals Procedure 17

POL00423565

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:**
Final V1.5	Annually from policy effective date	19th May 2016	Z:\NEW COMPLIANCE\New Policy Framework 2015\Refreshed Policies 2016

DOCUMENT REVISION HISTORY			
Version	**Date**	**Author**	**Reason For Change**
Draft v1.4	30th March 16	**Jane MacLeod**	Sponsor review and sign – off
Final v1.5	30th March 16	**Ben Foat**	Policy Owner final review and sign off

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)	5 May 2016
Board Committee	Post Office Audit, Risk and Compliance Committee (ARC)	19 May 2016

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.	No later than 19th May 2017

POL00423565

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 is directly related to this code ensuring the highest standards of ethics 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 on a regular basis.

POL00423565

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 on a regular basis and at least at quarterly 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.

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; and
- 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 the appendices, assist Post Office in preventing and detecting corrupt conduct and form an essential component of Post Office's adequate procedures.

POL00423565

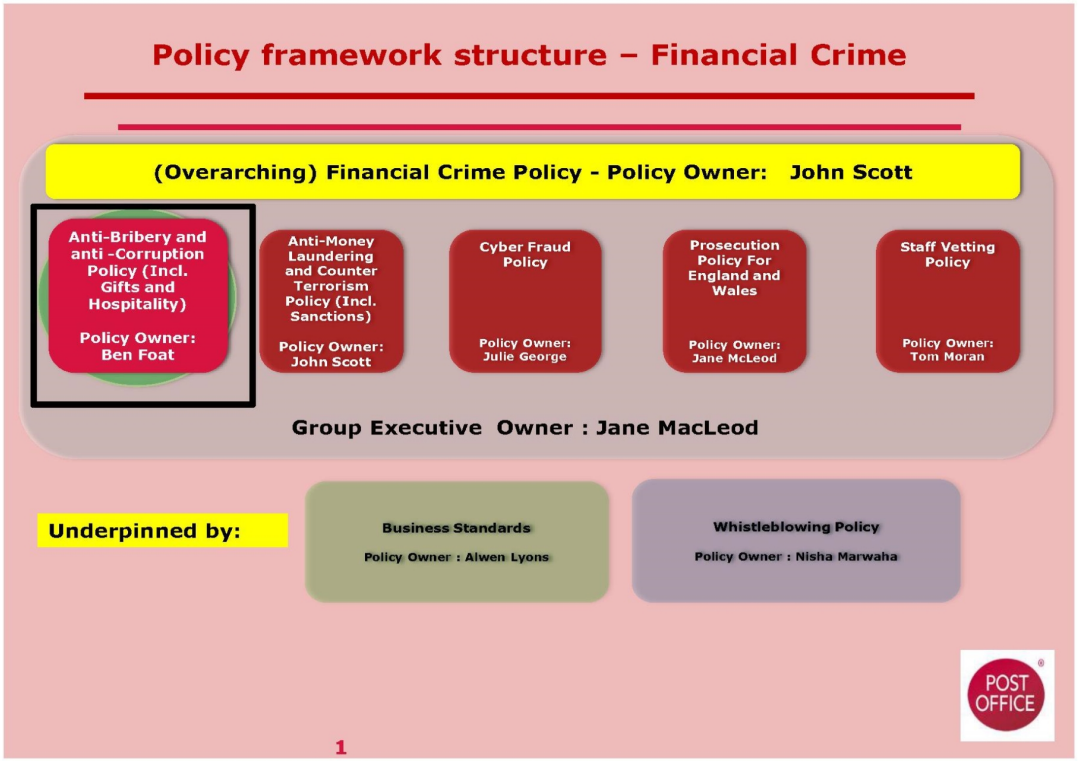
Post Office Ltd must also comply with particular regulatory obligations arising through contracts with directly regulated companies or directly through its subsidiary, Post Office Management Services (POMS). As an Appointed Representative of each of the Bank of Ireland and POMS, Post Office Ltd is contractually 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 this regulatory obligation.

Risk Appetite

The Post Office risk appetite is averse for not complying with law and regulations or deviation from its business conduct standards. Post Office is therefore intolerant of bribery and corruption risks (i.e. Post Office has zero tolerance). 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)

POL00423565

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; and
- 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; and
- 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.

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.

POL00423565

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 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.

POL00423565

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.
- 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; and
- Associated Parties, which include persons or entities that perform services for or on behalf of Post Office.

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; and
- Charitable Donations.

POL00423565

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

The specific types of ABC risks can be classified as:

Payment Risks – arising from, for example, charitable or political donations, facilitation payments, gift and entertainment, client training programs and ex gratia/ legal settlements. Payment risks include:

- 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 Entertainment (G&E): As these are part of corporate life, it is important that such G&E 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&E Policy annexed to this Policy;
- 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;
- Client training programs: 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&E, the training provided should not be excessive or lavish. Records of any training should be kept by the relevant business areas;
- 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. There must be no perceived inducement for the purpose of improperly obtaining or retaining business or securing an advantage for Post Office; and
- Ex gratia payments/ legal settlement: an ex gratia payment or a legal settlement is the usual 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.

POL00423565

Third Party/ Associated Party Risks – arising from third parties who provide services on behalf of Post Office and engage in bribery and corruption while performing those services. The scope of this would include, for example, agency operators within the Post Office network as well as suppliers who are procured through the Procurement Team. Examples of Associated Parties include agents, consultants, suppliers, introducers, and intermediaries. Before engaging with an Associated Party, the business area and employee should:

- Undertake a risk assessment and due diligence on the proposed Associated Party to determine the ABC risk profile of the Associated Party; and

- When undertaking the ABC risk assessment and due diligence consider whether there are any red flags or heightened risks arising from that assessment.

Employment Risks – arising from Post Office employees breaching ABC legal and regulatory requirements by requesting something of value from a third party in exchange for providing employment or a work opportunity at Post Office or providing work opportunities, paid or unpaid, to Connected Individuals (see Section E for definition of this term) with the purpose of improperly obtaining or retaining business or securing an advantage for Post Office.

Post Office employs a merit based approach in its hiring of staff. 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. 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.

Our Controls

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.

POL00423565

Business areas systems and controls

All business areas must ensure that they have in place adequate systems and controls to comply with this policy and manage bribery and corruption risks including:

Specific ABC Controls	Description
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 the following specific issues are incorporated into the design, management and implementation of its ABC processes and procedures: • Payment Risks – arising from, for example, charitable or political donations, facilitation payments, gifts & entertainment, and client training. • 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 would include agency operators within the Post Office network and suppliers procured through the business or through the Procurement Team. • Employment Risks – arising from Post Office employees breaching ABC legal and regulatory requirements by 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.
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: • Payment Risks – as set out in Section C and including the Gifts and Entertainment process which is set out in Appendix 1 of this Policy. • 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. In addition, each business area must identify, escalate and resolve any heightened risks arising from the ABC risk assessment and due diligence. Examples of these heightened risks include: o Remuneration which is not proportionate with the services being rendered or consistent with the market or relevant industry.

POL00423565

	○ 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. • Each business area is required to ensure that the relevant mandatory ABC contract clauses are included in the agreement with that party. Please liaise with Legal and Procurement Departments to ensure that all contracts include the appropriate ABC clauses. • Employment Risks – such assessment should include, for example, identifying employment and work opportunity risk, identifying relevant connections, managing candidates for employment with relevant connections, managing employee disclosure of relevant connections, identify and managing a risk based and proportionate PEP screening, bonus and compensation structures are based on objective and merit-based grounds and do not incentivise an employee to improperly exploit their relevant connections, and managing requests for work opportunities from external stakeholders.[1]
Incident reporting, response and recording	Each business area 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 in all cases escalated to the Central 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.
Risk Indicators	Each business area is to escalate existing and new bribery and corruption risks to the head of that area who shall, in turn, inform the Central Risk team. The Central Risk team determines the risk indicators and MI required.
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.
Audit	Each business area should test the effectiveness of its processes to ensure that the Post Office is able to monitor the application and effectiveness of this Policy and its controls.

POL00423565

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. In addition, Internal Audit will periodically test compliance with 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 Board 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

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** Ben Foat Head of Legal – Financial Services on GRO or by email at GRO

POL00423565

Section E. Key Terms and References

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
Whistleblowing 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 can contact Post Office's General Counsel, Jane MacLeod who can be contacted by email on: GRO or by telephone on: GRO 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.
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

POL00423565

	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.

POL00423565

Appendix 1 – Post Office Gifts & Hospitality Policy

Approvals Procedure

Gifts

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, such as when giving or receiving a gift from an overseas postal administration in an official capacity as a representative of Post Office, 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 GRO
- 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

Register of Gifts

The Central Risk team maintains a Register of all Gifts given and received over £20.

Hospitality - Purpose

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.

Hospitality – Practice and Register of Hospitality

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

POL00423565

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.

Hospitality – Awareness and Reporting

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.

POL00423565

Post Office Anti-Money Laundering and Counter Terrorist Financing Policy

POL00423565

Contents Page

Contents Page 2
Document Control Sheet 3
Section A. Introduction 4
Section B. Context 5
About this Policy 5
What is AML and CTF? 5
Risk Appetite 6
How we organise AML/CTF management 6
Who is responsible 6
Who must comply and how 7
Section C. Policy Details 8
Information 8
Our Controls 9
Section D. Governance 14
How do we monitor compliance 14
How to raise a concern 14
Contact us and more information 14
Section E Key Terms and References 15
Key Terms 15

POL00423565

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 V2.8	Annual (from effective date	19th May 2016	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

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)**	5th May 2016
Board Committee	**Post Office Audit, Risk and Compliance Committee (ARC)**	19th May 2016

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.	No later than 19th May 2017

POL00423565

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 is directly related to this code ensuring the highest standards of fraud prevention, detection and management are maintained.

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 and Risk Committee considers AML and CTF matters as a standing agenda item and the Post Office Board is updated on a regular basis.

POL00423565

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 and it is a set of standards to minimise the likelihood of regulatory breach. This policy is effective from 19th May 2016.

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.

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

POL00423565

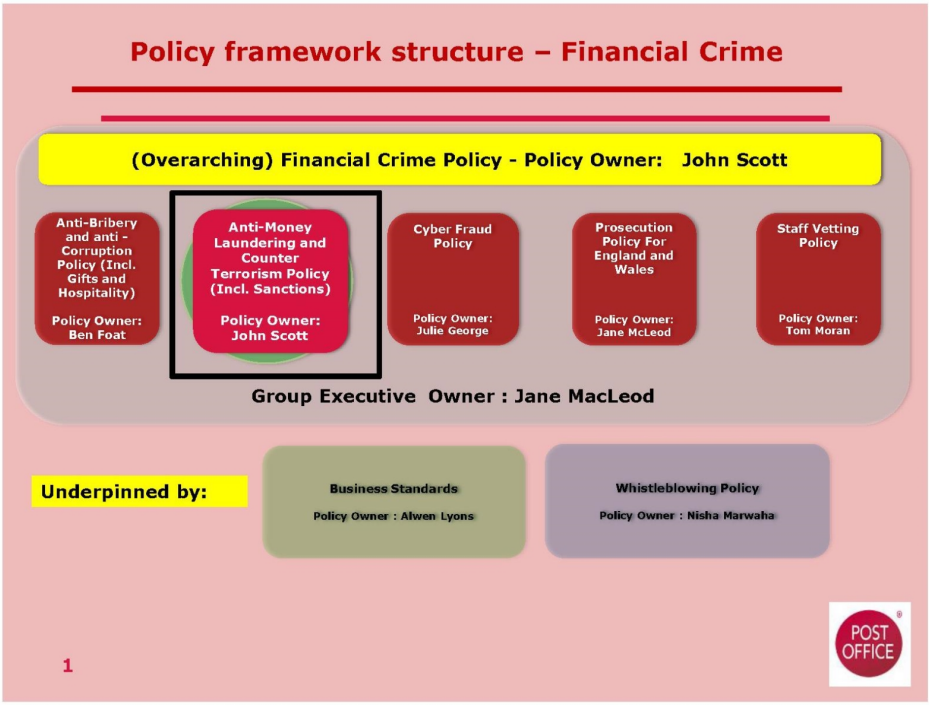
suspicious activity, provide appropriate AML/CTF training for relevant individuals, and maintain adequate transaction records.

Risk Appetite

Post Office has an averse appetite for regulatory and legal risks. This policy reflects this and sets out controls to reduce and/or mitigate AML/CTF 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 Financial Crime through reports to its committees – principally to the Board Audit, Risk & Compliance Committee ('ARC'). The key individuals and their specific responsibilities in relation to this policy are:

POL00423565

- The General Counsel who is a member of the Post Office Executive is the policy Executive Owner and policy Sponsor, accountable to the CEO and to the Post Office Board overall,
- The Head of Security and Financial Crime (MLRO) is the policy Owner who is responsible for the day to day implementation of and compliance with this policy and reports to the General Counsel, and
- The Senior Security Manager, Financial Crime is the policy Implementor who is responsible for and accountable to the policy Owner for the day to day implementation of the policy lifecycle (including monitoring).

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 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 Policy Owner, the Head of Security and Financial Crime.

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.

POL00423565

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.

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 unless he has in place procedures for:

- Obtaining satisfactory evidence that the client is the person he claims to be,
- Keeping records of the identity of those clients and the transactions carried out by them for a least five years,
- Training staff on the firm's preventative procedures and about spotting money laundering; and
- The reporting of suspicions of money laundering and designating a Nominated Officer to whom internal reports may be made.

Failure to put such procedures in place 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.

POL00423565

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,
- Screening all direct customers of Post Office and their transactions for potential financial sanctions breaches, and
- Monitoring regulated transactions and periodically 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 at all times a relevant policy supported by appropriate procedures 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 paragraph and 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

POL00423565

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 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
  - Identity and source of wealth information will be obtained and verified for any PEPs
  - Post Office will record and validate the business relationship with the customer to be on-boarded including:

POL00423565

- The nature and details of the business
- The source and origin of funds
- The relationship with an ultimate beneficial owner (UBO)
- 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** - Money Laundering Regulations dictate that Post Office monitors all PEP relationships 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

POL00423565

- **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 and is are able to delay it for seven working days without arousing the suspicion of the customer

- **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

  Records relating to customers with whom a business relationship exists should be retained for 5 years after the business relationship ceased.

  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

POL00423565

- **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.

POL00423565

Section D. 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. In addition, Internal Audit will periodically test compliance with 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.

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 GRO

POL00423565

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)

POL00423565

Post Office

Business Continuity Management Policy

POL00423565

Contents Page

Contents Page 2
Document Control Sheet 3
Section A. Introduction 4
Section B. Context 5
About this Policy 5
What is Business Continuity? 5
Risk Appetite 5
How we organise Business Continuity Management 5
Who is responsible 7
Who must comply and how 7
Section C. Policy Details 8
Information 8
Our controls and arrangements 8
1. Baseline and on-going Business Continuity objectives 8
2. Satisfying BCMP Requirements 9
3. Approach to Managing Risk & Audit Requirements 10
4. Continual Service Improvement 11
Section D. Governance 12
How we monitor compliance 12
How to raise a concern 12
Contact us and more information 12
Section E. Key Terms and References 13
Key Terms 13
References 13

POL00423565

Document Control Sheet

POLICY SUMMARY			
GE Policy Sponsor	Policy Owner	Policy Implementor	Policy Approver(s)
General Counsel **Jane MacLeod**	Business Continuity Manager **Jonathan Waples**	Business Continuity Manager **Jonathan Waples**	Post Office **RCC and ARC Committees**
Version and Status:	Policy Review Period	Effective from :	Policy location:
Final - V0.7	Annually from policy effective date	19th May 2016	Z:\NEW COMPLIANCE\New Policy Framework 2015\Refreshed Policies 2016

DOCUMENT REVISION HISTORY			
Version	**Date**	**Author**	**Reason For Change**
Draft v0.6	21/03/2016	**Mike Morley-Fletcher**	Head of Risk sign – off /readiness Review
Final v0.7	30/03/2016	**Jane MacLeod**	Final review, sponsor sign off

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)**	5 May 2016
Board Committee	**Post Office Audit, Risk and Compliance Committee (ARC)**	19 May 2016

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.	No later than 19th May 2017

POL00423565

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 is directly related to this code ensuring the highest standards of business continuity 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 Business Continuity Manager, 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 business continuity management framework to the Board of Directors. Post Office's Audit, Risk and Compliance Committee considers business continuity as a standing agenda item and the Board is updated on a regular and timely basis.

POL00423565

Section B. Context

About this Policy

The purpose of this document is to define Post Office's policy with regard to business continuity management that is appropriate to the aims and objectives of Post Office. This includes:

- A framework for:
  - setting business continuity objectives;
  - satisfying appropriate requirements;
  - continual improvement of the Business Continuity Management Programme; and
- A high level statement of our key controls in respect of business continuity.

