POL00423564

Risk & Compliance Committee Meeting
Friday 1 May 2015, 10:00 – 12:00
Boardroom 1.19 Wakefield, Finsbury Dials London

Dial in Details:
Freephone Number: GRO
Toll Number: GRO
Participant passcode: GRO

Members:	Jane MacLeod (Chair) Alisdair Cameron Neil Hayward Alwen Lyons Nick Kennett Paula Vennells	**Attendees:**	Gavin Lambert Garry Hooton Steve Miller Georgina Blair Martin George
Apologies:			

	Agenda Item	Purpose	Timing	Paper	Owner
1	Committee minutes and actions	Agree minutes of last meeting and review actions	10:00 – 10:05 5 minutes	One	Chair
2	Principles of risk management	Discuss and approve principles and implementation plan prior to submission to GE	10:05 – 10:20 15 minutes	Two	Steve Miller
3	Review of effectiveness of risk and internal controls framework	Discuss and approve review prior to submission to ARC	10:20 – 10:35 15 minutes	Three	Steve Miller
4	Principal risks	Review POL principal risks and risk management section of the Annual Report prior to submission to ARC	10:35 – 11:05 30 minutes	Four	Steve Miller
5	Risk incidents reporting process	Review and approve proposed reporting process	11:05 – 11:15 10 minutes	Five	Georgina Blair
6	Vulnerable customers update	Discuss approach to developing policy on vulnerable customers	11:15 – 11:25 10 minutes	-	Martin George
7	Review of policy approvals process	Review and approve proposed approach	11:25 – 11:35 10 minutes	Six	Steve Miller
8	Internal Audit Report	Review latest update from Internal Audit prior to submission to ARC	11:35 – 11:50 15 minutes	Seven	Garry Hooton
9	Gifts & Hospitality Annual Report	Review report	11:50 – 12:00 10 minutes	Eight	Georgina Blair

Papers for noting

10	ID Cards Policy	Note policy	-	Nine	John Scott
11	Information Security Policies (4)	Note policies	-	Ten	Julie George

POL00423564

RCC 1 MAY 2015 PAPER ONE

Post Office Ltd – Confidential

Risk and Compliance Committee (R&CC)		**Reference: R&CC March**
Date: 16 March 2015	**Venue: Boardroom, Finsbury Dials**	**Time: 14:00 – 16:00**
Attending:		
Jane MacLeod	General Counsel	Chair
Alisdair Cameron	Chief Financial Officer	Member
Neil Hayward	Group People Director	Member
Nick Kennett	Financial Services Director	Member
Gavin Lambert	Chief of Staff	On behalf of the CEO
Alwen Lyons	Company Secretary	Member
Steve Miller	Head of Risk - incoming	Observer
Arnout van der Veer	Head of Risk and Assurance - outgoing	Report
Georgina Blair	Risk Business Partner	Secretariat
Paul Beaumont	Risk Business Partner	Report
Garry Hooton	Head of Audit – incoming	Report
Apologies:		
Paula Vennells	CEO	Member

Introduction

The Chair declared the committee quorate and opened the meeting.

Agenda Item 1, Committee minutes and matters arising

The committee reviewed the minutes and actions from the last meeting.

The following amendments to actions were noted:
Action 1655 – Whistleblowing comms plan to be brought back to the next meeting.
Action 1649 – Commercial Director to give his view on vulnerable customers at the next meeting.
Action 1646 - Produce a paper on what the policy governance process should be (for May meeting).
Action 1645– Workshops no longer needed given the other risk assessment activity in place. Action to be closed.
Action 1631 – Head of Telecoms to confirm that he knows who is responsible for compliance in his team.

The committee agreed the minutes of the previous meeting and the attached actions subject to the amendments noted.

Agenda Item 2, Updated Terms of Reference & Rolling Agenda

The committee discussed the updated terms of reference. It was noted that there was inconsistency in the reporting from sub-committees to the RCC and the committee requested that an appropriate form of reporting was agreed with the chairs of the sub-committees (**Action 1656**).

The committee discussed the rolling agenda. The Head of Risk and Assurance explained that it was based on a meeting frequency of six times a year. It was noted that it had been intended for RCC meetings to coincide with Group Executive Team meetings, and to take up the last two hours of the GE meeting agenda, but that this was not yet possible due to current pressures on the GE agenda. The Committee noted that the timing of reporting from sub-committees needed to be clarified and that the risk team was working on an incident reporting process.

It was noted that there were a number of the scheduled items which could potentially include reports on POMS (eg. AML compliance). It was agreed that further discussion was required as to the interaction between POMS and POL on these items, given that the POMS board would also require assurance around these matters it was agreed that the Chair would discuss this with the Financial Services Director (**Action 1657**).

POL00423564

RCC 1 MAY 2015 PAPER ONE

Post Office Ltd – Confidential

The committee agreed the terms of reference and rolling agenda.

Agenda Item 3, POL risk management progress and key principles

The Head of Risk and Assurance introduced the risk management key principles, noting that fundamental parts of the principles were:

- A general review of risks and upward reporting to RCC and GE to take place twice a year
- A risk champion in a frontline role in each part of the business
- Management confirmation that the assessment of risks and controls is accurate (to start in September 2015).