The Policy is consistent with business continuity "ISO22301", which are the Business Continuity Institute's Good Practice Guidelines.

Policy Scope: It is important to understand which areas of the business currently fall under the protection of the policy, and which do not. The boundaries of the Post Office business continuity framework are detailed within a separate document, "Business Continuity Context, Requirements and Scope", and these documents should be reviewed together when assessing a BC response requirement.

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

What is Business Continuity?

Post Office adopts the Business Continuity Institute's Good Practice Guidelines definition of business continuity as: *"A holistic management process that identifies potential threats to an organisation, and the impacts to business operation those threats, if realised, might cause, and provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities."*

Risk Appetite

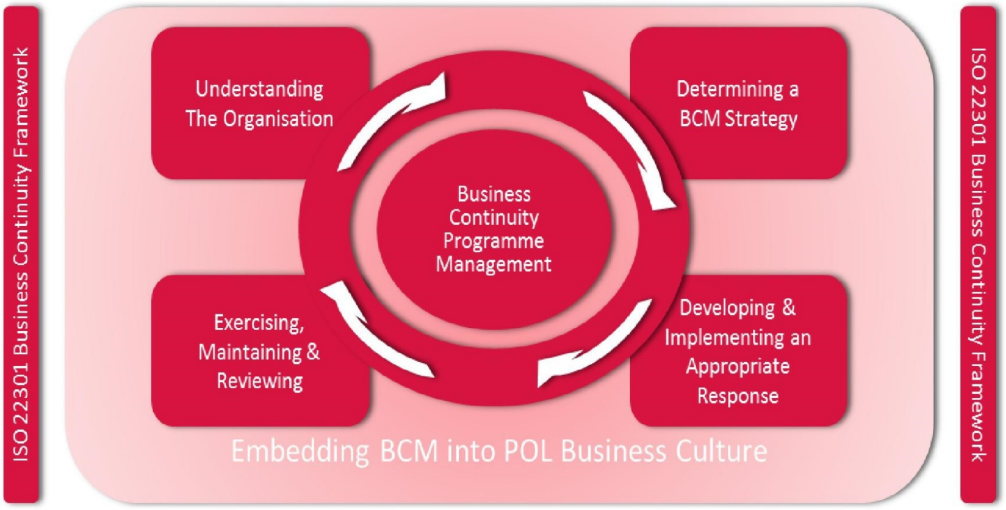
Post Office has an averse appetite for business continuity risk. Post Office recognises that it cannot completely eliminate this risk. However, this policy sets out controls to reduce and/ or mitigate such risks.

How we organise Business Continuity Management

This policy describes Post Office's Business Continuity Management policy and should be read in conjunction with other Post Office resilience, health & safety, and physical security related policies and procedures.

POL00423565

The BCM Framework



This Business Continuity Management Policy is stored electronically, and is available to all relevant stakeholders within the organisation.

POL00423565

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 business continuity by reports from its committees including its ARC Committee. The key individuals and their specific responsibilities in relation to this policy are:

- The General Counsel is a member of the Post Office Executive team and is the Group Executive Owner and policy Sponsor, accountable to the Board.
- The Group Business Continuity Manager is the Policy Owner who is responsible for the day to day implementation of and compliance with this policy and is accountable in this regard 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. 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 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 Investigations Policy. If the cause is found to be due to wilful disregard or negligence, it will be treated as a disciplinary offence.

POL00423565

Section C. Policy Details

Information

Post Office recognises the need to ensure that our business operates safely, smoothly and without interruption for the benefit of our colleagues, customers, shareholders and other stakeholders.

To ensure such levels of safe, continuous operation, Post Office has implemented a Business Continuity Framework consistent with "ISO 22301".

The operation of a Business Continuity Framework has many benefits for Post Office, including:

- The safe-guarding of colleagues at times of duress;
- Ensuring the supply of goods and services to our customer; Protection of revenue streams and business profitability;
- Maintenance and enhancement of shareholder / stakeholder value; and
- Compliance with legal and regulatory requirements.

In addition, our Business Continuity Framework is a commitment to the development, maintenance, improvement and socialisation of a Business Continuity Management Programme within and across the organisation.

Our controls and arrangements

1. Baseline and on-going Business Continuity objectives

The baseline objectives for business continuity within Post Office are defined within the "Business Continuity Context, Requirements and Scope" document. These are fundamental steps required which are led by business areas and are not subject to frequent change.

These baseline objectives guide the setting of lower level detail for short-term objectives for business continuity planning arrangements within an annual cycle. They coincide with the organisational budget planning. This ensures that adequate funding is obtained for necessary activities identified in the previous cycle.

These business continuity objectives will be documented in the Business Continuity Management Plan ("BCM Plan"), produced each financial year, which will also identify how objectives will be achieved, over what estimated period, and at what level of estimated cost. Once the annual BCM Plan is approved by the Post Office Risk and Compliance Committee it will be subject to regular management review to ensure that its objectives remain valid.

Amendments to objectives will be managed through the standard Post Office change management process.

POL00423565

2. Satisfying BCMP Requirements

Senior Managers commit to the provision of the appropriate resources to establish and develop the Business Continuity Management Programme ("BCMP").

Systematic performance review of the programme. This is conducted by the Business Continuity Manager on a regular basis, ensuring that quality objectives are being met. Qualitative evaluation is undertaken and any issues identified through the audit programme and management processes. Management review includes departmental and other management meetings.

Business Continuity Management Quality System. The Business Continuity Manager has overall authority and responsibility for this and implements and manages the system carrying out the following:

- The identification, documentation and fulfilment of applicable requirements;
- Assigning authorities and responsibilities for the implementation, management and improvement of the BCMP;
- Integration of business processes with the BCMP;
- Compliance with statutory, regulatory and contractual requirements in the management of assets used to deliver products and services; and
- Reporting to senior management on performance and improvement of the BCMP

Role definition and responsibilities are reviewed by the Business Continuity Manager to ensure that colleagues understand the roles they are required to fulfil, and that they have the appropriate skills and competences to do so. These controls are necessary to ensure the continued BCMP success and to mitigate risk.

Post Office will ensure that colleagues involved with the BCMP are competent on the basis of appropriate education, training, skills and experience. The skills are required to ensure business continuity will be determined and reviewed on a regular basis, together with an assessment of existing skill levels within Post Office. Training needs will be identified and executed via individual's training plans maintained to ensure that competences are in place.

Full details of the business continuity responsibilities associated with each of the required roles, and how they are associated within Post Office are given in a separate document, "Roles, Responsibilities and Authorities".

Use of third parties. Post Office uses third parties, both internal and external, in the delivery of products and services. Where this involves the operation of a business process, or part of such process, that falls within the scope of the BCMP, then this should be identified by the Business Continuity Manager within the annual Business Continuity Management Plan.

Post Office retains governance of the relevant business continuity management processes for third parties by demonstrating:

- Accountability for the process;

POL00423565

- Control of the definition of, and interface to, the process;
- Performance and compliance monitoring; and
- Control over process improvements.

This will be evidenced by documentation and records, including contracts, meeting minutes and performance reports.

Third party agreement contractual business continuity terms. Specific, high level, requirements for new and existing relationships will be made available to associated third parties by the relevant third party relationship manager. These requirements set out minimum expectations for service continuity provision (as appropriate to the contractual service level terms). For further information see "Supplier Business Continuity Evaluation Process".

3. Approach to Managing Risk & Audit Requirements

The risk management strategy defined under ISO 22301 requires that relevant assets are identified and the following considerations made:

- Threats;
- Vulnerabilities;
- Impact & likelihood before risk treatment;
- Risk treatment (e.g. reduction, removal, transfer);
- Function responsible/ owner; and
- Timescale and review frequency.

Risk management will occur at multiple levels within the BCMP, including but not restricted to:

- Business continuity management planning – risks to the achievement of objectives;
- Business Continuity risk assessment;
- Assessment of the risk of changes under the established business change model; and
- At the project level as part of the management of significant business change.

High level risk assessments will be reviewed annually, or upon significant change to the business environment. More detail on the approach to risk assessment can be found in the document "Risk Assessment Process".

Regular reviews must take place concerning how well business continuity management processes and procedures are being observed. These occur at two levels:

- Structured regular management review of conformity to policies & procedures within Post Office; and
- Internal audit reviews against the ISO 22301 standard by the Post Office Internal Audit Team.

POL00423565

Certification auditing. Additionally, should certification to ISO 22301 be sought and attained, a third audit level applies:

- External audit against the standard in order to gain and maintain certification to ISO 22301.

Details on the process for internal audits can be found in the document "Procedure for Business Continuity Audits".

4. Continual Service Improvement

The approach to continual improvement of the BCMP is to:

- Consider effectiveness across all business areas and end to end systems, processes within scope;
- Enhance current processes to bring them in to line with best practice (as defined within ISO 22301);
- increase the level of proactivity (and the business perception of proactivity) with regard to the on-going management of business continuity;
- Achieve an enhanced understanding of and relationship with the business units to which the BCMP applies;
- Review relevant metrics on an annual basis to assess their appropriateness, or to make changes to them based on collected historical data and feedback;
- Obtain ideas for improvement via regular review meetings with stakeholders, documenting them in the "Procedure for Continual Improvement"; and
- Review the "Procedure for Continual Improvement" document at regular management meetings in order to prioritise and assess timescales and benefits.

Ideas for improvement may be obtained from any source, including but not restricted to: Customers; Suppliers; Colleagues; Risk Assessments & Audits.

In order to evaluate any proposed improvements to the BCMP, the following criteria would be applied:

- Cost;
- Business benefit;
- Risk;
- Implementation timescale; and
- Resource requirement.

Accepted improvement proposals will be prioritised, and planned according to standard project management principals. Additional information on continual improvement methodology can be found in "Procedure for Continual Improvement".

POL00423565

Section D. Governance

How we monitor compliance

The Business Continuity Manager will ensure that this policy is implemented, reviewed and remains effective. Post Office's internal systems of business continuity risk control ensure that controls are regularly independently assessed for effectiveness, suitability and adequacy. In addition, Internal Audit will periodically test compliance with this policy.

Review and assessment of compliance with this policy is done on a timely basis and regular gap analysis is undertaken by the Business Continuity Manager and reported to the Risk and Compliance Committee.

Business continuity testing is planned and pre-determined. See further information in the "Business Continuity Exercising and Testing Schedule". Post Office's capability to maintain business operation will be subjected to exercise, and the results of these exercises will also be made available to the Risk and Compliance Committee.

We require third parties who do business with Post Office to have at least equivalent arrangements, systems and controls to this policy, and these should be demonstrable on request.

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 Jon Waples – Business Continuity Manager on GRO or by email at GRO

POL00423565

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 (POMS)
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
ISO 22301	The International Standard for Societal Security (Business Continuity).

References

References	Description
Business Continuity Context, Requirements and Scope	The purpose of this document is to describe the way the business operates, internal and external factors influencing it and to highlight in general terms the potential consequences of a business interruption. This will allow the most appropriate level of measures to be put in place to reduce the level of risk and to ensure that plans are available and tested to manage the impact of any interruptions that do occur.
Roles, Responsibilities and Authorities	The purpose of this document is to set out the organisation structure in terms of job roles, management and numbers of resources in each area and then to define how responsibility for each of the processes within the Business Continuity Management System (BCMS) is allocated within that structure.
Supplier Business Continuity Evaluation Process	This document sets out a process for the evaluation of the business continuity arrangements of our suppliers so that a degree of confidence may be gained that

POL00423565

	they possess sufficient resilience to support our requirements.
Risk Assessment Process	It is important that Post Office has an effective risk assessment process in place to ensure that potential impacts do not become real, or if they do, that contingencies are in place to deal with them. The starting point for risk assessment is the list of key business activities documented in the most recent business impact analysis.
Procedure for Business Continuity Audits	The purpose of this document is to set out how the Business Continuity Management Quality system will be audited internally.
Continual Improvement Action Log	Management of BCMP improvements can become unwieldy if they are spread across multiple reports, action plans and meeting minutes. The idea of this spreadsheet is to act as a focal point to record, assess and track all such improvement items in a common manner.
Procedure for Continual Improvement	In general Post Office will use the Plan-Do-Check-Act method (the Deming Cycle) for managing improvements as defined in the ISO 22301 standard
Business Continuity Exercising and Testing Schedule	The purpose of this document is to set out a schedule for testing / exercising activities.
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: 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

POL00423565

Post Office IT Disaster Recovery Policy

POL00423565

Contents Page

Contents Page 2
Document Control Sheet 3
Section A. Introduction 4
Section B. Context 5
About this Policy 5
What is IT Disaster Recovery? 5
Risk Appetite 5
How we organise IT Disaster Recovery 6
Who is responsible 6
Who must comply and how 6
Section C. Policy Details 8
Information 8
Our policy aims, controls and arrangements 8
Section D. Governance 11
..... 11
How do we monitor compliance 11
How to raise a concern 11
Contact us and more information 11
Section E. Key Terms and References 12
Key Terms 12
References 12

POL00423565

Document Control Sheet

POLICY SUMMARY			
GE Policy Sponsor	**Policy Owner**	**Policy Implementor**	**Policy Approver(s)**
Chief Financial Officer **Alisdair Cameron**	Head of IT Service Management **Stephen Hayes**	Head of IT Service Management **Stephen Hayes**	Post Office **RCC and ARC Committees**
Version and Status:	**Policy Review Period**	**Effective from :**	**Policy location:**
Final V6.0	Annually from policy effective date	19th May 2016	Z:\NEW COMPLIANCE\New Policy Framework 2015\Refreshed Policies 2016

DOCUMENT REVISION HISTORY			
Version	**Date**	**Author**	**Reason For Change**
Draft V5.0	31st March 2016	**SH/GB**	Policy Owner review & QA
Final V6.0	19th April 2016	**Stephen Hayes/Alisdair cameron**	Owners final review and sign-off

POLICY APPROVAL		
Role/Forum	**Name**	**Date**
Executive Owner and Sponsor	Chief Financial Officer (Alisdair Cameron)	15 April 2016
Executive Committee	Post Office Risk and Compliance Committee (RCC)	5 May 2016
Board Committee	Post Office Audit, Risk and Compliance Committee (ARC)	19 May 2016

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.	No later than 19th May 2017

POL00423565

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 is directly related to this code ensuring the highest standards of disaster recovery management are maintained.

This policy sets out what is and what is not acceptable but if you have any doubts or questions, these should be referred in the first instance to the Head of IT Service Management who oversees compliance with this policy. It is essential that you read this policy.

Introduction by the Group Executive Policy Owner: Chief Financial Officer

As Post Office's Chief Financial Officer and the Group Executive Policy Owner and Sponsor, I have overall accountability for IT Disaster Recovery to the Board of Directors. Post Office's Audit, Risk and Compliance Committee ("ARC") considers IT Disaster Recovery risks as an agenda item and the Board is updated on a regular basis.

POL00423565

Section B. Context

About this Policy

The purpose of this document is to define Post Office's policy with regard to IT disaster recovery and to demonstrate that it is appropriate for the aims and objectives of Post Office. This includes a framework as follows:

- The documentation of specific policy statements;
- A methodology for recording compliance with the IT Service Continuity policy;
- Management processes and procedures managed by the Post Office Service Integrator under their Service Integration Service Desk (SISD) agreement;
- Reporting the tests conducted within each IT supplier's Business Continuity Plan; and
- The recording of the Post Office IT eco-system resilience and disaster recovery tests that have been completed, the risks identified and service improvements to be implemented to the various service provider deliverables within their agreements.

The policy complies with the relevant provisions of the following standards ISO/ IEC17799:200, BS15000.

This policy sets out what we must all do to ensure Post Office complies with its IT disaster recovery obligations in its client and partner contracts and that Post Office follows a robust process to ensure the IT eco-system supplier's resilience and fail over solutions are regularly tested to ensure Post Office service continuity is maintained. This policy's effective date is 19th May 2016.

What is IT Disaster Recovery?

The Post Office IT disaster recovery policy sets out a mechanism whereby specific IT eco-system supplier processes, procedures and controls are effectively followed and test outputs measured with service improvements qualified to mitigate any risks identified during testing.

On the condition that the policy and processes are rigorously applied and measured, Post Office will have an effective audit trail of documentation and will have a high degree of confidence that the IT eco-system suppliers have the correct level of resilience within their IT architectural solutions to deliver high quality products and services as defined in their contractual obligations to Post Office.

Risk Appetite

Post Office has an adverse risk appetite for IT disaster recovery risk. Post Office recognises that whilst it cannot completely eliminate this risk, this policy sets out controls to reduce and/ or mitigate such risks.