The committee discussed the principles. The Group People Director noted that the risk management guidance (Paper 3, Appendix A) that had been issued by the risk team had been very useful to his team when they were considering their own risks. The committee requested that a risk management session be provided for the SLT at the next appropriate opportunity (**Action 1658**).

The committee endorsed the key principles.

Agenda Item 4, Key Risks for POL

The committee discussed the key risks. The committee noted that the aggregation of risks obscured their meaning and requested that they be disaggregated in order to provide greater transparency over the individual risk. The committee also asked that the likelihood and impact scores for each risk be reviewed (**Action 1659**).

Agenda Item 5, Business Transformation Assurance

The committee reviewed the proposed approach to Business Transformation Assurance. It was suggested that the hard reporting line for the two Business Transformation risk and assurance roles should be to the General Counsel and/or Head of Risk and the dotted line to the Head of Transformation, which is the reverse of the current situation. Chair and Head of Risk to discuss with the Transformation Director **(Action 1660).**

Agenda Item 6, Risk and Assurance at POMS

The committee discussed the papers.

Agenda Item 7, Internal Audit Plan 2015/16

The committee reviewed the Internal Audit Plan and requested some amendments (**Action 1661**).

Agenda Item 8, FOIA request on EUC tower – for noting

The committee noted the paper and that the FOI process is under review.

Agenda Item 9, Joiners, Movers and Leavers access policy – for noting

The committee discussed the paper and requested further investigation into the seriousness of the problem. Group People Director to review the external audit report on adherence to the joiners, movers and leaver processes. Head of Audit to provide external audit view to Group People Director (**Action 1662**).

Any other business

The General Counsel gave an update on Sparrow.

POL00423564

RCC 1 MAY 2015 PAPER ONE

Post Office Ltd – Confidential

Action Summary and Updates					
Date	**Ref**	**Action**	**Lead**	**By**	**Update**
03/15	1662	Provide external audit view on adherence to joiners, movers, leavers processes as referenced in Joiners, Leavers, Movers Policy to Group People Director.	Garry Hooton	1st May	Done – ACTION CLOSED
03/15	1661	Amend audit plan in accordance with feedback from committee members	Garry Hooton	1st May	Done – plan approved by ARC in March 2015 – ACTION CLOSED
03/15	1660	Discuss reporting lines of Business Transformation risk and assurance roles with the Transformation Director.	Jane MacLeod/ Steve Miller	1st May	Done – ACTION CLOSED
03/15	1659	Revise presentation of principal risks in line with feedback from committee members	Steve Miller	1st May	See agenda item 4
03/15	1658	Provide a risk management session for the SLT at the next appropriate opportunity	Jane MacLeod/ Neil Hayward	22nd June	
03/15	1657	Discuss interaction between POL and POMS with regard to reporting at RCC with Financial Services Director	Jane MacLeod	1st May	POMS RCC to report to POL RCC – format to be agreed.
03/15	1656	Develop proposal for sub-committee reporting to RCC and discuss at GE	Steve Miller/ Alwen Lyons	22nd June	
01/15	1655	Prepare and implement a communications plan to raise awareness of the whistleblowing line.	Steve Miller	22nd June	Whistleblowing framework currently under review. Action point carried forward to next meeting.
01/15	1653	Gather views from committee members on incident reporting de-minimis limits and provide an update.	Steve Miller	1st May	See agenda item 5
01/15	1652	Prepare note clarifying the current approach to compliance with new the Corporate Governance Code	Steve Miller	1st May	See agenda item 3
01/15	1649	Write to the Commercial Committee with the committee's comments on vulnerable customers, and request an update for the next meeting. **Updated March 2015**: Commercial Director to give his view on vulnerable customers at the next meeting.	Jane MacLeod	1st May	See agenda item 6

POL00423564

RCC 1 MAY 2015 PAPER ONE

Post Office Ltd – Confidential

12/14	1646	Provide a report on the list of policies that need to be approved. **Updated March 2015:** Produce a paper proposing an appropriate process.	Steve Miller	1st May	See agenda item 7
12/14	1644	Hold a scenario-analysis workshop to try and identify unexpected risks.	Steve Miller	22nd June	
10/14	1631	Brief the Telecoms team on the importance of registering risks and provide an update on training on regulatory matters and the allocation of accountability for compliance with General Conditions within the Telecoms team. **Updated March 2015**: Head of Telecoms to confirm he knows who is responsible for compliance in his team.	Geoff Smyth	1st May	Head of Telecoms has confirmed that he is the accountable individual within POL and provided the name of the accountable individual within Fujitsu. –ACTION CLOSED

POL00423564

Risk Management in Post Office

Implementing 'first line' risk capability

April 2015

POL00423564

Contents

POL00423564

The Three Lines of Defence Model 1:

The Post Office has adopted the **Three Lines of Defence Model** for risk management. This is the most common risk management structure implemented by complex organisations today.

The **First Line of Defence** is provided by employees and support functions in the businesses responsible for providing products and services and for execution of activities. The First Line of Defence has ownership and accountability for:

- Risk identification, assessment, mitigation, monitoring and reporting in accordance with established policies, procedures and guidance, and risk appetite.
- Ensuring appropriate and adequate capability for managing risk
- Implementing the requirements of the risk management principles in business areas.

The **Second Line of Defence** is provided by areas with independent oversight accountabilities such as in Central Risk Team, ISAG, Security functions. The Second Line of Defence:

- Establishes the risk management framework and underlying policies and procedures and provides risk guidance
- Provides oversight of the effectiveness of first line risk management practices
- Monitors and independently reports on the level of risk relative to stated risk appetite.
- Oversight of strategic risk through the Group Executive

The **Third Line of Defence** is primarily provided by Internal Audit and provides independent assurance to senior management, ARC and the Board on the effectiveness of risk management policies, processes and practices.

POL00423564

The Three Lines of Defence Model 2:

Group Executive Committee (and sub-committees), Audit and Risk Committee, Board of Directors

First line of defence

Risk Owners
- Business and their local support functions embedded in the business
- Risk assessments, incident reporting
- Reporting risk appetite metrics / scorecards
- Implementing the risk management principles

Second line of defence

Risk Oversight
- Establish risk management practice and provide guidance
- Provide oversight of the effectiveness of first line risk practices
- Monitor and independently report on the level of risk

Third line of defence

Independent Assurance
- Provided by internal audit
- Independent assurance to management and the Board of Directors on the effectiveness of risk management practice.

4

POL00423564

Risk management principles (presented to RCC 16 March):

These are basic requirements for meeting the UK Corporate Governance Code

	Risk Principle	First line responsibilities
1	**Sponsorship and ownership at the highest level**	• Demonstrate support and ownership of risk management by providing time and resource. • Allocate suitably senior resource for risk management to implement a first line risk function • Have a regular risk management discussion at LT meetings, attended by the central risk team as relevant.
2	**A dynamic process resulting in continuous improvement and mitigation of the risk inherent in the businesses**	• Have processes for tracking changes in the risk profile, made up from the risk assessments, risk incidents and key risk indicators (KRIs). • Develop timetable to assess business unit risks to meet bi-annual requirement, and using methodology provided by central risk team. • Apply risk assessment process to smaller units within business function based on risk exposure. • Develop a reporting process for incidents to the LT for discussion and then to the central risk team. • Monitor risk appetite metrics for relevant categories. • Demonstrate improvements in the risk profile over an agreed time horizon.
3	**Clearly articulated performance objectives aligned with the risk appetite**	• Use business objectives in the identification and assessment of risks. • Assess profile against appetite using risk appetite metrics.
4	**Factoring risk considerations into decision making**	• Include risk evaluation in investment decisions. • Assess risk evaluation against risk appetite • Ensure external testing against any risk based forecasting used for investment assessments.

POL00423564

Risk management principles (presented to RCC 16 March):

	Risk Principle	First line responsibilities
5	**A sound control culture**	• Review effectiveness of controls as part of assessing or reviewing risks. • Assess controls when reviewing risk incidents. • Implement SMART actions where controls are partially or not effective and allocate owners to actions. • Track action progress and report to LT
6	**Implementation and monitoring of risk and control improvements**	• Have appropriate control monitoring mechanisms in place (eg. metrics, action tracking, and control improvements). • Reduce risk exposure over time by improving control environment (see 5 above).
7	**The completion of the assessment of risks and control strategies twice a year including management representation.**	• Develop timetable to review and reassess top business unit risks to meet bi-annual requirement. • Develop a list of the key business controls, with owners and metrics for monitoring performance. • Validate and provide bi-annual management representation over the control framework and its operation (as per the UK Corporate Governance Code).
8	**Resourcing**	• Nominate a risk champion for each business unit (a risk champion must be a high enough grade to influence management effectively to implement the first line risk framework). • Risk champion to lead risk assessment, implementation of controls and monitoring of effectiveness. • Allocate time at LT meetings to discuss risks, incidents and metrics.

POL00423564

Building capability: the risk champion

Integrating risk management into ways of working and promoting effective risk management enables more informed decision making.

A critical success factor is building adequate first line risk management capability. The main agents for this are the **Risk Champions**.

The Risk Champion owns the delivery of the risk management process in specific areas or functions, but is not the risk owner. The Risk Champion does not have to be a risk expert but should possess a good understanding of risk management principles and be prepared to develop their skills through training and mentoring.

Key Risk Champion Responsibilities:

- Promote risk awareness and support the central risk function in the implementation of risk management framework.
- Representing risk management and team meetings
- Overseeing the inclusion of risk elements into any business area presentations to GE and Board
- Providing advice and guidance on risk management to colleagues and managers.
- Supporting the risk identification and assessment processes including completion of the business unit risk register, and ensuring risk reporting is delivered to timescale.
- Reporting incidents and risk appetite exposure metrics to the central risk team.
- Representing the business unit at risk forums and meetings.