POL00423565

How we organise IT Disaster Recovery

The Post Office IT Service Integrator provides an IT Service Continuity Management service within the IT service delivery model, based on a Service Integration and Management (SIAM) framework and works as a Managing Agent for the IT incumbent providers. Post Office procures these services through its SISD agreement with the Post Office IT Service Integrator.

For each IT supplier within the eco-system that has business continuity/ disaster recovery obligations within their direct contracts with Post Office, the Post Office IT Service Integrator will manage these supplier obligations on Post Office's behalf within the provision of the ITIL IT Service Continuity Management service.

The IT Service Continuity Management service is detailed within the following separate documentation; SIAM ITSCM Policy.v1b, SIAM ITSCM Process.v1a, POL-17645-HLD001-3.5 Operations_Manual_IT_Service_Continuity_Mgmt.v1c. These documents are pending Post Office final approval.

Who is responsible

Post Office's Board of Directors have overall responsibility for ensuring that Post Office has a framework to ensure compliance by (i) Post Office with its contractual obligations, and by (ii) 3rd party suppliers with Post Office's IT Disaster recovery obligations as set out in the relevant contractual agreements. The Board is kept abreast of relevant matters relating to the management of IT Disaster Recovery by reports from its committees, including the Audit, Risk and Compliance Committee. The key individuals and their specific responsibilities in relation to this policy are:

- The Chief Financial Officer, who is a member of the Post Office Group Executive team, is the policy Executive Owner and policy Sponsor, accountable to the Post Office Board overall;
- The Head of IT Service Management is the policy Owner, who is responsible for the day to day implementation of and compliance with this policy; and
- The Head of IT Service Management is also the policy Implementer, who is responsible for and accountable for the day to day implementation of the policy (including monitoring and reporting).

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.

POL00423565

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 Policy Owner.

If non-compliance is identified the matter must be referred to the Head of IT Service Management for investigation. 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.

POL00423565

Section C. Policy Details

Information

Post Office recognises the need to ensure that our business operates safely, smoothly and without interruption for the benefit of our colleagues, customers, shareholders and other stakeholders. To ensure such levels of safe, continuous operation, Post Office has implemented a Business Continuity Framework consistent with "ISO 22301".

The operation of a Business Continuity Framework has many benefits for Post Office, including:

- The safe-guarding of colleagues at times of duress;
- Ensuring the supply of goods and services to our customers;
- Protection of revenue streams and business profitability;
- Maintenance and enhancement of shareholder/ stakeholder value; and
- Compliance with legal and regulatory requirements.

Post Office is committed to the development, maintenance, improvement and socialisation of a Business Continuity Management Programme within and across the organisation.

As part of the Post Office Business Continuity Framework, this IT Disaster Recovery policy outlines the IT approach to delivering continuity of services under a Disaster Recovery event within the Post Office.

Our policy aims, controls and arrangements

Aims of the policy

- Maintain an acceptable level of service during a service invocation;
- Ensure plans and alternative service options are in place to meet the organisation's needs in the event of a significant business outage or disruption;
- Support Business Continuity Management ensuring the appropriate communication and management plans are in place and available to support business critical needs;
- Reduce the likelihood of a disruption occurring through the identification and mitigation of risks;
- Ensure each IT eco-system supplier will have processes and plans supporting the delivery of their contracted services. End to end delivery must underpin the recovery of business systems based on the business needs; and
- Comply with relevant provisions of ISO / IEC17799:200, BS15000 (as amended) and all other industry standards in force.

POL00423565

Analyse the IT Landscape, define responsibilities and prepare plans

- Analyse threats and estimate the probability of having an effect on Business Service Continuity;
- Maintain an overall business criticality matrix of services using the baselines provided by Supply Chain and Customer;
- Detect and report the most vulnerable points of infrastructure;
- Ensure all continuity team members have an in depth knowledge of the IT infrastructure and of the items involved in providing each IT service that underpins business services;
- Identify areas of the IT service model where there are constraints and to define the process to manage and mitigate the risk;
- Identify the responsibilities of all parties in the event of an invocation;
- Detail in recovery plans all necessary information required by the customer in order to invoke a successful continuity plan and maintain service;
- Ensure that any plans designed by the key stakeholders are within the authority matrix.
- Establish processes to plan for, respond to and recover from, disruptive events.

Develop and Test and Report on the Recovery Procedures

- Develop and maintain the recovery procedures for specific business services delivered through the IT eco-system supplier network.
- Test and improve recovery procedures, working with IT eco-system supplier.
- Ensure each IT eco-system supplier has processes and plans supporting the delivery of their contracted services.
- Validate a working continuity programme by evidencing that recovery plans are in place and that they are being tested in line with the requirements set out in the contract.
- Receive all IT eco-system supplier written reports following their Continuity testing.
- Provide written reports within agreed timescales following Continuity Exercises to the key stakeholders within the authority matrix.

Manage invocations

- Inform key stakeholders within the authority matrix of any invocation of IT Continuity plans.
- Provide for the restoration and ongoing performance of the services following disaster, or a failure in or disruption to services.
- Conduct a post supply chain disaster review following any invocation of IT service continuity, business continuity or supply chain members disaster Recovery plans to understand the cause of the supply chain disaster and plan for the restoration of the IT Services to the pre- supply chain disaster state and implement actions to eliminate or mitigate future occurrences.

POL00423565

Continuous improvement

- Continually review all IT eco-system supplier continuity plans where applicable, to ensure they meet continue to meet the business requirements and amend where appropriate through the contractual process.

Co-ordination of the IT Disaster Recovery plan with the Business Continuity Plan

- Ensure a business continuity plan is made and includes the planning for non-IT related aspects such as key personnel, facilities, crisis, communication and reputation protection, and that it refers to the IT Service Continuity Plan for IT related infrastructure recovery/ continuity.

POL00423565

Section D. Governance

How do we monitor compliance

The Head of IT Service Management will ensure that this policy is implemented, reviewed and remains effective. Post Office internal systems of risk control ensure that disaster recovery controls in this policy are regularly independently assessed for effectiveness, suitability and adequacy. In addition, Internal Audit will periodically test compliance with this policy.

We assess compliance with this policy on a regular basis and regular Disaster Recovery reports will be issued by Head of IT Service Management to the IT Supplier and Service Committee.

We require our subsidiaries and third parties to have at least equivalent arrangements, systems and controls to this policy, and these should be demonstrable on request.

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 **Stephen Hayes, Head of Service Management** GRO **or by email** GRO

POL00423565

Section E. Key Terms and References

Key Terms

Term or Acronym	Description

References

References	Description
1. Post Office Group	Post Office Limited and all subsidiaries and entities within the Post Office Group which includes Post Office Management Services (POMS).
2. 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: GRO or by telephone on: GRO 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

POL00423565

Post Office

Pre-Employment Vetting Requirements

POL00423565

Contents

Contents 2
Document Control Sheet 3
Section A. Introduction 4
Section B. Context 5
About this Policy 5
What is pre-employment vetting? 5
Risk Appetite 5
How we manage pre-employment vetting 6
Who is responsible 6
Who must comply 6
Section C. Policy Details 8
How you comply 8
Our Records 8
Section D. Governance 9
How do we monitor compliance 9
How to raise a concern 9
Contact us and more information 9
Section E. Key Terms and References 10
Key Terms 10
References 10
Appendix. Further Guidance on how vetting will be conducted 11
Proof of Qualifications 13
Money Laundering Regulations (MLR) 14

POL00423565

Document Control Sheet

SUMMARY			
GE Policy Sponsor	**Policy Owner**	**Policy Implementor**	**Policy Approver**
Group People Director **Neil Hayward**	Head of Human Resources **Sean Leahy**	Head of Human Resources **Sean Leahy/Andrew Lewis**	Post Office **RCC and ARC Committees**
Version and Policy Status:	**Document Review Period**	**Policy – effective date :**	**Policy location:**
Draft V5.0	Annually from policy effective date	19th May 2016	Z:\NEW COMPLIANCE\New Policy Framework 2015\Refreshed Policies 2016

REVISION HISTORY			
Version	**Date**	**Author**	**Reason For Change**
Draft v4.1	18th April 2016	**Jane MacLeod**	Legal Team Final Review
Draft v5.0	21st April 2016	**Andrew Lewis/Sean Leahy**	Policy Owner final review
Draft v5.0	25th April 2016	**Neil Hayward**	Policy Sponsor sign-off

POLICY APPROVAL		
Role/Forum	**Name**	**Date**
Executive Owner and Sponsor	Group People Director (Neil Hayward)	30th April 2016
Executive Committee	Post Office Risk and Compliance Committee (RCC)	5th May 2016
Board Committee	Post Office Audit, Risk and Compliance Committee (ARC)	19th May 2016

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.	No later than 19th May 2017

POL00423565

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 is directly related to this code ensuring the highest standards of employment vetting 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 who oversees compliance with this policy. It is essential that you read this policy.

Introduction by the Group Executive Policy Owner: Group People Director

As Post Office's Group People Director and the Executive Policy Owner I have overall accountability for vetting to the Post Office's Board of Directors. Post Office's Audit, Risk and Compliance Committee considers HR (see section E for the definition of "HR") legal and compliance risks as a standing agenda item and the Post Office Board is updated on a regular basis.

POL00423565

Section B. Context

About this Policy

This policy supersedes and replaces all previous policies relating to employment vetting for and on behalf of Post Office.

The purpose of this policy is to set out a framework for the employment vetting of all roles within Post Office, and within contract partners offering products and services as any part of Post Office Group, which meet our legal, regulatory and contractual obligations and therefore reduces risks of human error, theft, fraud and/ or misuse of facilities. This policy is effective from 19th May 2016.

What is pre-employment vetting?

Vetting is the process of performing a background check on someone before offering them employment or conferring a contract of work.

This policy addresses and minimises any potential security risks that are posed as a result of recruiting new employees as well as those recruited as a result of redeployment of employees into roles with different vetting requirements. The policy also applies to contract partners offering products and services under any part of Post Office Group branding, such as Sub-Postmasters and their employees (Referred to as Partners in this policy). Successful deployment will reduce and minimise security risks to the business, our customers, our Partners and employees.

This policy re-iterates the terms set out in Condition 8 of the January 2006 postal operators' licence; Protecting the Integrity of the Mail, which specifies the vetting standards that Post Office is obliged to meet under the Mails Integrity Code of Practice (2006). This policy meets Post Office regulatory obligations of Ofcom, the Financial Conduct Authority (FCA) and Security Industry Authority (SIA); which encompass all recruitment - employees, agents and assistants. Failure to adhere to this vetting policy may put trading licences at risk and, as a result, Post Office Groups ability to operate in key business markets (including but not limited to; postal services and financial services) could be withdrawn or fines applied.

This policy ensures all legal (Right to Work) documents are collected and verified as required in accordance with Post Office's duty to prevent illegal working. Other requirements addressed by this policy include the need to adhere to the legal, regulatory and contractual requirements for certain roles, such as obtaining relevant security clearance or evidencing required qualifications.

Risk Appetite

Post Office has an averse risk appetite for regulatory and legal risks. This policy reflects this and sets out controls to reduce and/ or mitigate risks associated with offering employment or conferring contracts for work.

POL00423565

How we manage pre-employment vetting

Post Office HR Service Centre commences pre-employment vetting process once all relevant documentation has been received; vetting must be completed prior to a prospective employee's or Partner's start date. A contract will only be issued once the vetting process is complete.

Exceptional Circumstances:
In exceptional circumstances (for example, to deal with industrial action, Christmas pressure outside of planned engagement of Christmas casuals or an outbreak of a serious contagious disease) different and possibly reduced levels of vetting may be applied. However only with the prior authorisation of, and to the specific requirements determined by and agreed with the Head of Human Resources for the business area the candidates will be joining.

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 vetting by reports from its committees including its ARC Committee. The key individuals and their specific responsibilities in relation to this policy are:

- The Group People Director is a member of the Post Office Executive team, and is Group Executive policy owner and policy Sponsor, accountable to the Post Office Board;
- The Policy Owner, the Head of Human Resources, is responsible for the day to day implementation of and compliance with this policy, and is accountable to the Group People Director; and
- The Policy Implementor is responsible for the day to day implementation of the policy lifecycle (including monitoring) and is responsible for and accountable to the policy Owner for reporting all policy matters.

Who must comply

Compliance with this policy is mandatory. This policy will apply to the recruitment approval process for all Post Office employees, officers, contractors, casual workers, and Partners. 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 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

POL00423565

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 HR Vetting 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 Investigations Policy. If the cause is found to be due to wilful disregard or negligence, it will be treated as a disciplinary offence.

POL00423565

Section C. Policy Details

How you comply

It is the policy of the Post Office that all applicants agree to undergo a pre-employment vetting process. The nature of this process will include verifying eligibility to work in the United Kingdom or Northern Ireland, and electronic searches of information already available in the public domain. Such information may include the following: sanction lists, criminal records, lists of politically exposed persons, FCA Register Search, embargo lists, Companies Office records, etc.

All successful applicants based in the United Kingdom and Northern Ireland will be subject to a basic financial check (sometimes referred to as Credit and Voters Checks). This will provide us with information including data from the electoral register to verify date of birth, where appropriate publicly available data to reveal any adverse information, including County Court Judgments, Bankruptcies, Voluntary Arrangements etc.

Pre-employment vetting guidelines may be updated to reflect current best practice and/ or required legislation or other Post Office change of policy.

It is the policy of Post Office that all non-payroll contractors complete pre-employment vetting prior to gaining access to systems and work locations. For details of non-payroll contractor pre-employment vetting requirements contact the HR Service Centre.

HR Service Centre will commence the pre-employment vetting process once all the relevant documentation has been received; the vetting must be completed prior to the employees start date. A contract will be issued once the vetting process is complete.

Our Records

This policy document must be maintained and be available for review at all times. The policy will be kept in the resourcing section of the HR, Advice and Guidance intranet site. Other policy related records created as a result of vetting activity must be kept in accordance with Post Office retention of records policy and must comply with legal and regulatory record keeping requirements.

In all cases, records must be maintained to show:

- that the verification process was properly carried out and all documentation retained in the personal file including the pre-employment checklist (except for where data protection rules prohibit the retention of the data); and
- the candidate's personal file and all documentation therein must be retained throughout the period of employment and for 7 years post-employment.

POL00423565

Section D. Governance

How do we monitor compliance

The Head of Human Resources will ensure that this policy is implemented and reviewed, vetting controls in this policy are regularly independently assessed for effectiveness, suitability and adequacy. In addition, Internal Audit will periodically test compliance with this policy.

HR assess compliance with this policy on a regular basis and reports will be issued by the Group People Director to Post Office's RCC and to the Board ARC Committee.

We require third parties who do business with Post Office 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, contact the policy Owner, the Head of Resourcing Manager.

POL00423565

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 (POMS) and FRES
Executive Policy Owner	As defined by the Post Office Policy Framework-Roles and responsibilities Matrix document V0.5
FCA	Financial Conduct Authority
HR	Post Office Human Resources team
Partner	Any contract partner or their employees who offer products or services under the branding of Post Office Group or its subsidiaries. Such as Agents, Sub-Postmasters and their Assistants.
Policy Owner	As defined by the Post Office Policy Framework-Roles and responsibilities Matrix document V0.5
SIA	Security Industry Authority

References

References	Description
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: 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

POL00423565

Appendix. Further Guidance on how vetting will be conducted

Application Form Declaration: Each candidate must complete an application form either online or hard copy. The application form must be signed or the candidate must declare online that the information is correct.

A copy of the application form must be kept. This can either be stored securely within the recruitment system or in the candidate's personal file.

Criminal Convictions Declarations: The candidate must declare any unspent criminal convictions, impending prosecutions and cautions. Also any military Martials must be declared.

Proof of Identity: All candidates are required to produce one document which has photographic proof of the person's identity. (Refer to Document Checklist for Candidates at Appendix2).

Proof of Right to Work in the UK: The candidate's Right to Work documents are checked against the Home Office guidelines to ensure that these documents constitute a valid Right to Work (see Appendix 2).

Proof of Address: All candidates are required to provide documentary evidence of their address/place of residence (refer to Document Checklist for Candidates Appendix 2)

Proof of National Insurance Number: A check must be made to ensure the number is in the format of an official National Insurance (NI) number i.e. 2 Letters, 6 numbers and a single letter

In addition to the official NI number card and official notification of the NI number from the Inland Revenue, P60's and payslips may be used. These documents must not be handwritten.

Health Consent Form: For Post Office employees this consent is required should an offer of employment be made. The employee will be asked further screening questions against a matrix provided by the POL Employee Health Service (EHS) providers ATOS Origin. Where further medical advice is required, candidates are referred to ATOS Origin.

Personal Declaration to Post Office Ltd. (P13 form): In part this goes toward satisfying the condition of the operating licence issued to Post Office Ltd.