POL00423564

Building capability: actions for first and second line

Action – for delivery by central risk team	Action – for delivery by GE / First line risk owners	Due date
	Announce adoption of risk management principles / three lines of defence model by GE	08-May-15
Develop training programme for first line risk capability		31-May-15
Develop incident management & key risk indicators reporting processes and guidance		31-May-15
	Allocate senior individual to be business area risk champion	31-May-15
	Include risk discussion on Lead Team agenda	31-May-15
Deliver training programme & roll out guidance documentation (risk assessments, risk incidents & key risk indicators) for first line risk champions		30-Jun-15
	Develop timetable to meet bi-annual risk assessment requirement.	31-Jul-15
	Implement incident and key risk indicator reporting processes	31-Jul-15
Review risk appetite and update as necessary Develop policy model and compliance oversight activity		31-Aug-15
	Develop list of key business controls, identify owners and metrics.	31-Aug-15
	Review control monitoring mechanisms (eg. metrics, action tracking)	31-Aug-15
Develop regular enterprise risk reporting & show trend on risk assessments		30-Sep-15
Review systems of risk management and internal control in each business unit, and representations from management		30-Sep-15
	Report progress against actions on exception basis to Lead Team	30-Sep-15
	Review effectiveness of controls as part of assessing or reviewing risks.	30-Sep-15
	Complete bi-annual risk assessment and annual representation on state of internal controls under the Corporate Governance Code	30-Sep-15
	Review requirement for more lower level risk registers within business unit	31-Oct-15
	Annual back test of assessments with incidents and metrics	31-Mar-16
	Link bi-annual risk assessments with risks to achieving business objectives	31-Mar-16

POL00423564

RCC 1 MAY 2015 **PAPER THREE**

RISK AND COMPLIANCE COMMITTEE

UK Corporate Governance Code: Annual review of the effectiveness of risk and internal control frameworks

1. Purpose

The purpose of this paper is to provide the Risk & Compliance Committee (R&CC) with an assessment of the extent to which Post Office has carried out the annual review of the effectiveness of risk and internal control frameworks required by the UK Corporate Governance Code.

2. Background

2.1 The UK Corporate Governance Code the states (at C.2.3) that in order to comply with the Code:
The board should monitor the company's risk management and internal control systems and, at least annually, carry out a review of their effectiveness, and report on that review in the annual report. The monitoring and review should cover all material controls, including financial, operational and compliance control

2.2 The old Turnbull guidance also required the board to review the effectiveness of the company's risk management and internal controls.

2.3 This review has not been undertaken in the past year, mainly due to disruption in the nature, focus and approach to developing a framework to comply with the code.

3. Current status

A top down view of current status is given by the table at Appendix A, which lists the questions boards should ask in completing a review (based on the most recent guidance – October 2014) along with

a) The response we would be able to make to the question based on existing status.
b) Current common practice in making a response as outlined by PWC.

4. Action

The Committee is asked to note:

4.1 We have not conducted a review this year.

4.2 That, prior to performing a full gap analysis against the risk management sections of the code, the attached schedule sets out a brief snapshot of position and current common practice in performing the annual review.

4.3 We have engaged with PWC to determine current best practice.

Steve Miller
1 May 2015

POL00423564

RCC 1 MAY 2015 **PAPER THREE**

The Code: Questions for board to consider in its annual assessment process

	Risk appetite and culture	Status	Common Practice (PWC)
1.	How has the board agreed the company's risk appetite? With whom has it conferred?	Appetite paper agreed by the Board in January 2015. Currently awkward to implement; more useful as statement of intent. There is an opportunity to re-present at the time of the interim statement and produce a more quantitative approach to facilitate assessing risk exposures.	The Board needs to satisfy itself that any potential breach of its appetite would be identified before it occurred; monitoring arrangements will need to be defined. Although not a requirement, the Board could consider disclosing risk appetite in the annual report and accounts. Defining the early warning indicators for principal risks, setting tolerance levels and monitoring metrics as part of the oversight conducted by Risk Committee and the Board.
2.	How has the board assessed the company's culture? In what way does the board satisfy itself that the company has a 'speak-up' culture and that it systematically learns from past mistakes?	The PO has a whistleblowing policy, code of conduct and key behaviours set out. Employees are represented by union leadership, and other representative organisations.	We are seeing many businesses defining the desired culture and associated behaviours in order to have a reference point for review, monitoring and taking action.
3.	How do the company's culture, code of conduct, human resource policies and performance reward systems support the business objectives and risk management and internal control systems?	There is a risk management policy and RCC has ToR setting out roles and responsibilities. Code of conduct refers to risk appetite.	Risk management accountabilities to be defined, agreed and communicated covering the Board, ARC, GE, Risk Function, Internal Audit, business areas, management and staff. Adjust performance management system to measure behaviours for individuals and rewards and sanctions determined as a result.
4.	How has the board considered whether senior management promotes and communicates the desired culture and demonstrates the necessary commitment to risk management and internal control?	Board, ARC and GE refer risk management approach in PO and desire for improvement in risk framework; including the design and implementation of an enterprise risk management framework.	See point 2 above
5.	How is inappropriate behaviour dealt with? Does this present consequential risks?	Disciplinary process and policies.	There may indeed be consequential risks although unaddressed inappropriate behaviour will have a bigger risk impact

POL00423564

6.	How does the board ensure that it has sufficient time to consider risk, and how is that integrated with discussion on other matters for which the board is responsible?	ARC / Board timetable. Strategic risk – policy on articulating strategic risks in update papers for the board.	The Board (as a minimum) should debate the following on an ongoing basis: - The strategic risk profile, transformation risk profile - Horizon scanning for emerging risks - Deep dive on all strategic/principal risks - Risk management maturity and progress of how the risk framework is being embedded across the business - Risk appetite and risk appetite breaches - The effectiveness of controls in place to manage key risks - The extent, source and effectiveness of assurance over the risk management and internal control system and key controls
7.	**Risk management and internal control systems**		
8.	To what extent do the risk management and internal control systems underpin and relate to the company's business model?	Strategy papers and updates require an outline of the key risks. The internal control system is embedded in the policies, procedures and processes used to manage the day to day activities of the PO. These are designed to facilitate effective and efficient operation of the processes required to achieve the PO business objectives, and to respond effectively to risks. There are gaps in reporting effectiveness and efficiency of control operation to provide management with sufficient oversight and transparency of the control systems.	The key here is if risk management is appropriate and proportionate to the business model and the extent of inherent risk the business model presents. The annual assessment could consider a statement on proportionality and relevance. In addition this also asks how risk management is embedded in strategic planning and the relationship to strategy and objectives. This poses questions about what the strategy is, and how risks have been identified and assessed. Does risk identification and assessment coincide with strategy setting, does strategy formulation determine the need for risk assessment and do we monitor changes in the business environment that impact strategy?

POL00423564

9.	How are authority, responsibility and accountability for risk management and internal control defined, co-ordinated and documented throughout the organisation? How does the board determine whether this is clear, appropriate and effective?	Risk policy, RCC ToR. Local policies for control ownership and management. RCC / ARC review and sign off on key control and risk management policies.	Clear risk management accountabilities should be defined, agreed and communicated across the Business covering the Board, ARC, GE, Risk Function, Internal Audit, Business Divisions, management and staff. These accountabilities form an essential component of the risk management framework and should be agreed by the Board and GE.
10.	How effectively is the company able to withstand risks, and risk combinations, which do materialise? How effective is the board's approach to risks with 'low probability' but a very severe impact if they materialise?	A POL wide risk assessment has been undertaken, and the results presented to GE. Further work on evaluating mitigating actions was prepared as a result.	The Code asks for an assessment of risks that happen at the same time (risk in aggregation) so scenario analysis should be considered which should include high impact low probability risks. The Code also requires inherent and residual assessment of risk to determine the extent of control effectiveness. Deep dive risk reviews should consider this specifically.
11.	How has the board assessed whether employees have the knowledge, skills and tools to manage risks effectively?	Risk owners periodically called to committees to discuss risk and actions for incidents	The risk framework document is key and when agreed, communicated across the business. Training should be provided on the framework. The Board should consider Internal Audit's role in providing assurance over the application of the framework and receives reports on this as part of their annual assessment.
12.	What are the channels of communication that enable individuals, including third parties, to report concerns, suspected breaches of law or regulations, other improprieties or challenging perspectives?	Whistleblowing policies.	Outside the formal process of whistleblowing, this is really down to culture and how open communication is being encouraged. Are there other communication channel exist and are these being used effectively?
13.	How does the board satisfy itself that the information it receives is timely, of good quality, reflects numerous information sources and is fit for purpose?	ARC / Board timetable. Strategic risk – policy on articulating strategic risks in update papers for the board.	See point 6 above

POL00423564

14.	What are the responsibilities of the board and senior management for crisis management? How effectively have the company's crisis management planning and systems been tested?	Crisis management procedures and business continuity policy	How frequently tested?
15.	To what extent has the company identified risks from joint ventures, third parties and from the way the company's business is organised? How are these managed?	External commissioned review of recent joint ventures (Titan – Grant Thornton). Clear procedures for risk with third parties (BoI) and engagement.	
16.	How effectively does the company capture new and emerging risks and opportunities?	Bi-annual risk assessment process. Risk assessed in strategic plans.	
17.	How and when does the board consider risk when discussing changes in strategy or approving new transactions, projects, products or other significant commitments?	See above. Change / projects / commitments; new business transformation assurance processes, staff and activities.	Explicit articulation of risk and reward to be included in the investment approval process to aid Boards decision making.
18.	To what extent has the board considered the cost-benefit aspects of different control options?	Currently this has been at a strategic level.	The Code requires Board to assess the effectiveness of material controls to manage principal risks and whether fit for purpose and operating as intended. POL will need to consider conducting detailed control optimisation work around key controls and processes.
19.	How does the board ensure it understands the company's exposure to each principal risk before and after the application of mitigations and controls, what those mitigations and controls are and whether they are operating as expected?	Risk registers by area assessed on net basis. Controls and actions recorded on register and presented to GE.	This is a key element of the Code's requirements around principal risks. The framework must consider risk, cause and consequence, inherent assessment, existing controls and control effectiveness, residual exposure, the need for addition mitigation to manage risk to tolerated levels. Also see point 18 above as understanding control effectiveness and control optimisation is a key part of the spirit of the Code