The P13 form should be read, signed and dated by all candidates at the document checking part of the interview process and by agency staff or contractors at the registration session.

The candidate's signature should be witnessed, countersigned and dated by an appointed Post Office Ltd Representative, (this can be the hiring manager or a member of the HR team).

POL00423565

The P13 form must be retained within the candidate's personal file and a copy supplied to the candidate

The requirements are specific to roles which are deemed "Fit and Proper" (F&P) and in line with the FCA.

Fitness and Propriety Form: The Fitness and Propriety (F&P) declaration form will be sent to successful candidates for completion by the Recruitment Team.

It is a mandatory element that all successful candidates (internal and external) for the roles within scope fully complete a F&P declaration form and answer **all** questions **honestly**. For the avoidance of doubt, honesty at all times when completing the F&P form is a crucial factor in considering whether a successful candidate is deemed to be "Fit and Proper."

Post Office can request that the F&P declaration form to be completed by employees within scope on an on-going basis and those members of staff that change their role into a role that fall within the F&P scope.

Directorship Search: The Directorship Search requires the successful candidate to answer specific questions, which are: - have they **ever** been a director, secretary or LLP of a company (Yes or No) or **ever** been disqualified from acting as a director (Yes or No)

If the successful candidate answers yes to either or both questions they must list the company name, country of registration, company number, dates of position held, country in which disqualified, reason for disqualification and dates when disqualified.

A search will be carried out irrespective of yes or no answers directly with Companies House to verify what the successful candidate has stated on the consent form.

FCA Register Search: The FCA Register Search requires the successful candidate to answer specific questions which are; - Are you currently or have you **ever** previously been approved by the FCA to carry out a controlled function (Yes or No). If yes, then the candidate will need to supply their individual reference number (if known)

Irrespective of the answers, a search will be run directly with the FCA to verify what the successful candidate has stated on the consent form. In the case of employees, this search will be conducted by Post Office Ltd.

In the case of agency staff/contractors, this search will be conducted by the relevant supplier.

The relevant supplier will verify all information and report on any discrepancies indicating the risk of severity of the discrepancy

Globex Criminality Database Search (By Exception): The Global Criminality Database Search will only be undertaken **by exception** in circumstances when amber/red flag issues have arisen primarily within the Directorship search area.

POL00423565

A "global" database search may be run, using the candidates name and previous names to identify any crime or information relating to,

- Bribery
- Corruption
- Counterfeiting
- Falsifying information on official documents
- Fraud
- Embezzlement
- Theft
- Tax evasion
- Money laundering
- Insider trading and market manipulation
- Currency counterfeiting
- Securities fraud

Proof of Qualifications

Where appropriate for the role, proof of valid and up to date qualifications must be obtained.

Specific roles and Supply Chain staff: Valid Driving License (where relevant to the role). A check is required to ensure that the candidate has a valid and acceptable driving licence suitable for the role.

- If the individual is required to drive a vehicle above 3.5t then they will need to have a C1 on their licence. For drivers who passed their test before January 1997 they should have this as an acquired right, for any drivers who passed their test after this date then they would not have this as a part of passing their car test, and are required to undertake an additional driving test to drive rigid vehicles above 3.5t.
- In the case of agency staff/contractors, the relevant supplier will be made aware by Post Office as to which type of licence is required.

SIA Licence Check: Where a candidate has an SIA licence the licence number must be checked against the Home Office register.

POL00423565

References (5, 6 or 10 years)

- The candidate is required to give consent for references to be requested by completing the Multi Consent Form or equivalent for agency staff and contractors.
- This consent allows Post Office and approved agencies to apply to the following in order to gather reference information prior to employment;
    - Previous employers;
    - Accountants;
    - Education establishments
    - DWP and HMRC
    - The consent also gives Post Office permission to disclose any reference information with auditors from a third party.
- Where the role is a regulated role such Financial Services Area Manager or Mortgage Specialist or the candidate is required to complete a F&P declaration, written confirmation shall be sought from all the former employers, educational establishments, etc., listed by the applicant that the dates given are accurate and that there is nothing in their experience of the applicant which suggests a lack of integrity or otherwise adversely reflects upon his/her suitability for the employment in question.
- Confirmation of periods of registered unemployment must be sought from the Employment service or other government agencies.
- Employment cannot be offered until all relevant information has been received.
- Where any lack of integrity is indicated and a clear decision not to employ cannot be made, any decision of employment must be referred to the Head of Resourcing in Post Office.

Money Laundering Regulations (MLR)

Successful candidates will be required to make an application to HM Revenue and Customs for a "fit and proper test" in line with the Money Laundering Regulations 2007.

Once the application is completed it will be sent by the HR Service Centre (HRSC) Recruitment Team to the Vetting Team who will then process the application.

POL00423565

Conflicts of Interest Form: In accordance with section 175 of the UK Companies Act 2006, it is the duty of a director of a company who is in any way, directly or indirectly, interested in a contract or proposed contract with the company to declare the nature of his interest at a meeting of the directors of the company.

A director has a duty to make a section 175 declaration at each board meeting if appropriate, and a questionnaire on conflicts of interests will be circulated to Directors on appointment. If any conflicts are disclosed in the questionnaire they should be discussed with the Company Secretary.

A Conflicts of Interest Form will be presented to the successful candidate to complete.

Companies House Application: In accordance with Section 167 of the Companies Act 2006, the successful candidate must be registered with Companies House. The application will be the responsibility of the Company Secretary via the on line an APO1 form.

More information on appointments of Directors and the requirement to register can be found at www.gov.uk/government/publications/appoint-a-director-ap01

POL00423565

Post Office Whistleblowing Policy

POL00423565

Contents Page

Contents Page 2
Document Control Sheet 3
Section A. Introduction 4
Section B. Context 5
About this Policy 5
What is Whistleblowing 5
Section C. Policy details 7
How to raise a concern 7
Whistleblowing Officer and 'Speak Up' details 7
Confidentiality and anonymous reporting 7
Investigating concerns 8
Outcomes and Reports 9
External Disclosures 9
Protecting the Whistleblower 10
Contact us 10
Who is responsible for this policy 11
How we monitor compliance 11
Section D. Key Terms and References 12
Key Terms 12
References 12

POL00423565

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 **RCC and ARC Committees**
Version and Policy Status:	Policy Review Period	Effective from:	Policy location:
Final V1.4	Annual Review (from Effective date)	19th May 2016	Z:\NEW COMPLIANCE\New Policy Framework 2015\Refreshed Policies 2016

REVISION HISTORY			
Version	**Date**	**Author**	**Reason For Change**
Draft v1.3	18/04/16	**Nisha Marwaha**	Policy Owner review
Final v1.4	27/04/16	**Jane MacLeod**	Sponsors review and sign-off

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)	5 May 2016
Board Committee	Post Office Audit, Risk and Compliance Committee (ARC)	19 May 2016

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.	No later than 19th May 2017

POL00423565

Section A. Introduction

Chief Executive's Note

Post Office is committed to conducting business with the highest standards of honesty, integrity and openness in order to create a workplace where workers feel able to raise concerns. A culture of openness and accountability is essential in order to prevent illegal, improper or unethical conduct and an effective Whistleblowing Policy helps us to identify and address situations when they occur.

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 Whistleblowing obligations. Post Office's Audit, Risk and Compliance Committee ("ARC") considers Whistleblowing as an agenda item and the Post Office Board is updated on a regular basis.

POL00423565

Section B. Context

About this Policy

The purpose of this policy is to encourage the reporting of suspected wrongdoing and/or dangerous practices, (see section entitled What is Whistleblowing below), within Post Office, to make it easier for management to address those concerns and therefore avoid serious accidents, fraud, regulatory breaches, financial impropriety and/or reputational damage.

The aims are:

(1) to encourage staff to report matters as soon as possible in the knowledge that their concerns will be taken seriously and investigated, and that confidentiality will be respected,
(2) to provide staff with guidance as to how to raise those concerns, and
(3) to reassure staff that they should be able to raise concerns without fear of reprisals, even if they turn out to be mistaken.

This policy enables Post Office to comply with its Whistleblowing obligations under applicable legislation and to be in line with regulatory requirements. This Policy is effective as at 19th May 2016.

What is Whistleblowing

"Whistleblowing" refers to the act of exposing wrongdoing and/or dangerous practices by reporting it either internally within an organisation, or externally, for example to a regulator. The law on Whistleblowing is contained in the Employment Rights Act 1996 as amended by the Public Interest Disclosure Act 1998. Wrongdoing includes criminal activity, civil offences (including negligence, breach of contract, breach of administrative law), miscarriages of justice, dangers to health and safety or to the environment and the cover up of any of these.

Workers should raise a concern if they are aware of, or suspect, wrongdoing which affects others (e.g. customers, members of the public, colleagues or the Post Office). Some examples (this is a non-exhaustive list) of situations where a worker may raise a concern are:

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

POL00423565

A Whistleblower is a person who raises a genuine concern relating to any wrongdoing including any of the above. If a worker has any genuine concerns related to suspected wrongdoing, they should report it under this Policy.

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

POL00423565

Section C. Policy details

How to raise a concern

In the first instance, workers should raise concerns with their line manager, or a senior HR manager in Post Office. Alternatively workers can notify the Whistleblowing Officer directly, using the contact details provided in this Policy.

It is recognised that sometimes raising a concern directly with the business may not be possible, for example, if the worker considers that the line managers may be involved in the issue or if they have a concern about confidentiality.

In such instances workers should contact the **"Speak Up"** confidential reporting service which is run by InTouch MCS Ltd, an independent company (see section below entitled Whistleblowing Officer and Speak Up details for more information).

InTouch will treat concerns in complete confidence and the worker does not have to provide contact details. **Post Office treats all concerns raised under this Policy very seriously.**

Whistleblowing Officer and 'Speak Up'

The Whistleblowing Officer for the Post Office Group is Post Office's General Counsel, currently Jane MacLeod who can be contacted by telephone on: GRO or by email on: GRO

The Speak Up service is available on GRO or via a secure on-line web portal http://www.intouchfeedback.com/postoffice.

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

Confidentiality and anonymous reporting

Post Office hopes that workers will feel able to voice Whistleblowing concerns openly under this Policy. However, if a worker wants to raise a concern confidentially, Post Office will make every effort to keep their identity secret. If it is necessary for anyone investigating a concern to know the worker's identity, the investigator will discuss it with that individual.

When reports are made anonymously via Speak Up, there is no requirement to provide contact details. However, not providing details may reduce Post Office's ability to undertake a thorough investigation into the concerns raised.

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

POL00423565

Investigating concerns

All concerns (including those raised via Speak Up) will be passed to the Whistleblowing Officer who will carry out an initial assessment of the issue to determine the scope of any investigation.

The Whistleblowing Officer will decide whether an investigation is appropriate and what form the investigation should take. The type of investigation will depend on the nature of the concern and may be:

- investigated internally (or the Whistleblowing Officer may decide to appoint an external investigator if there are good reasons),
- resolved by agreed action as determined by the Whistleblowing Officer without the need for investigation,
- referred to the police, and
- referred to a regulatory authority.

If an investigation is appropriate, the Whistleblowing Officer will appoint an investigator. The appointed investigator should be an individual at an appropriate level for the matter under investigation and they must not have any conflict of interest with the individuals or issues concerned.

In some cases an investigator or team of investigators may be appointed including staff with relevant experience of investigations or specialist knowledge of the subject matter.

The Whistleblowing Officer may determine that the matter should be investigated under the terms of other more appropriate Post Office Group policies, such as those covering grievance or bullying and harassment matters, in which case the process described in the applicable policy will apply. The Whistleblowing Officer can also decide to take no action if the complaint appears to be without a reasonable basis.

During an investigation under the Whistleblowing Policy, the investigator may wish to contact the worker directly to request additional information. Where the worker's identity is known, this will be done only where the worker has consented to a representative from Post Office speaking to them directly. Where the worker's identity is anonymous, questions or requests for information can be raised anonymously either through the Speak Up service, or via secure voicemail or messaging on the web portal.

Subject to concerns about confidentiality, the worker may be required to attend meetings to provide further information. Workers can bring a colleague or union representative to any meetings under this Policy. The companion must respect the confidentiality of the worker and any subsequent investigation.

POL00423565

Investigators should consider the principles set out in Post Office's internal Investigations Policy and adhere to those wherever possible when undertaking the investigation.

Outcomes and Reports

The investigator should aim to keep the Whistleblower informed of the progress of the investigation and its likely timescale.

The investigator must write a report containing the findings of the investigation, including conclusions as to the validity of the allegations and recommendations for further action. The report should be submitted to the Whistleblowing Officer.

After the investigation, the investigator will inform the Whistleblower of the outcome of the investigation and what action, if any, has been taken. Sometimes the need for confidentiality may prevent Post Office disclosing specific details of the investigation or any disciplinary action taken as a result. If it is determined that no action will be taken, then the individual concerned should be informed of the reason for this.

The Whistleblowing Officer will determine what further action is required. If Post Office concludes that a Whistleblower has made false allegations maliciously or with a view to personal gain, the Whistleblower will be subject to disciplinary action.

Post Office cannot always guarantee the outcome the Whistleblower is seeking, but will aim to deal with concerns fairly and in an appropriate way. If a worker is unhappy with the way in which their concern has been handled, they should raise it with the Whistleblowing Officer or if that is not appropriate for any reason, the Chairman of the Post Office Board Audit and Risk Committee.

The investigator will share any reports with the Whistleblowing Officer. In all cases a report of the outcomes of any investigation will also be made to the Audit Committee as a means of allowing the committee to monitor the effectiveness of the Policy.

Copies of such reports should be held in accordance with Post Office's document retention policies.

External Disclosures

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

However, the law recognises that in some circumstances it may be appropriate for workers to report their concerns to an external body such as a regulator. It will very rarely, if ever, be appropriate to alert the media.

POL00423565

The independent Whistleblowing charity, Public Concern at Work, have a list of prescribed regulators for reporting certain types of concern. Their contact details are as follows:

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

Public Concern at Work operates free, confidential advice to people concerned about crime, danger or wrongdoing in the workplace. We strongly encourage you to seek advice from them before reporting a concern to external parties.

Protecting the Whistleblower

It is understandable that Whistleblowers are sometimes worried about possible repercussions. Post Office has a statutory obligation to protect Whistleblowers and will support workers who raise genuine concerns under this Policy, even if they turn out to be mistaken.

Post Office will take all reasonable steps to ensure that Whistleblowers do not suffer any detrimental treatment as a result of raising a concern. Detrimental treatment includes disciplinary action, dismissal, threats or other unfavourable treatment connected with raising a concern.

Workers must not threaten or retaliate against Whistleblowers in any way. If anyone is involved in any such conduct, it will be taken seriously and they will be subject to disciplinary action.

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

Training will be provided to managers to make them aware of the rights of Whistleblowers.

Contact us

If you need further information about this Policy or wish to report an issue in relation to this Policy , contact Nisha Marwaha – Employment Lawyer on GRO or by email : GRO

POL00423565

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 Whistleblowing by reports from its committees including its ARC Committee.

- 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.

How we monitor compliance

The Principal Employment Lawyer will ensure that this policy is 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 and Compliance Committee.

The General Counsel provides an annual summary of reports made via the Speak Up line and other known instances of Whistleblowing to (i) the Post Office Board and the Post Office Management Services Board as appropriate, and (ii) the Post Office Board Audit and Risk Committee. In making these reports, the confidentiality of Whistleblowers will be respected.

Any serious concerns reported by Whistleblowing will be escalated by the Whistleblowing Officer to the Chairman of the Post Office Board Audit and Risk Committee.

POL00423565

Section D. Key Terms and References

Key Terms

Term or Acronym	Description
HR team	Post Office Human Resources team

References

References	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 (POMS)
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

POL00423565

6) Oversight of Post Office FCA regulated activities - RCC

Author: Jonathan Hill Sponsor: Kevin Gilliland Date: April 2016

Executive Summary

Context

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.

Post Office is an Appointed Representative 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 (AR) allows Post Office to be exempt from authorisation under FSMA to undertake FCA regulated activities provided certain conditions are met, including that BoI and POMS will take regulatory responsibility for Post Office in respect of such activities. 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 Distribution Agreement (DA) which includes a Regulatory Governance Manual (RGM) to govern the conduct of regulated activity.

The questions addressed in this paper:

1. What are Post Office's obligations under the AR, DA and RGM?
2. What framework is in place to ensure compliance with these obligations?
3. What assurance is provided to Post Office and its Principals to demonstrate compliance?
4. What would the consequences be if Post Office failed to comply?
5. What further actions should Post Office take to ensure compliance?