POL00423564

20.	**Monitoring and Review**		
21.	What are the processes by which senior management monitor the effective application of the systems of risk management and internal control?	Little control performance data currently. Incidents / events have been reported at past RCC. No regular risk profile created. No regular maturity analysis reported.	We are seeing internal audit including review of risk management application and effectiveness as part of Internal Audit plan. The Board should consider what this assurance needs to look like. This is supplemented by reports from the risk function on framework application. An 'assurance map' outlining the key sources and effectiveness of assurance over key controls is increasingly common place in large organisations.
22.	In what way do the monitoring and review processes take into account the company's ability to re-evaluate the risks and adjust controls effectively in response to changes in its objectives, its business, and its external environment?	A number of false starts in getting a common practice have taken place. Risk profile data has been sporadic, as has assessment of effectiveness of controls. Recent assessment does asses controls; further work required on validation.	The risk functions prepare a set of questions for the Board, ARC and Risk Committee to ensure effective challenge. Re-evaluation also needs to consider the implications of changes in risk appetite and tolerance. The Risk Committee and Board should also monitor the early warning metrics defined for each of the principal risks
23.	How are processes or controls adjusted to reflect new or changing risks, or operational deficiencies? To what extent does the board engage in horizon scanning for emerging risks?	See point 22 above.	See point 22 above. The Risk Committee should debate emerging risks as a standing agenda item and report the findings of this review to the Board bringing key issues to their attention.

POL00423564

24.	**Public reporting**		
25.	How has the board satisfied itself that the disclosures on risk management and internal control contribute to the annual report being fair, balanced and understandable, and provide shareholders with the information they need?	Draft annual disclosures in process.	The Code is requiring specific disclosure in a number of areas: - Acknowledge that the Board is responsible for the risk management system and reviewing its effectiveness and disclose that there is an on-going process in place - Report on the review of the risk management system, the effectiveness, main features, any significant failings and actions taken to address them - The extent to which the system accords with the Code - Report that a robust assessment of the principal risks has been conducted (also required by the Companies Act 2006) - Disclose the principal risks and their mitigation, ensuring risk descriptions are sufficiently specific to understand how it might affect the entity
26.	How has the board satisfied itself that its reporting on going concern and the longer term viability statement gives a fair, balanced and understandable overview of the company's position and prospects?		

POL00423564

Appendix A: Principal Risks

	Risk Title	Risk Description	Actions	Underlying risks
A	Risks to underperformance in income	Threats to market share, sales, profitability, and cost base rely for mitigation on managing a number of variables with critical dependencies. • MI quality and accuracy fails to provide adequate information for decision making. • Organisational inability to respond quickly and effectively to opportunities and threats • Competitors erode market share across all target product areas • Lack of effective and timely product and service development; offer to partners and customers not sufficiently attractive • Strategy not aligned with key partners (RMG, BOI) • People capability and capacity insufficient to meet market challenges. • Lack of effective and timely technological response means network changes do not deliver expected increases in profitability (e.g. Front Office deployment)	• Trading Committee and Commercial Committee review performance and Marketing/Sales action plans regularly • Sales pipeline and performance measure ratios in place and embedded at all levels to reinforce sales model • Improved performance management process deployed in crowns • Streamlined and clarified performance measures ownership and improved decision making processes • Programmatic approach introduced for network sales activities and sales capability • New crown area manager structure deployed • Digital and Data Revenue plan for 15/16 being deployed and 3 year plan in development • Training and rollout of Customer Relationship Managers and deployment of Guiding Coalition in agency branches • Project to develop short term financial MI solution • Mails strategy review • End to end review of customer experience/journeys for each product • Effective stakeholder plans and governance processes for key partners • Product Profitability Programme to optimise profitability by product across all pillars	8, 9, 11, 13, 14, 16, 17 PR2, PR4, PR7
B	Transformation not delivered in full	Cost savings may be delayed or not achieved, or overall service compromised. • IT replacements and upgrades not timely leading to increased costs or infrastructure failure • Inaccurate investment assessments lead to costly errors in new product / customer solutions or structural changes • People capability / capacity inadequate to deliver plan or compromised by industrial action	• Embed risk management in programme. Transformation assurance plan. • Create design framework for FO application • Review reward structure and develop PO vision and change narrative • Re-invest in systems • Communicate change requirements and implement IR strategy • Project to develop short term financial MI solution • Roll out improved proposition across branch network	1, 2, 3, 4, 7, 9, 14, 17 PR1, PR2, PR3, PR4, PR5, PR6, PR7, PR9, PR11, PR14

POL00423564

Appendix 1: Principal Risks

	Risk Title	Risk Description	Actions	Underlying risks
C	External environment	A change in political administration may change the shareholder's view of POL. • Uncertainty over the availability of funding beyond 2017/18 • Support required for changes in network transformation ('Cliff') may risk industrial action • Stakeholders are unclear surrounding the limits to commercial sustainability for a public purpose Post Office • Ability to respond to evolving shareholder request	• Include solvency requirements for identified critical risk exposures • Communicate change requirement to stakeholders • Implement IR strategy; secure Unite agreement • Planning for new government with investment case	5, 7 PR5, PR6
D	Operational / Legal / Regulatory risks	Post Office operates under an extensive and varied regulatory environment, and is increasing the size and scope of the heavily regulated financial services business (which includes direct FCA authorisation). • Regulatory/legal breaches or failures in the operational control framework lead to financial and/or reputational loss. • Risk of aggressive FCA enforcement; potential for disaffected 'whistle-blower' in high change environment triggers FCA investigation • High change environment may compromise manually based control framework	• Upload historic contractual information into new system and review • Clarify approach to policy setting and strengthen central compliance management • Review ISAG policy set and plan compliance programme • Improved contract management	6, 10, 12, 15
E	Market, macro-economic and environmental risks	Changing market developments, competitors response and changing consumer needs may lead to a mis-directed strategy. • Response to market (product design and delivery) may not be adequate or timely enough to prevent loss of market share • BOI financial position may change and restrict support of POL • Network propositions to retailers not commercially or operationally attractive; restrictions policy impacts on potential multiple partners	• Work with BOI to minimise any limitations on growth • Build negotiation strategy and modelling • Roll out CRM and develop improved customer experience • Guiding coalition of agency mails specialists to be deployed to increase mails sales • Roll out improved proposition across branch network. • Stronger focus on and improvements to retailer proposition	11, 13, 14, 16, 17