Conclusion

BoI and POMS take the ultimate responsibility for regulatory compliance through their FCA authorisation and under the Appointed Representative agreements. The obligations in place with our regulatory Principals require Post Office to comply with the relevant FCA handbook requirements and Post Office's CEO is the FCA Approved Person for the AR responsibilities.

There is an established framework in place for providing regulated financial services for compliance through the BoI relationship and reporting of compliance

POL00423565

risks and issues to the Principal. It is however recognised by both Principals that there are gaps and there are areas that need to be improved, particularly through 1st line ownership of controls in the network. The key areas for improvement have been identified with action plans and are outlined in this paper.

The Network lead team fully support this activity. It is our assessment that both the introductory and sales activities in our network should continue pending further work on controls and oversight. Planned Internal Audit oversight activity in network sales this year will further test the adequacy of the control environment across the key risk areas identified in this report.

Background

All Post Office FS distribution can be conducted online, via call centres or through the branch network. The exception to this are loans which are conducted by call centre or internet only. All contact centres and website fulfilment is managed directly by the Principals and/or their third party providers.

Internet

The customer interaction will be on an 'execution only' basis. The relevant web sites and on line journeys and are all reviewed and signed off directly by the regulatory principals in respect of the sales and service journeys. There are established 'sign off' processes in place between sales teams and Principal compliance teams for this approval.

So for example for credit card internet journeys the Post Office/BOI product teams and the Post Office digital team may construct the website and the journey. But BOI compliance are then responsible for reviewing and approving the site from a compliance perspective.

Call Centres

The customer interaction will be on a non-advised basis, with the exception of mortgage sales. The sales and service call centres for Post Office's FS products are operated by third parties operating on behalf of Post Office Money.

Post Office has a general help line for customers (POEX), Post Office call centre staff will not fulfil financial services sales or service calls from this call centre but are trained to direct these calls to the financial services firms.

Post Office Branch Network

The Post Office branch network provides different levels of distribution with customers' dependant on product and who engages with the customer (see below).

POL00423565

Table 1: Insurance Distribution in the Post Office Network-POMS

	Motor and home insurance	Life term assurance	Over 50s Life	Travel Insurance	Other insurance products e.g., pet, business
Financial and Mortgage specialists	Can complete sales on non-advised basis (use 3rd party insurer website for sale)	Can complete sales on non-advised basis (use 3rd party insurer website for sale)	Can complete sales on non-advised basis (use 3rd party insurer website for sale)	Can complete sales on non-advised basis (sales captured through Horizon platform)	Introduction only
Customer Relationship managers	Introduction only	Introduction only	Can complete sales on non-advised basis (sales captured through Horizon platform)	Can complete sales on non-advised basis (sales captured through Horizon platform)	Introduction only
Counter colleagues in Crown and Agency	Introduction only	Introduction only	Can complete sales on non-advised basis (sales captured through Horizon platform)	Can complete sales on non-advised basis (sales captured through Horizon platform)	Introduction only

Banking distribution in the Post Office Network-BOI

	Mortgages	Credit Card	Savings Products including Pre paid funeral
Mortgage specialists	Fully Advised sales process	Can complete sales on non- advised basis	Can complete sales on non- advised basis
Financial specialists	Capture leads only	Can complete sales on non- advised basis	Can complete sales on non- advised basis
Customer Relationship managers	Capture leads only	Introduction only	Introduction only
Counter colleagues in Crown and Agency	Capture leads only	Introduction only	Introduction only

POL00423565

Financial and Mortgage Specialists ("FSs and MSs") in Crown branches

The scope of FSs/MSs activities extend beyond insurance products. For example, all mortgage specialists are qualified mortgage advisors and all specialists can arrange the sale of a variety of Post Office Money products. These specialists will have customer appointments where customers can discuss their needs and specialists provide information for customers to facilitate them making an informed decision on whether to take out a product.

Customer Relationship Managers ("CRMs") in agency branches

Postmasters or agency approved staff are trained by Post Office to undertake a more engaging introductory sales journey with the customer using sales aids and scripted conversations. The journeys remain introductory-only except for Over 50s Life and Travel Insurance where CRMs can complete the sale on the Horizon platform. For the other insurance products the CRM can introduce the product and signpost to the customer options on how to complete the sale; typically online or through a contact centre.

Counter Colleagues

Counter colleagues can complete sales for Over 50s Life and Travel Insurance using the Horizon platform. This capability is available in 9,600 branches for Over 50s Life and 7,500 branches for Travel Insurance, providing immediate cover to the customer. For Travel insurance this includes requesting the customer to declare any medical issues via the contact centre where medical screening may be required.

The remaining activity is composed of product introductions to customers in Crown and Agency branches. This is where the customer is provided with limited oral 'introductory' information about a product (either in response to a customer's request or introduced to the customer) and, if the customer is interested in finding out more or wants to apply, he/she is either provided with an application pack to complete, invited to contact the relevant contact centre go online or bring the completed application pack in to branch for a counter colleague to send.

1. What are Post Office's obligations under the RGM?

The regulatory Principals have appointed Post Office as its agent to carry out the regulatory activities as outlined contractually in (a) and (b) below and Post Office is required to carry out its business in accordance with the requirements of the FCA handbook. In this respect the CEO of Post Office is the Approved Person for these purposes and has been approved as such by the FCA.

a) The Regulatory Governance Manual (RGM)
b) The Distribution Agreement
c) and the FCA Handbook

The RGM outlines the compliance requirements to be followed in key areas covering the FCA handbook together with relevant product related schedules.

POL00423565

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 insurance products

Post Office is required to have in place systems and controls to meet the requirements identified above.

e.g., for Training and Competence the RGM requires staff to be competent, to be adequately supervised and regularly trained. It also requires that Post Office must establish, maintain and communicate to Post Office staff such systems and controls as are necessary for it to ensure that Post Office staff:

(a) involved, either directly or indirectly, in the sale or promotion of the Products; or

(b) responsible for the supervision of those involved in the sale or promotion of the Products,

are 'fit and proper' persons for the role they perform including confirming financial soundness, honesty, integrity and reputation.

For Financial Promotions the regulatory requirements are that these promotions should be 'clear, fair and not misleading'. Post Office is required to establish, maintain and communicate to staff such systems and controls as are necessary for it to ensure that the promotional material it uses, displays and distributes in relation to the Products is:

a) Approved for use by POMS and BoI;
b) Current and up-to-date; and
c) Withdrawn in accordance with any instructions provided for this purpose

2. What framework is in place to ensure compliance with these obligations?

Governance

Post Office

POL00423565

In Post Office, FS and network risks are overseen by regular reporting into the Risk and Compliance Committee and the Audit and Risk Committee. The Post Office CEO is the FCA Approved Person, the General Counsel is responsible for ensuring we have the appropriate framework in place to ensure compliance and the Network and Sales Director is responsible for ensuring compliant branch sales.

Post Office/BoI

PO risk report into the monthly Sales Oversight Compliance Forum (SOCF) which reports into the monthly Customer and Conduct Risk Committee (CCRC). As well as the respective teams from risk and compliance the CCRC has business representation from the Director of FS, the Network and Sales Director, senior business representation from BoI and the Chief Risk Officer of BoI.

PO/POMS

POMS has a monthly Risk & Compliance Committee. This is attended by the Post Office Head of FS risk and POMS Head of Risk and Compliance and their respective teams. This forum will report into the POMS ARC.

Management Information

The current focus of the MI is Post Office branch distribution as the Principals receive directly and oversee themselves compliance management information in respect of call centre and internet distribution directly.

The MI reported into these forums is currently being reviewed as part of the network conduct risk action plan to ensure that that there is adequate information to mitigate risk and to better assess the sources of assurance that are available in the first line.

The typical MI reviewed includes.

- Training and Competence reports
- Risk registers
- Regulatory Horizon scanning
- Reports into incident breaches
- Complaints reporting
- Compliance monitoring reports and planned activity

In addition to this, both teams will meet regularly to discuss compliance risks and issues as they arise.

There is also a Post Office/POMS/Bank of Ireland tripartite meeting. This does not report into a formal reporting 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.

POL00423565

Risk Management

Post Office FS has a comprehensive bottom up risk register across its product areas that are owned by each business/product area together with a Post Office FS 'top risks' register.

FS Risk requires that material new business initiatives (such as the CRM programme) are formally risk assessed. These business risk assessments are shared with the POMS risk team to review progress and understand compliance risks.

POMS also has risk management processes in place and risk registers that are shared and reviewed. Both POMS and Post Office registers are broadly aligned with a similar risk register structure building on best practice from group risk.

Post Office follows the incident reporting processes of 'group' and reports any relevant incidents and breaches into the POMS risk team.

Compliance

The POMS RGM and approach to compliance was largely adopted from that used by the Bank of Ireland. This is helpful in ensuring a consistency of framework across Post Office bearing in mind that the Bank has a higher risk portfolio of activities to oversee across the network. The FS risk team work together with BOI and POMS to ensure compliance, such activities include:-

- Working with the wider business to ensure compliance of business initiatives
- Following up on monitoring reviews
- Investigating compliance breaches and undertaking root cause analysis
- Working with the Principal on the design and approval of incentive schemes
- Design approval and oversight of T&C schemes
- Agreeing updates to policies and procedures including the RGM

3. What assurance is provided to Post Office and our Principals to demonstrate compliance?

The reporting referred to in section 2 above is the pre-dominant source of assurance provided to the Post Office. This has provided assurance to BoI since it became Post Office Principal in 2004. The risk approach agreed has been to prioritise focus on mitigating the distribution areas of greatest risk.

Therefore, mortgage specialists, who give mortgage advice and are subject to professional qualification requirements have the most extensive control and monitoring framework in place. This is followed by the focus on Financial Specialists who have customer appointments with customers and carry out a wider scope of assisted sales. Then more recently the CRM programme with its higher level of introductory customer engagement has had controls designed to manage these particular risks.

POL00423565

It is, recognised that more widely across the network further work needs to be done to improve appropriate local management ownership of compliance risks and to improve the MI and assurance in the first line.

However, this is set in the context of the sales processes and literature all being approved and re-approved by the regulatory Principal. For example, this would include Principal approval of all incentive schemes used in the network and the scripts and sales journeys for over 50s Life and travel insurance are all reviewed and approved by the regulatory Principal.

In the agency network, the move to CRM branches has put greater first line control around the sales process. This is because the enhanced introductory process has been backed up with dedicated line management reviewing compliance MI, the obligations of the dedicated Training and Competence scheme and line management reviewing monitoring MI such as video mystery shopping and customer validation calls. The programme currently stands at 400 branches but is expected to extend to up to 1,000 of our most active branches in the next 18 months.

Financial and Mortgage Specialists and CRMs

The assurance sources available for specialists and CRMs include detailed monthly MI reporting on compliance covering conduct risk. These reports cover accreditation, product knowledge testing, product sales, product mix, cancellations, complaints and the results of monitoring activity which includes video mystery shopping, customer validation calls and one off reviews such as T&C file audits.

There are, however, some gaps in this reporting that need to be filled such as not all products are currently covered by video mystery shopping. Complaints MI and processing also needs to be improved.

Counter colleague introductions and sales

The sources of assurance in the network include;-

- Network quality of sales MI. This is a report on network activity covering, sales broken down by branch covering product line, cancellations and complaints. This MI can be used to review spikes in activity or trends to investigate in the network.
- Product provider management information on sales, lapses, cancellations and complaints and any customer surveys conducted by them
- BoI team individual branch reviews, whilst they are now 'banking' focussed they provide key data on branch conformance. This includes non- accredited activity (branch staff acting beyond their remit such as offering advice), data protection, AML procedures and inspections for non-compliant brochures and financial promotions. This branch review activity has recently begun in POMS to supplement the oversight given by BoI.
- Intelligence reports received from BoI network coaching and development managers (CDMs). The 40 CDMs in the network provide to the risk team regular updates on any breaches uncovered in the network
- Social media monitoring tools. The social media team reviews the network using key word searches to pick up on non- compliant activity.

POL00423565

The conduct risk action plan identifies that further work should be done to identify the adequacy of current MI as well as the current use and first line oversight of the MI that is currently available.

4. What would the consequences be if Post Office failed to comply?

It is important to note that the MI reviewed to date by Post Office and the regulatory Principals has identified past and current control failures in the network that have led to appropriate mitigating action. For example, recent social media monitoring had identified unapproved financial services promotions on agency branch websites in breach of Post Office requirements. As a result rapid mitigating action was taken to close the sites down and social media training has been given to area managers to ensure that good and poor practices are communicated across the network, together with enhanced monitoring.

There have been no systemic or significant risks (eg mis-selling resulting in customer detriment) under the current POMS or BoI principal relationships that have led to regulatory action. Nevertheless section 5 below (further actions) does outline a number of improvements to the controls in the network that are being deployed.

The RGMs states that Post Office must establish, implement and maintain systems and controls to ensure that the Principals are notified of any material or significant breach of the RGM or any regulation, law or voluntary Code of Practice applicable to Post Office in relation to the distribution of the Products for which they are responsible.

Post Office has systems in place to report any breaches to BoI and for POMS it uses the 'Group incident reporting' processes. The consequences of any breach would depend on its nature and if it was reportable to the regulator based on an assessment of materiality by the Principal. A significant breach as well as having regulatory consequences could lead to reputational damage to Post Office as well as any regulatory fines or censure that was imposed.

Under the AR agreements the Principals ultimately would be entitled to suspend any or all relevant Post Office activities that are not compliant with the AR agreement, the RGM or other regulatory rules.

Whilst the FCA senior managers' regime does not currently apply to Post Office, the direction of travel clearly is to make directors/senior managers personally responsible for systems and controls breaches in areas they control or are responsible for.

5. What further actions should Post Office take to ensure compliance?

As reported above the FS Risk team has undertaken a comprehensive risk assessment of the wider 'network risks', reviewing FCA best practice guidance including the FCA's performance management guidance FG 15/10. The action plan has been shared and agreed with the network lead team and is reported to both POMS and BoI on a monthly basis. Both Post Office and POMS risk registers have

POL00423565

compliance and conduct risks as key areas that require on-going actions to mitigate.

The systems and controls surrounding a) FSs, MSs and b) CRMs, are established. The FS risk team has driven risk management disciplines around these sales structures and oversee, training and competence regimes that are regularly tested, together with regular compliance monitoring tools and accompanying reporting MI that is reviewed.

We have developed plans to ensure that as these sales models evolve (for example the CRM population is expected to increase) the control environment is maintained commensurate with the scope and size of future activity.

There are however identified gaps and risk areas where further improvement is being implemented, many of these are captured in the Post Office conduct risk action plan. The conduct risk plan was put in place in February and is broadly on track. However, it is recognised that this is a significant programme of change to implement.

This action programme is fully supported by the network lead team and covers further work to improve controls in the following thematic areas.

- Sales Model risk assessment and external review of conduct risks in sales model *(This is a key area to assess whether the sales model could drive conduct risk, internal assessment by Q1, external review Q2).*
- Training and Awareness of conduct risk and regulation for all relevant staff from the General Executive downwards.(*This work has begun with training of GE, specialists and FS trainers, a plan is in place to extend training coverage across FS and the network split into two stages 'conduct risk awareness' and 'conduct risk application' to be complete by December 2016)*
- Performance management communications and incentives (*Performance management and communication form part of the training work above and includes ongoing monitoring of communications. Recent work has been completed to strengthen and regularise the existing incentive schemes, FS risk needs to oversee the performance of scheme governance in Q1 and Q2).*
- Review of staff performance processes (*this has been reviewed and completed and found to be appropriate)*
- Process to review exit interviews for conduct risk issues (*alert to FS risk team now in place)*
- Enhanced whistleblowing policy and communication plan (*Policy review complete, awaiting update on communication plan Q2)*
- Staff assessment and vetting (*This will be a significant piece of project work driven by HR completion date Dec 2016*)

POL00423565

- Comprehensive review of MI, quality and quantity and first line review and oversight (*This will review the MI available, whether this is appropriate, who should review it and how action is taken as a result Q2*)

The 2015 PWC Internal Audit review on Post Office FS conduct risk also reported that further action should be taken in this regard:

Priority recommendation
Post Office to perform further work in the identification and assessment of conduct risks across the financial services business in order that a complete conduct risk universe is captured and monitored going forward.

This action was completed in 2015 with a detailed risk assessment performed in partnership with BoI who were Post Office's sole Principal at the time. The outcome of the risk assessment was the conduct risk action plan outlined above.

Priority recommendation
…, we are supportive of the recommendation for a more detailed assessment of the adequacy of the current regulatory and conduct risk controls in place to manage and monitor the individuals employed by Sub-postmasters and Multiples. If not already done so, we recommend that Post Office conducts the more detailed assessment as soon as possible and where inadequate controls are identified, introduces an action plan to address.

The risk assessment conducted in 2015 and the resulting action plan covers this area of risk. This encompasses the training, vetting, management information and oversight work streams.

<u>Facilitating evidence of controls and oversight for Over 50s Life and Travel Insurance sales</u>

Over 50s Life and Travel Insurance sales now have updated and approved training and sales processes in place and MI for Post Office/POMS to review activity (such as sales trends, cancellations and complaints). The gaps are around being able to improve the oversight of the efficacy of these arrangements. For example, for CRMs and specialists we undertake video mystery shopping to assess competence, compliance and customer experience. This is not undertaken in the wider network and as part of the conduct risk action plan we are reviewing what other assurance can be put in place. For example, there are action points, for Post Office Risk and both Principals to:-

- *Review existing monitoring programme with BoI/POMS to identify areas of risk and significant gaps by* 31/5/2016
- *To review the key data that is available or can be obtained on a cost effective basis to oversee conduct risk by* 31/05/2016.

POL00423565

Staff vetting

Post Office is reviewing its vetting policies and procedures to ensure that they reflect industry recognised practice. Whilst there are detailed policies and procedures in place for Mortgage Specialists and their managers, the wider policies and procedures need improving to reflect best practice (e.g., current practice includes criminal record checking but does not, for most staff, cover credit checking)

FS Risk and POMS and have given HR feedback on what the minimum regulatory standards should be for vetting and progress on this is being tracked with HR.

Third Line reviews (Internal Audit) reviews 2016/17

Internal Audit supported by PWC are conducting three further relevant reviews this year. These are:

- FS-Branch network sales Training and Competence Review, reporting to Post Office ARC Sep 2016
- FS-Branch network sales process review, reporting to Post Office ARC Jan 2017
- FS-Branch Network sales quality review, reporting to Post Office ARC Mar 2017

The scope of the audits will be reviewing the systems and controls for specialists, CRMs and counter colleagues. This will be an important 'third line of defence' review to benchmark Post Office's assessment of the control environment.

Jonathan Hill
Head of FS Risk
Post Office

POL00423565

7) Annual report on operation of gifts and hospitality procedure

Author: Georgina Blair Sponsor: Jane MacLeod Meeting date: 05 May 2016

Executive Summary

Context

Post Office has had a Gifts and Hospitality procedure in place as part of its anti-bribery procedures since June 2011. The purpose of this paper is to update the Risk & Compliance Committee on the operation of the Gifts and Hospitality procedure in Post Office over the past year.

Questions this paper addresses

1. How many reports of gifts and hospitality were made in in the year to 28 February 2016 and by which business units?

2. How does this compare to last year?

3. Is the gifts and hospitality procedure operating properly as part of our anti-bribery procedures?

Conclusion

1. 305 reports were received in the year to 28 February 2016. The highest number of reports were from Financial Services; some business units reported very little gifts and hospitality.

2. Overall this is more than last year but reporting patterns are similar to last year.

3. There is evidence that most lead teams understand the need to report and ask for authorisation when offered gifts and hospitality, but that these reports are not always passed on to the Central Risk Team to record on the central register. Instead reports are held at local level. The gifts and hospitality reporting procedure needs to be better publicised as it forms a key part of our anti-bribery procedures. Awareness and compliance will be improved by:

- Including the gifts and hospitality procedure in Anti-Bribery training which is currently overdue given our contractual arrangements under the MDA.
- Updating the presentation of the gifts and hospitality procedure on the intranet to make it easier to find
- Working with HR to ensure the procedure is included in an improved induction process.

Input Sought

The Committee is asked to review the report and approve the proposed actions. ARC will be updated on the operation of the procedure as part of an annual anti-bribery update in March.

POL00423565

Appendix 1

Summary of reports to the Gifts and Hospitality register in the year to 28 February 2016 and a comparison for the year to 28 February 2015

Area	**1 March 2015 to 28 Feb 2016**				**1 March 2014 to 28 Feb 2015**			
Business Unit	Total reports of gifts received	Total reports of hospitality received	Reports of gifts received by GE members**	Reports of hospitality received by GE members**	Total reports of gifts received	Total reports of hospitality received	Reports of gifts received by GE members**	Reports of hospitality received by GE members**
Business Transformation	0	1	0	1	0	0	0	0
Commercial	0	33	0	0	0	3	0	0
Corporate Services	1	28	0	2	0	27	0	2
Finance	0	3	0	3	1	13	3	4
Financial Services	3	203	3	26	3	85	1	29
Operations*	0	14	0	7	2	25	2	14
Network and Sales	3	10	0	1	7	18	0	3
Office of the Chief Executive	0	4	0	4	0	19	0	19
People & Engagement	0	2	0	0	1	0	0	0
Total	**7**	**298**	**3**	**43**	**14**	**190**	**6**	**71**

* Operations includes POL IT, Supply Chain and Procurement

**Reports of gifts and hospitality received by GE members are included in the totals for each business unit.

POL00423565

8) Review of whistleblowing procedures in 2015/16

Author: Georgina Blair Sponsor: Jane MacLeod Meeting date: 05 May 2016

Executive Summary

Context

The purpose of this paper is to update the Risk & Compliance Committee on the operation of the whistleblowing procedures in Post Office over the past year.

Questions this paper addresses

1. Is the whistleblowing policy fit for purpose?
2. Has the policy been complied with in the year?
3. How many reports of whistleblowing reports were made in the year to 31 March 2016 and how does this compare to last year?
4. What else needs to be done?

Conclusion

1. The whistleblowing policy has been updated and needs to be approved (see agenda item 5).
2. The whistleblowing procedure is operating but needs to be publicised more.
3. Seven reports were received (see Appendix 1 for summary). This is more than last year, when a total of three reports were received, but still a low number given the total number of employees in Post Office. A large number of calls are made annually to the Security reporting line 'Grapevine' and it is likely that some of these calls could be classed as whistleblowing reports, but there is currently no mechanism to distinguish them.
4. Implementation of the updated whistleblowing policy will require training and awareness activities. ARC will be updated on the operation of the policy and procedures annually in March.

Input Sought

The Committee is asked to review the report and approve the proposed actions.

POL00423565

The Report

Is the whistleblowing policy fit for purpose?

1. The whistleblowing policy has been revised and updated. As part of the process our external auditors reviewed it for compliance with the new whistleblowing regulations for the financial services sector.

Has the policy been complied with in the year?

2. The previous version of the whistleblowing policy was complied with during the year, but awareness of the whistleblowing line among employees is low.

How many reports of whistleblowing reports were made in in the year to 31 March 2016 and how does this compare to last year?

3. Seven whistleblowing reports were received in the year to 31 March 2016 (see Appendix 1). This is an increase on the previous year, when a total of three calls were received. This is still a low number given the total number of employees within Post Office.

What else needs to be done?

4. The updated policy needs to be implemented. As part of this awareness of the policy, the correct method of dealing with whistleblowing reports and the availability of the Speak Up line and other methods to report whistleblowing will be communicated to all employees.

POL00423565

Appendix 1

Summary of whistleblowing reports in the year 2015/16

Number	Date	Subject of report	Mode of contact	Action	Result
1	September 2015	Behaviour of senior management	Verbally to GC	Investigated – insufficient evidence to support allegation	Closed
2	November 2015	Activity of postmaster	Speak Up Line	Investigated – no evidence found	Closed
3	December 2015	Procurement process	Verbal to Legal team	Further information requested	Closed
4	January 2016	Relating to Sparrow investigation	E-mail forwarded from Lord Arbuthnot	Investigation to confirm whether matters have been addressed	Closed
5	January 2016	Activity of postmaster	Speak Up Line	Investigated – no evidence found	Closed
6	January 2016	Employment matters within third party	E-mail to Paula Vennells	Referred to third party and investigated in conjunction with them. No evidence of misconduct.	Closed
7	March 2016	Activity of colleague in branch	Speak Up Line	Investigated and matter resolved without intervention.	Closed

POL00423565

9) AML and CTF Risk Update

Author: Tom Basquille Sponsor: Jane MacLeod Meeting date: 5th May 2016

Executive Summary

Context

This paper updates the Risk and Compliance Committee on progress with the HMRC Regulatory Activity project which has been established to manage both the HMRC's Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) audit, and to progress the recommendations set out on 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. A steering group has been convened to oversee the assessment and implementation of the Promontory recommendations, and to manage the HMRC compliance audit activity. The Steering Group includes representatives from key impacted areas such as Network (inc. Supply Chain), People & Engagement, and Financial Services. External financial crime legal specialists have also been engaged.

HMRC Audit

2. POL continues to work closely with HMRC through the current 'Discovery' phase of the Audit. Following requests for information from HMRC, we have provided a significant amount of information covering areas such as Branch Registration, FRES Data and Sub-Postmaster On-boarding processes.
3. HMRC has also requested transactional information on the regulated services provided by POL and documents such as the current Bureau workbook have been supplied. In addition, HMRC's lead representative, Lee Simpson has been hosted in Model Office at Finsbury Dials to observe operational processes and procedures for these transactions.
4. In relation to branch audits, HMRC have indicated that they propose to conduct hosted visits at two Crown Offices and at one WH Smith branch, and a visit to one branch of each of the next three largest agents – all within close proximity to Finsbury Dials. We have notified WH Smith and the other multiples of the fact of the audit and that a visit is likely. These visits will be used as an 'educational tool' for the main audit comprising scheduled visits by HMRC only to circa. 150

POL00423565

independent branches. We will have the opportunity to comment on the proposed list of branches to be visited and agreed communications will be issued to each branch at least a week prior to the visit.

5. As the HMRC's approach to the audit emerges and the links to Promontory Report's recommendations are established, we will develop the engagement plan for external stakeholders including Treasury, BIS, FCA and Bank of Ireland.

AML training

6. AML compliance training was rolled out to all staff during March and was released to the Network in the week commencing 25th April. Agents will be able to access the training via Horizon On-line and the mandatory test though Horizon itself. A communications framework is in place to promote this regulatory training, including a Message Broadcast on the launch date.

Promontory Report Recommendations

7. Recruitment is underway for 2 roles required to implement the recommendations arising from the Promontory Repot. These roles are (i) an AML analyst to be based in Chesterfield supporting activity such as the Suspicious Activity Reporting and transaction monitoring; and (ii) an AML Manager Role to be based in London, focussing initially on priority tasks such as the AML/CTF Risk Assessment. The Risk Assessment is itself a key recommendation and the output of that work will inform our approach to many of the other recommendations.

8. Many of the recommendations made in the Promontory Report relate to improvements in current processes and procedures such as implementing product risk assessment tool, transitioning to electronic suspicion reports and increasing training and awareness, and the viability of these will be assessed during the project.

9. A breakdown of the areas of focus within the Promontory Report is provided below. Further detail of these recommendations and progress against them will be provided at the next RCC update.

	Priority		
Area	**Level 1**	**Level 2**	**Totals**
Governance and Culture	2	1	3
Risk Assessment	7	4	11
Policies & Procedures	7	7	14
Monitoring Arrangements	3	1	4
Operation of relevant systems and processes	0	4	4
Training, Awareness and Testing	4	2	6
Suspicion Reporting	4	2	6
MSB	5	2	7
Resourcing	3	1	4
	35	**24**	**59**

POL00423565

10) Property compliance update

Author: Steve Norris Sponsor: Thomas Moran Meeting date: 05 May 2016

Executive Summary

Context

This paper addresses the request made by the Audit and Risk Committee (ARC) on the 17th of March to receive an update on Property Compliance Governance.

Questions this paper addresses:

1. What improvements have been made to property compliance governance?
2. What progress has been made to address the other property compliance issues raised in the March audit report?
3. What remains to be done?

Conclusion

1. The Property team, assisted by the Post Office Legal and Risk and Audit teams and Property experts from BNP Paribas, has completed the assessment of the key risks and the prioritisation of any remedial projects.

The Property team has assessed its operating model and specific monitoring controls over Property regulatory including environmental and H&S risks have been clearly assigned within the Property Team and service suppliers. Engagement and co-ordination processes have been established with stakeholders from other business units.

2. There has been significant progress towards achieving full property regulatory compliance since the last update. Work to remedy identified high risk items has been completed and plans have been developed and included in our 2016/17 budget for dealing with identified medium risk remedial works.

3. Further work is needed to improve the culture of prioritising the identification and reduction of property and health and safety risks at operational sites, including the prevention of fire hazards. This will be achieved by closer working between the Property (Steve Norris), Health and Safety (Martin Hopcroft) and Network Operational teams (Steve Blampied) and branch manager training by the H&S Team which will be completed by June.

POL00423565

4. The future stability of the Property and Health and Safety team members is a key component of successful property compliance and must be addressed.

Input Sought

The Risk and Compliance Committee is asked to approve this report for submission to the Audit and Risk Committee.

POL00423565

The Report

What improvements have been made to property compliance governance?

1. The Property team is implementing improvements against five pillars of good governance processes:

(1) Leadership, accountability and culture

a. The desired risk appetite has been discussed with all property and facilities management suppliers (H&S team is aware of the business risk appetite).
b. The scope and responsibilities for service suppliers and Facilities Managers have been reviewed and H&S responsibilities have been clearly assigned to them.
c. Representatives from Network and Health and Safety teams will attend the monthly Property Compliance Forum which provide oversight of all the key property related H&S risks and incidents.

(2) Structure, processes and performance oversight

a. We have re-prioritised the role of Facility Managers to focus on identifying and minimising the higher risks within the property estate and the suppliers' operations. -We have recruited a senior Facilities and Compliance Manager, additionally we are training an existing employee as an assistant Facilities Manager. "Duty holders" and "Responsible Persons" roles have now assigned to POL staff, but Duty Holders will need changing from Kevin Seller as a result of Post Office restructuring.
b. Training for the Post Office property team, Duty Holders and Responsible Persons on key statutory compliance areas is ongoing and will be completed by the end of June.
c. Facilities Management suppliers' competency has been self-assured against best standard.
d. Relevant policies and handbook have been reviewed and will be signed off shortly.

(3) Risk Monitoring

a. Assessment of the key risks and the prioritisation of any remedial projects have been completed.

POL00423565

b. The development of the compliance controls framework, which defines the ongoing compliance controls across the property estate for all the key stakeholders, has been almost completed, pending update on Person in Control ("PiCs") and Facilities Managers new responsibilities.
c. Facilities management contractors' polices, compliance regimes have been checked and approved by the Post Office Property team.
d. Relevant policies and handbook have been reviewed and will be signed off shortly.

(4) Engagement with stakeholders

a. Continue integration and co-ordination with other key H&S team has improved and we are now attending each other's planning meetings and report jointly.
b. Compliance communication and planning with facility management suppliers has improved with visibility of their performance via attendance to the Property Compliance Forum and formal monthly supplier operational meetings.

(5) Management of information

a. Regular incidents/near miss reports are being produced by facility/estate management suppliers and discussed at the Property Compliance Forum.
b. Board/Committee papers: a joint monthly report including H&S and Property will be issued to the Group Executive team on property compliance issues from April onwards

What progress has been made to address the other property compliance issues raised in the March audit report and what remains to be done?

1. Regulatory risk progress

There has been significant progress towards achieving full property regulatory compliance including reducing the risk of breaches of health and safety and environmental law since the last update.

2. Property regulatory compliance risk assessments

Risk assessments have now nearly all been completed by our suppliers (see Appendix 1). There has been some slippage owing to practical difficulties encountered by our suppliers e.g. difficulties gaining access and reliable information. Work to remedy identified high risk items has been completed and plans have been developed and

POL00423565

included in our 2016/17 budget for dealing with identified medium risk remedial requirements; mainly electrics, asbestos, building fabric and legionella.

3. Electrical testing

Electrical testing is now 91% complete. There has been a 1 month slippage due to access issues, but these assessments will be 100% complete in May.

4. Residential risk assessments

Residential risk assessments for fire and fixed wire testing are ongoing due to be completed by the end of May and lower risk water risk assessments (which are not a statutory responsibility) by the end of May. Remedial works such as fitting smoke alarms and carbon monoxide should all have be fitted by the end of April. External fabric of residential properties has been assessed. Internal inspections have only highlighted damp issues at one property. Gas inspections are also complete.

5. Environmental law

There has been significant focus on waste management across the POL estate to avoid fixed penalties and other enforcement being taken against POL. Regulation concerning the management of waste is restrictive and easy to breach. POL is reliant upon Servest and our PiCs to ensure compliance. Servest have retrained and communicated with their staff the need for strict compliance and POL has sent communications to PICs followed up by phone calls to ensure their responsibilities are understood. This is an area of ongoing concern as breaches are still occurring. We have an action plan in place now with Servest to address this. While the most usual enforcement is by small fixed penalty fines £50 to £100 we have faced prosecution for abandonment of waste outside our own premises (successfully defended) where the fine could have been within a range of £7K to £25K.