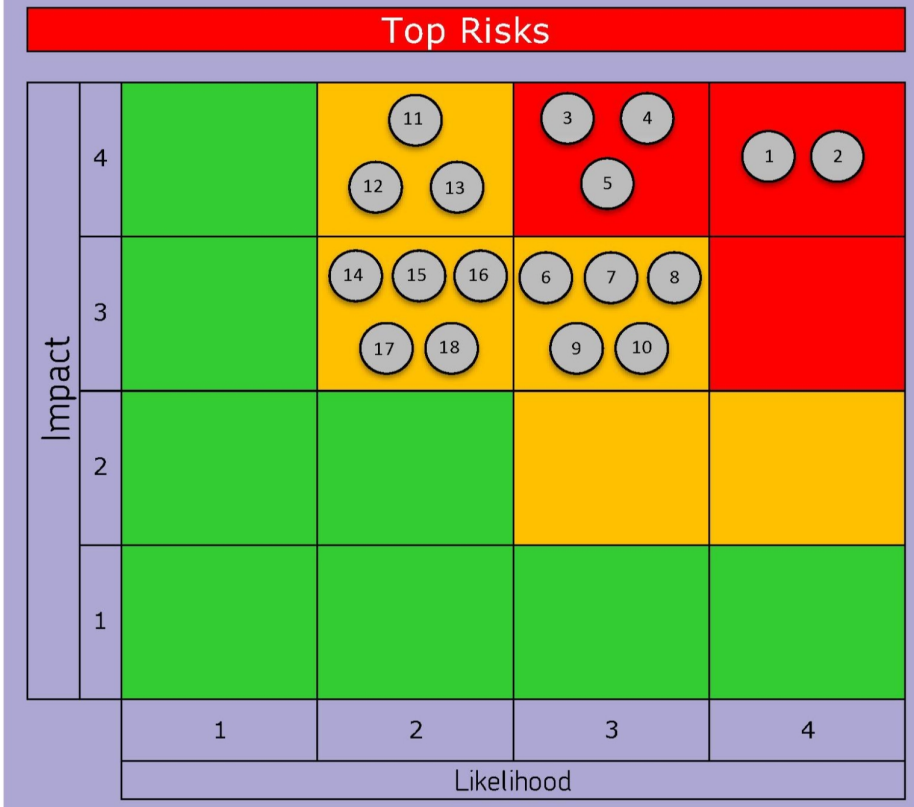
POL00423564

Highest rated risks from business area risk registers

	Risk	Category	Score	Owner	Principal Risk
1	Delivery of new Front Office application delayed	Operational	16	Lesley Sewell	B
2	People capability and capacity are inadequate to deliver the strategic plan	Strategic	16	Neil Hayward	B
3	Business transformation doesn't deliver objectives	Strategic	12	Transformation Cttee	B
4	Failure of infrastructure and application environments	Operational	12	Lesley Sewell	B
5	Unintentional breach of contractual terms	Legal	12	Jane MacLeod	D
6	Government funding is insufficient to enable POL to operate until 2018	Financial	9	Al Cameron	C
7	Risk of strike action	Operational	9	Neil Hayward	B, C
8	Risk of doing too much in a competitive field (FS)	Strategic	9	Nick Kennett	A
9	Poor quality financial data and inadequate evaluation processes results in sub-optimal investment decisions	Financial	9	Al Cameron	A, B
10	Non-compliance with law and regulation	Legal	9	Jane MacLeod	D
11	BoI financial situation will not provide capability to support POL	Strategic	8	Nick Kennett	A, E
12	Inadequate controls around the management of information result in a breach of company data	Legal	8	Jane MacLeod	D
13	Ineffective relations and agreement with Royal Mail	External	6	Martin George	A, E
14	Proposition to agents/retailer becomes unattractive (leading to unsustainable network)	Operational	6	Kevin Gilliland	A, B, E
15	FS mis-selling risk: non-compliant product distribution, design or marketing or tougher regulation	Legal	6	Nick Kennett	D
16	Loss of market share in mails due to inability to respond quickly to market developments leading to loss of revenue	Strategic	6	Martin George	A, E
17	Delivering customer experience and propositions that customers want	Operational	6	Martin George	A, B, E
18	Risk that sales capability fails to deliver on FS growth targets	Financial	6	Nick Kennett	A