POL's annual Carbon Reduction Submission was completed and submitted to the Environment Agency in September last year for the year 2014/15. The Environment agency additionally carried out an audit on the previous year's submission in 2013/14 which was also found to be satisfactory.

.

POL00423565

6. Fire risk and housekeeping

The most significant area to improve is in housekeeping to manage fire risk. This was reported by CBRE to the Property Compliance Forum as a finding from their risk assessments, currently carried out over 93% of the estate.

PiCs are being issued with the results of the fire risk assessment audits from CBRE and requested to address any areas identified. We are defining a process which will provide assurance that all steps to address risk have been actioned.

Many PiCs are Managers who have relocated, are new in post or are simply overdue a refresh of their original training. A H&S led PiC training programme has also started and due for completion in June. This is outlined in Appendix 3.

We are engaging with Network Operations to propose the implementation of:

a) Peer to peer compliance review in accordance to industry best practices or an equivalent alternative process. This will be actioned in May.
b) Regular reviews and appraisal of PiCs Property compliance performance by their line managers.
c) Clear audit trail of compliance actions identified and resolved.
d) Improve communications processes between Property, Network Operations and H&S teams.

7. Leadership, accountability and culture

Work is ongoing to ensure that the culture of health and safety across the business is aligned to the 'risk averse' appetite for the areas where opportunities to improve have been noted. The plan in summary is as follows:

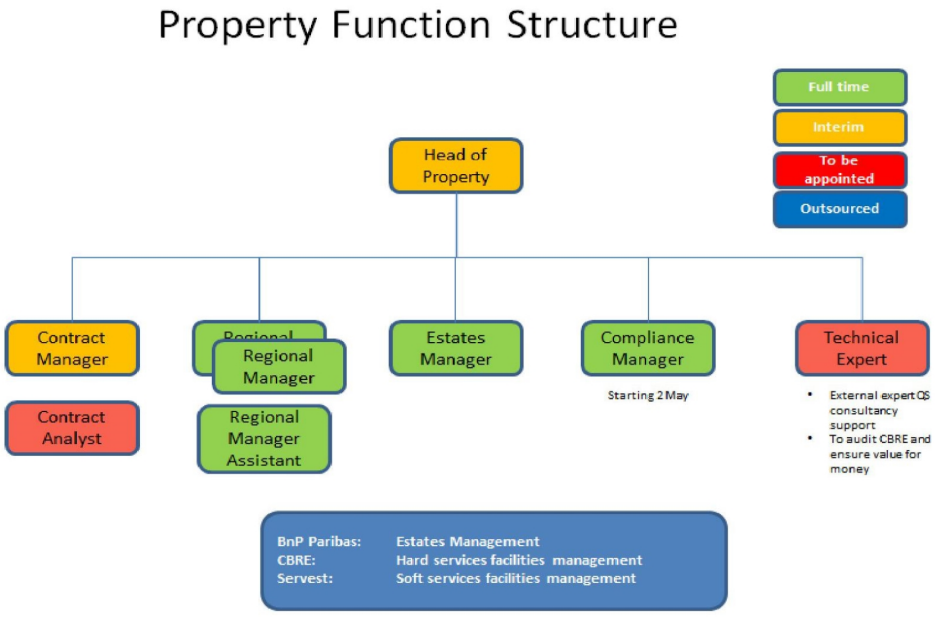
7.1 Compliance programmes addressing the risk assessments as set out in Appendix 1 will be completed in the financial year 2016/17. The Compliance Forum, chaired by Steven Norris, is the entity which will manage completion of this programme of work. The delivery of compliance works will be undertaken by CBRE.
7.2 Site by site risk assessments will be produced by CBRE, who manage the high risk areas and enhanced with insights from Servest and the H&S team. This will be live from April onwards for consideration by the Compliance Forum. This risk based view will be used to prioritise site visit audits by POL's Facilities Managers to ensure high risk areas are continually identified and addressed either through the PiCs, CBRE, BNP the H&S teams or Servest. This will be an ongoing process in perpetuity and key risks will be escalated up to the RCC and POLs Exec through monthly reporting from the Compliance Forum.

POL00423565

The role and responsibilities of the PiCs and training needs are being reviewed by the H&S and property teams in May. The Network Operations Team has been engaged and they will attend the Compliance Forum to ensure that PiCs responsibilities get implemented and monitoring mechanisms of their activities are established by June.

8. Structure, processes and performance oversight

The future stability of the Property and Health and Safety teams must be assured in order to enable the implementation of the new operating model and ensure that appropriate property regulatory compliance including health and safety matters are properly addressed and monitored going forward. The structure of the Property Team is shown below:



(Note: the above structure exclude: Crown Transformation and NT and Equipment teams. These teams have a different reporting line)

There are additional statutory roles of Duty Holders and Competent persons required under environmental law, health and safety law and other statutory compliance, for each of the 14 areas of compliance. These roles have all been defined and individuals appointed within the Post Office. The table at Appendix 2 explains these roles and the appointee. In addition the role of Competent Person is fulfilled by our suppliers, Servest and CBRE and their competency has been

POL00423565

recently checked. Due to internal restructuring, the Duty Holder will have to be re-appointed from Kevin Seller.

The business should be aware that in the event of enforcement, the relevant authority may look to enforce against Group Executive Members and Directors.

The compliance controls activities for PiCs and H&S teams are to be finalised and integrated with the activities of the Property Team and a final meeting to implement this is planned on 25th May.

There is ongoing work to improve the management of risks across the estate and risk reporting. Particular focus will be given to shared premises and third party occupied properties where obligation may be shared especially between Royal Mail Group (RMG) and POL. A programme of work covering these risks is being prepared by CBRE which will then need to be for action to by RMG.

9. Risk Monitoring

The compliance control framework has been developed which has addressed critical areas. Other priority areas are now being addressed. Amended policies will be signed off and implemented.

The Property Compliance Forum recommended that once the new operating model and compliance governance framework has reached business as usual, an operating benchmark exercise is carried out to ensure that structure and processes in place are designed and operating as expected for an organisation of this size and complexity. We anticipate this to be around August.

10. ARC and RCC support

Continued support is required from the ARC and RCC to ensure all involved give these objectives the high priority they demand and that behaviours are fostered and appropriate decision are taken to fully support these objectives.

POL00423565

Appendix 1

Status of compliance risk assessments

Planned Maintenance	% inspected	Risk	Completion date	Next steps
Fire Risk Assessments	93%	M-H	End May	13 sites remaining. Cultural improvements still needed at sites
Asbestos	99%	M	30 April	All high risk items access controlled while containment is completed. Huyton CO (Vacant) is still outstanding due to difficulties in obtaining access
Radon	100%	L	Complete	No risk areas identified nor unlikely to be in phase 2 assessments
TM44	100%	L	Complete	Highly inefficient boilers, coolers and lighting systems being replaced in 2016
Lift Insurance Inspections	100%	L	Complete	Minor defects remedials actioned to Lift service contractor
PAT Testing	100%	L	Complete	Minor issues. All have been addressed
Fixed Wire	91%	M	End May	All high risk areas addressed. Medium risks will be addressed in 16/17
Pressure	100%	L	Compete	No issues
Energy Certificates	100%	L	30 April	Minimal issues. Reports now being received
Legionella	91%	M	End May	43 remaining, these are being planned to be completed within May
Building fabric	100%	M	Complete	Mainly security and access risks which will be addressed in 16/17

Note: This table explains the recovery of the backlog of overdue risk assessments over the last 6 months. Going forwards risk assessments will be undertake on a rolling programme as they become due.

POL00423565

Appendix 2

Duty holder and Responsible Persons roles and appointed person

STATUTORY RESPONSIBILITIES					
TOPIC	**LEGISLATION**	**Main Regulatory Bodies** (provided by Ashfords- legal firm) other bodies may regulate some aspects of these topics, e.g. Food Standard Agency, FinancIAL Conduct Authority)	**RESPONSIBLE PERSON**	**JOB TITLE**	**DUTY HOLDER**
1. Electricity	Electricity at Work 1989 (Regulation 3)	Health and Safety Executive Local Authority	**Steve Norris**	Interim Head of Property	**Kevin Seller**
2. Legionella Management	The Control of Legionella Bacteria in Water Systems (AcoP L8) & The Notification of Cooling Towers and Evaporative Condensers Regulations (1992)	Environmental Agency	**Kevin Harris**	Facility Manager	**Kevin Seller**
3. Waste	Environmental Protection Act 1990, Section 34.	Environmental Agency	**Cherly Hurd**	Facility Manager	**Kevin Seller**
4. Asbestos	The Control of Asbestos Regulations 2012, Regulation 4	Health and Safety Executive Local Authority	**Andy Mason**	Equipment, Facilities and Deployment Manager, Service Delivery	**Kevin Seller**
5. Health & Safety	The Health and Safety at Work Act 1974, Section 4 COSHH regulation Environmental Liability Directive	Health and Safety Executive Local Authority Natural England (i.e. Environmental Liability Directive)	**Martin hopcroft**	National Safety, Environment & Wellbeing Manager	**Martin Hopcroft**
6. Pressure Systems	Pressure Systems Regulations 2000	Health and Safety Executive	**Steve Norris**	Interim Head of Property	**Kevin Seller**

POL00423565

STATUTORY RESPONSIBILITIES					
TOPIC	LEGISLATION	**Main Regulatory Bodies** (provided by Ashfords- legal firm) other bodies may regulate some aspects of these topics, e.g. Food Standard Agency, FinancIAL Conduct Authority)	RESPONSIBLE PERSON	JOB TITLE	DUTY HOLDER
7. Lifts & Lifting Equipment	Lifting Operations and Lifting Equipment Regulations 2008	Health and Safety Executive Local Authority	**Kevin Parkin**	North Network Change Manager, Property	**Kevin Seller**
8. Fire	Regulatory Reform (Fire Safety Order) 2005 & Part 3 of the Fire (Scotland) Act 2005, supported by the Fire Safety (Scotland) Regulations 2006.	Health and Safety Executiv	**Martin Hopcroft**	National Safety, Environment & Wellbeing Manager	**Kevin Seller**
9. Natural Gas Systems	Gas Safety (Installation and Use) Regulations 1998	Health and Safety Executiv	**Steve Norris**	Interim Head of Property	**Kevin Seller**
10. Construction/Projects	Construction (Design & Management) Regulations 2015	Environmental Agency Health and Safety Local Authority	**Andy Mason**	Equipment, Facilities and Deployment Manager, Service Delivery	**Kevin Seller**
11. Ionising Radiation	Ionising Radiation Regulations 1999		**Steve Norris**	Interim Head of Property	**Kevin Seller**
12. Carbon	Carbon Reduction Commitment		**Kevin Harris**	Interim Head of Property	**Kevin Seller**
13. Environmental & Sustainability		Environmental Agency Health and Safety	**Kevin Harris**	Facility Manager	**Kevin Seller**
14. F-Gas		Health and Safety	**Steve Norris**	Interim Head of Property	**Kevin Seller**

Note: The Duty Holder Kevin Seller needs to be re-appointed as a result of internal restructuring at Post Office. Deputy Responsible Persons are covered by the property team.

POL00423565

Appendix 3

PiC training approach

Context - There was a requirement to refresh the content of the online Person in Charge training product and make available to all PiCs across the Post Office Estate. Although this was recognised by the Health & Safety Team, this was also a recommendation through the Property Compliance Risk Review.

Reason - Many PiCs are Managers who have relocated, are new in post or are simply overdue a refresh of their original training. Due to IT issues, it has been difficult to update the previous version of the PiC Training and therefore a new product has been created and is currently being tested by our external provider and H&S Business Partners.

Topics – The PiC training covers the general PiC duties and areas of responsibility including Health & Safety Duties, undertaking risk assessments, hazard surveys, ensuring Site Log Books are maintained, keeping H&S training records, fire risk assessments and training, evacuation plans, testing fire alarms and emergency lighting, knowledge of RIDDOR and control of contractors including signing in logs.

Assurance – The H&S Business Partners will have access to Certificates of Compliance with dates that PiC training has been completed and these will be supported by a central view of certification of PiC training module completion via the Training team. There is a requirement for PiC Training to be refreshed every 3 years.

Inspections – These are undertaken by Trade Union rep Inspections (2 per year) and H&S BP Audits at high risk sites. Facilities Managers will also be auditing high risk sites and undertaking property audits. At all inspections and audits the question will be asked whether the PiC training has been undertaken and certificate in date.

Timescales – The new product has been returned to the H&S Team for final review and it is expected that the PiC Training will be launched across POL be the end of May 2016. Local Risk Assessments will be completed in May / June 2016 at all sites and the Certificates of Compliance collated and checked in June 2016.

POL00423565

11) Modern Slavery Act - update

Author: Nisha Marwaha Sponsor: Jane MacLeod Meeting date: 5 May 2016

Executive Summary

Context

The Modern Slavery Act 2015 (the Act) challenges slavery, domestic servitude, forced and compulsory labour and human trafficking. Post Office is required to produce an annual slavery and human trafficking statement (Statement) setting out what steps have been taken to ensure its business and supply chains are slavery free. This paper attaches the Statement which must be approved by the Post Office Board and signed by a Director.

Questions this paper addresses

1. What specific risks should the board be aware of?
2. What action have we taken so far?
3. What are other businesses doing and how do we compare?

Conclusion

- Post Office has been undertaking due diligence on its business and supply chains to identify any risk areas.
- Post Office has prepared a Statement which must be published within 6 months of year end.
- A steering group appointed in January 2016 is responsible for creating a project plan and undertaking due diligence on Post Office's and POMS supply chains.
- The steering group has identified that the highest level of risk is within our Agency network. We will be taking action to address this risk including amending our contracts with our Postmasters to require compliance with the Act.
- Post Office's Statement has been prepared using Home Office guidance and in consideration of other available Statements by UK and international companies.
- Post Office will have to take ongoing action to meet the requirements under the Act.

Input Sought

The Committee is asked to note the contents of the Statement and provide any comments before it is submitted to the Board for approval.

POL00423565

The Report

What specific risks should the board be aware of?

- The requirement to publish a Statement applies to "commercial organisations" which (a) supply goods or services and (b) have a total turnover of not less than £36,000,000. It will therefore not apply directly to Postmasters if their turnover is less than £36 million per year.
  → However, Postmasters are part of the Post Office supply chain. Post Office must state what steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business.

- To date we have not identified any direct relationship with an individual or company registered in a high risk country.

- The due diligence that we have undertaken so far indicates that there is a potential risk on non-compliance within our agency Network:
  → The reason for this is that there are a large number of people employed by Postmasters (including multiple partners) but who are not employees of Post Office or POMS. They work directly for the Postmasters (including multiple partners). We will be taking action to address this risk (see below) including working to amend our contracts with our Postmasters to require compliance with the Act and we will be delivering training to Postmasters as and where it is appropriate.

What action have we taken so far?

1. GE member Neil Hayward delegated responsibility for our Modern Slavery initiatives to a steering group lead by Hannah Dalton (Head of HR). The steering group was appointed in January 2016.

2. The steering group has developed a project plan to carry out due diligence of our business and implement change. Our ongoing work involves a risk analysis of our core business and its related supply chains.

What are other businesses doing and how do we compare?

1. We looked at statements for international companies with complex supply chains to get a flavour for content and examples of initiatives.

   ➢ For example: **Ford**
   - They have published a statement which is approx. 2 pages long.
   - Ford recognise their supply chain is extensive and complicated and that it presents challenges.
   - Some of Ford's initiatives are similar to ours - this is encouraging given that Post Office's business and supply chains are not as extensive as Ford.

POL00423565

2. Many companies have not yet published their Statements, but we have looked at a variety to ensure that our approach is consistent. We are confident that the detail in our Statement and our project plan is appropriate at this stage, but we will monitor developments and keep the adequacy of the Statement under review.

3. We also looked at what some of our partners are doing:

WH Smiths

- Statement not yet published.
- They use the Ethical Trading Code of Conduct and Human Rights Policy. It incorporates the ILO Conventions to scope out the current position on Modern Slavery related matters.
- The policy specifies a person who takes responsibility for the Code.

Bank of Ireland

- Do not currently have a Modern Slavery statement.
- Publish a Responsible Business Report which currently makes no reference to Modern Slavery.
- As a key partner, Post Office should investigate directly with BOI as there appears to be very little in terms of Modern Slavery related matters.

POL00423565

Post Office Limited (Post Office) & Post Office Management Services Limited (POMS)
Modern Slavery Transparency Statement 2015-2016
May 2016

Executive Summary

This statement sets out the steps we have taken during the last financial year to ensure that Modern Slavery is not taking place in any of our supply chains or any part of our business. It is made pursuant to section 54(1) of the Modern Slavery Act 2015 (MSA).

Our business

Post Office is the UK's largest retail network and the largest financial services chain in the UK with more branches than all of the UK's banks and building societies put together. We have provided services for more than 370 years and currently supply more than 170 products and services (mails & retail; financial services; governments services; and telephony) from a Network of more than 11,500 Post Office branches nationwide.

Post Office directly manages currently over 300 of the Network branches. The remainder of the branches are managed on an agency basis by Postmasters and multiple partners.

Our supply chains

We currently operate throughout the UK, however our supply chains connect with suppliers with a global reach.

Banking services
Our banking services are provided through a joint venture with the Bank of Ireland (BoI).

Postmasters
Postmasters can operate one or more branches. As agents they have control on how they run their branches on a day-to-day basis. All those working in an agency Post Office branch are employees of the Postmaster.

Multiple partners
A large proportion of the agency part of our network is run by multiple partners.

Trade Unions
In our Crown network, we work closely with the Communications Workers Union (CWU) and Unite (CMA) Communications Managers Association.

Third Party Suppliers/Procurement
We also procure products and services from a wide range of national and international businesses.

Responsibility and due diligence

Responsibility for our Modern Slavery initiatives currently resides with a steering group which was appointed in January 2016. It is tasked with the development of a project plan to carry out due diligence and implement change. Our ongoing work involves a risk analysis of our core business and its related supply chains.

Where are the risks of Modern Slavery at Post Office/POMS?

To date we have not identified any direct relationship with an individual or company registered in a high risk country. The due diligence that we have undertaken so far indicates that there could be a risk of non-compliance within our agency network because there are a large number

POL00423565

of people employed by Postmasters (including multiple partners) but who are not employees of Post Office or POMS. They work directly for the Postmasters (including multiple partners). We will be taking action to address this risk (see below).

What we have done so far

- Our Whistleblowing Policy has been updated to include references to concerns about Modern Slavery.
- We have adapted the Post Office recruitment policy to address MSA requirements.
- We conducted an assessment of the Post Office procurement process to ensure it aligns with the MSA. As part of this process we conducted a review of the criteria used by Post Office to evaluate whether suppliers meet Post Office's minimum tendering requirements.

Next steps

Our work on Modern Slavery continues and we intend to introduce the following changes in the near future.

- Updating Postmaster's selection and appointment process to address MSA requirements.
- Amending our standard form procurement contracts.
- Developing a communication and training plan to ensure our suppliers, staff and agents are aware of Post Office's obligations in relation to Modern Slaver and informing them about the Modern Slavery Helpline.

Our policies

We currently operate the following policies that describe our approach to Modern Slavery:

- *Code of Business Standards*
- *Whistleblowing Policy*

Further information

If you have any concerns about the issues raised in this statement or if you think you have identified signs of Modern Slavery then please either contact us or call the Government's Modern Slavery Helpline on GRO.

Signed: .....
Name: .....
Position: .....
Date: .....

POL00423565

12) 'Horizon Spotting' Report

Author: Jane MacLeod
Meeting 5 May 2016

Executive Summary

Context

As part of its remit, the Risk & Compliance Committee should consider legal, regulatory and other external developments on behalf of Post Office in order to ensure that impacts on Post Office (including its customers, staff, suppliers and stakeholders) are understood and being appropriately managed. This report highlights current developments of relevance to Post Office and the work that is being done to monitor these.

Questions this paper addresses

1. What are the material legal, regulatory and other external risks the Post Office executive and Board should currently be aware of?
2. What work is being undertaken to assess, monitor and mitigate these risks?
3. Who is accountable for this work and how will it be reported through Post Office governance structures?

Conclusion

1. There are a number of material developments which either will or could impact Post Office and details of these are set out in this summary.
2. In each case work is being undertaken to monitor and assess the risks arising from these developments. 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.
4. The status of those developments which have previously been noted to the Committee is set out in the Appendix.

Input Sought

The R&CC is asked to note these developments.

POL00423565

The Report

Gender Pay Gap

1. The government issued its 'Consultation on Draft Regulations' for Mandatory Gender Pay Gap Reporting on 12th February 2016. Responses to the draft regulations were required by 11th March. Post Office responded, primarily to raise limited concerns over some of the proposed definitions of 'pay'.

2. Gender Pay Gap differs from Equal Pay: Gender Pay focuses on the position of women in the workplace, as measured by pay, whilst Equal Pay is concerned with ensuring that employees are paid equally for work of equal value. It is possible to have a Gender Pay Gap without having an Equal Pay issue and vice versa.

3. Subject to parliamentary approval, the legislation will come into force with effect from 1st October 2016. Companies with more than 250 relevant employees will be required to provide information as defined by the legislation.

4. The information should be published on a searchable website accessible to both employees and to the general public. The information will also need to be uploaded onto a government website. In order to monitor progress the information will need to be held for three years. There is currently no intention to impose penalties for failing to publish.

5. Gender Pay will be measured as at April each year. The first year of reporting will be in respect of pay in April 2017 with the deadline for publishing being April 2018. The information will need to contain:

   - the mean gender pay gap;
   - the median gender pay gap;
   - the numbers of men and women in each of the pay quartiles;
   - the difference between the mean bonuses paid in the preceding year; and
   - the proportion of men and women receiving a bonus.

6. The Human Resources Service Centre (HRSC) is currently able to report easily on most of the definitions of pay, the exceptions being the treatment, for these purposes, of clothing, first aider, and fire warden allowances.

7. It is not proposed to begin to rectify these limited shortcomings until the legislation is finalised on 1st October. Keith Murdoch, Head of Reward has attended external meetings with stakeholders and, whilst there is overwhelming support for the intent behind the legislation, there is widespread concern about the quality and clarity of the draft regulations. It is prudent, therefore, to await the final version of the regulations which will likely see improvements in drafting.

POL00423565

Trade Union Bill

1. On 15 July 2015 the government published a new Trade Union Bill 2015-2016 proposing amendments to the Trade Union and Labour Relations (Consolidation) Act 1992. The Bill aims to reform various aspects of the law on industrial action and trade union obligations and activities. The proposed reforms include increasing ballot thresholds, extending the notice of industrial action required to be given to employers and, a new expiry date for action to be taken following a ballot. The Bill would also introduce more stringent requirements for unions to supervise picketing. Key proposals include:
   - Requirement for a 50% turnout, so that a strike would not be able to go ahead unless half of the eligible members cast a vote.
   - In the case of 'essential public services', such as health, education, fire, transport, border security and some nuclear workers, at least 40% of eligible members would have to vote in favour of action for it to be lawful. This is in addition to the 50% above.
   - A four-month time limit to be introduced limiting the period that can pass between a ballot authorising industrial action taking place and the action starting, and unions will have to give employers fourteen days' notice of the commencement of industrial action instead of the current seven.
   - The ballot paper should state the form of intended industrial action, and when it is to take place.
   - Permitting the use of agency workers to provide cover for striking employees.

2. The Bill is now in its 3rd sitting in the House of Lords after which it will move to the Commons for consideration of Lords amendments.
3. For Post Office, like other unionised businesses, the Bill, if passed in its current form, will provide greater notice of impending strike action. In addition the ability to cover strike action using agency workers (if approved) will assist in mitigating the potentially adverse effect of strike actions on Post Office operations.
4. The progress of the Bill through Parliament and the assessment of the impact of the changes is being monitored by the Industrial Relations team reporting into Neil Hayward.

POL00423565

Ofcom Review

1. On 16 June 2015, Ofcom announced a wide ranging review of the regulation of Royal Mail. The scope of the review is to ensure that the regulatory framework within with Royal Mail operates remains appropriate to secure the efficient and financially sustainable provision of the universal postal service (USO) against the backdrop of changes in the competitive profile of the market.

2. In July 2015, Ofcom published a Discussion Paper providing further detail on the context and purpose of the review and asked stakeholders to consider and provide answers to a number of preliminary questions on the appropriateness of its scope and lines of enquiry. Ofcom intends to complete the review during the course of 2016, with any recommendations for changes to the regulatory framework to be implemented in the same time period.

3. Self-evidently, any changes to the regulatory framework for Royal Mail has the potential to impact on our own obligations, particularly under the Mails Distribution Agreement, thorough which POL effectively provides services to enable Royal Mail to discharge the USO.

4. Accordingly, in its response to the Discussion Paper, POL put down a marker of its interest in the work of the review and POL representatives from the Mails and Public Affairs teams also met with Ofcom last autumn to establish an open dialogue. Discussions have also taken place with colleagues in the Regulatory Affairs Team at Royal Mail, in order to develop a shared appreciation of the likely direction of travel and to ensure that POL is kept abreast of developments.

5. No update or progress report has be forthcoming from Ofcom since the publication of the Discussion Paper, but we anticipate that it will come forward with some proposals in the near future, not least if it is to keep to its intended timetable. Any material developments will, of course, be reported as soon as they occur.

POL00423565

STATUS OF PREVIOUSLY REPORTED DEVELOPMENTS

Issue	Brief Description	Update
Money Laundering	Implementation of the recommendations in the Promontory Report HMRC compliance audit	1. POL continues to work closely with HMRC through the current 'Discovery' phase of the Audit and numerous documents have been provided in response to HMRC requests. 2. HMRC's lead representative, Lee Simpson has been hosted in Model Office at Finsbury Dials to observe operational processes and procedures for these transactions. 3. HMRC have indicated that they propose to conduct hosted visits at two Crown Offices and at one WH Smith branch, and a visit to one branch of each of the next three largest agents – all within close proximity to Finsbury Dials. We have notified WH Smith and the other multiples of the fact of the audit and that a visit is likely. We await details of the 150 branches likely to be visited over the summer. **AML training** 4. AML compliance training has been rolled out to all staff and is due to be released to the Network in the week commencing 25th April. 5. Recruitment is underway for 2 roles required to implement the recommendations arising from the Promontory Repot.

POL00423565

Issue	Brief Description	Update
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.
GDPR	New and more onerous EU Data Protection Regulation	Work is about to start on scoping the likely impact of the Regulations and the Directive on PO ahead of commencing activity to implement necessary changes.
Networks and Information Security Directive	New EU Directive to support GDPR	
Modern Slavery Act 2015	New requirements for due diligence and reporting obligations on supply chain	Statement prepared for release subject to Board review. Work will be ongoing to assess and monitor areas of concern.
Enterprise Bill	Proposals to cap termination pay of public sector employees to £95k	The Government has confirmed that the regulations will not come into force before 1 October 2016 and therefore all exits before that date will not be within the scope of the public sector exit payment cap.
Senior Managers' Regime	Statutory accountability of senior management in FCA and PRA regulated firms	No developments at this stage.
Mails – International Data Capture	Information collection requirements to support mails related dangerous goods requirements	No developments reported at this stage.

POL00423565

RCC 16/20 – 16/28

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

Minutes of an RCCC meeting held at
Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ
on 29th February 2016 at 10am

Present:	Susie Hayward (SH)	Head of Risk and Compliance (Chairman)
	Russ Tavener (RT)	Head of Commercial
	Gerry Barrett (GB)	Head of General Insurance
	Paul Jones (PJ)	Head of Travel
In Attendance:	Karen Oates (KO)	Deputy Head of Compliance
	Michael Brown (MB)	Insurance Operations & Regulatory Manager
	Elizabeth McMenemy (EMM)	Compliance Advisor
	Sanjeeve Thakrar	Risk Manager
Apologies:	Emma McGinn (EMG)	ISAG Representative
	Ryan Griffin (RG)	Head of Protection

RCC 16/20 WELCOME, QUORUM AND CONFLICTS OF INTEREST

(a) The Chairman declared the meeting quorate and open.

(b) SH received apologies from Emma McGinn and Ryan Griffin

RCC 16/21 MINUTES OF THE MEETING HELD ON 9 FEBRUARY 2016

The minutes of the meeting held on 9 January 2016 were approved and the Chairman was authorised to sign them as a true record of the meeting.

RCC 16/22 MATTERS ARISING AND ACTIONS LIST

(a) **Action PRCC 15/47 (m)** – ST to meet with POL BCP representative to discuss alignment of BCP plans and testing

(b) **Action PRCC 15/50 (a)** – GB confirmed that Junction will be responding to the consultation and will share details

(c) **Action RCC 16/08 (d)** – SH updated the meeting on the discussions with MI to produce MI. Action plan in place with POL and we will start to see improvements.

(d) **Action 16/14 (a), 16/15 (b) 16/15 (c), 16/15 (d), –** The meeting considered this action closed

POL00423565

(e) **Action 16/15 (a) –** ST to review and update the incident management process and circulate for the next meeting

(f) **Action 16/16 (e) –** GB noted that information is available and will be included in future MI

(g) **Action 16/16 (h) -** EMM noted that the reasons had been checked and correct

(h) **Action 16/16 (i) –** MB to review travel complaints with PJ

(i) **Action 16/17 (d) –** GB confirmed that Junction had provided an update on the Add-on position and the changes would be implemented with the timeframe

RCC 16/23 **RISK MANAGEMENT**

ACTION ST

(a) SH introduced Sanjeeve Thakrar (ST) as POMS new Risk Manager to the meeting. ST discussed the existing risk management framework and the need to work with each product heads to update the registers particularly controls, actions and dates currently recorded and assist with imbedding the framework. ST will be working through the register to update the scoring to the POL 5x5 table. PJ suggested that the likelihood table be updated to show the likelihood within the 5 year plan.

(b) SH reminded the meeting of the need to ensure the registers are maintained to enable accurate reporting of risk position to ExCo and Board. ST working on a dashboard to assist the reporting structure.

RCC 16/24 **INCIDENT MANAGEMENT**

ACTION MB

(a) The incident register was reviewed however noted that some of the known incidents had not been captured. MB to circulate the incident log again and requested each to ensure incidents are actions are up to date.

(b) New incidents discussed included the Brand Bidding websites and Data incident of data sent to Junction.

ACTION ST

(c) SH noted that the incident management reporting process was in need of refresh and recirculation to all staff. ST to review and update.

RCC 16/25 **1st LINE COMPLIANCE REPORT**

ACTION EMM/PJ

(a) The 1st line QA data was reviewed and discussed. The number of calls monitored by WH has reduced to 4 calls per agent consisting where possible to one sales, renewals, cancellation and MTA however the results were showing high numbers of sales and renewals as these are where the majority of the calls taken. The risk based approach was discussed and how WH are assessing the

POL00423565

risk. It was agreed that EMM would check the criteria and PJ to provide some guidance on areas to assess such as high medical screening and complaints RCA.

(b) Team leaders to provide additional oversight of 20 calls per team commencing on 1st March, training has been completed. Results will be provided to EMM to include in 2nd line reporting.

(c) Claims MI was reviewed with no deviation to trend and no issues identified. Noted that the Travel repudiation numbers had been previously understated and now amended.

(d) Cancellations and NTU's data was reviewed and noted no life data for January. Again, discussed the ability to obtain reasons for cancellations from Aviva and whether the cancellation rate was higher than market

(e) The complaints report was reviewed and noted that complaints had increased 54% since December however seasonally no increase from last January.

(f) Complaints for pet increased 93% relating to renewal costs. Noted that retention rate had remained within the target of 75%, currently running at 78%. Agreed that price increases would be monitored closely with the provider and discussions underway with Pinnacle to proactively manager. RT to check analysis

ACTION RT

(g) The meeting discussed the FOS referrals which are generally low however would be useful to obtain full information of FOS referrals and decision from providers.

(h) The MI received from POL was reviewed at the meeting including the VMW results, Training & Competence Report and CRM Report. The levels of QA available across different areas of the nextwork was discussed and the reasons for POL not being in a position to provide full oversight. The criteria for scoring and incentives were also discussed. It was agreed that as the MI from POL improved, greater value would be obtained.

RCC 16/26 **2ND LINE COMPLIANCE REPORT**

(a) The 2nd line compliance report for Travel was reviewed with commentary from EMM. EMM noted that January had seen a 47% reduction in complaints from last year. However EMM considered redress payments to be high and suggested these be reviewed in line with the review of the Complaints Handling process.

ACTION SH

(b) EMM reminded the meeting of the Add-on review recently conducted and that work had commenced on a vulnerable customer review.

ACTION KO (c) The Regulatory change log was reviewed. KO noted that a meeting was scheduled to review the impact of each area on the business and the log would be updated and circulated accordingly.

POL00423565

(d) The level of Financial Promotions was discussed. As this is currently still outsourced to Thistle, the resource requirements are unknown. A defined marketing plan would be useful to determine anticipated activity in this area.

RCC 16/27 **ISAG REPORT**

As EMG is absent for this meeting, ISAG content was deferred to the next meeting

RCC 16/28 **ANY OTHER BUSINESS**

There being no further business the meeting was closed

The next meeting of the RCC would be held on 14th April 2016 at 1pm.

…….. ……

Chairman **Date**