POL00423564

Highest rated risks from business area risk registers: Heat Map



Risk		Impact	Likelihood	Score
1	Delivery of new Front Office application delayed	4	4	16
2	People capability and capacity inadequate to deliver plans	4	4	16
3	Business transformation doesn't deliver objectives	4	3	12
4	Failure of infrastructure and application environments	4	3	12
5	Gov't funding not sufficient to continue operations	4	3	12
6	Unintentional breach of contract terms	4	3	12
7	Risk of strike action	3	3	9
8	Risk of doing too much in a competitive field	3	3	9
9	Financial data and evaluation gives sub-optimal investments	3	3	9
10	Non compliance with law or regulation	3	3	9
11	BoI financial situation not capable of supporting POL	4	2	8
12	Inadequate control of information	4	2	8
13	Ineffective relations and agreement with RMG	4	2	8
14	Parts of network become non-viable	3	2	6
15	FS miss-selling	3	2	6
16	Loss of market share in Mails	3	2	6
17	Delivery of marketable customer propositions	3	2	6
18	Failure to deliver on FS growth targets	3	2	6

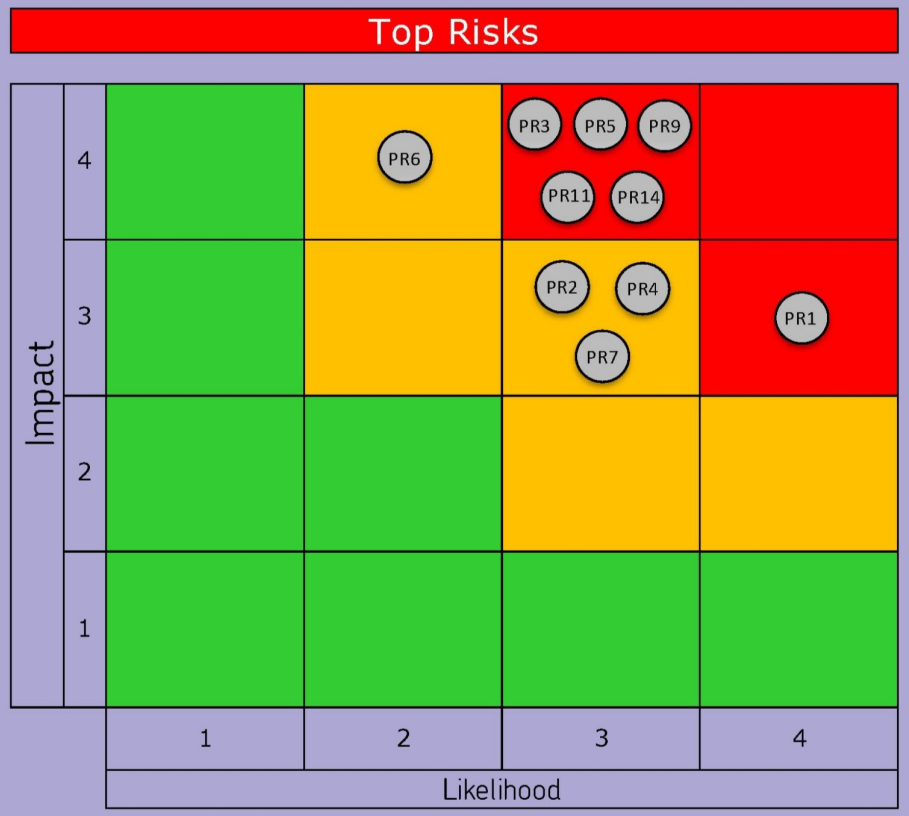
POL00423564

Highest rated risks from the Transformation Portfolio risk register

ID	Risk	Category	Score	Owner	Principal Risk
PR1	Transition Legacy IT Landscape	Operational	12	Lesley Sewell	B
PR3	Manage complexity of change (capability)	Operational	12	Neil Hayward	B
PR5	CWU/Unite don't buy in to organisational change	Stakeholder	12	Neil Hayward	B, C
PR9	Strategic Objectives misalignment	Strategic	12	David Ryan	B
PR11	Transformation function not designed and operating effectively	Strategic	12	David Ryan	B
PR14	Benefit realisation (including Success Criteria)	Strategic	12	David Ryan	B
PR2	Manage volume of change (capacity)	Operational	9	Neil Hayward	A, B
PR7	Competitive threat	Strategic	9	Martin George	A, B
PR4	Shareholder Agreement (Misalignment between programme and shareholder objectives)	Strategic	9	David Ryan	A, B
PR6	National Federation Sub Postmaster (NFSP) disrupts service	Stakeholder	8	Neil Hayward	B, C

POL00423564

Highest rated risks from the Transformation Portfolio risk register



Risk		Impac	Likelihoo	Scor
PR1	Transition Legacy IT Landscape	3	4	12
PR3	Manage complexity of change (capability)	4	3	12
PR5	CWU/Unite don't buy in to organisational change	4	3	12
PR9	Strategic Objectives misalignment	4	3	12
PR11	Transformation function not designed and operating effectively	4	3	12
PR14	Benefit realisation (including Success Criteria)	4	3	12
PR2	Manage volume of change (capacity)	3	3	9
PR7	Competitive threat	3	3	9
PR4	Shareholder Agreement (Misalignment between programme and shareholder objectives)	3	3	9
PR6	National Federation Sub Postmaster (NFSP) disrupts service	4	2	8

POL00423564

Business risk 2014/15

The information below details the key business risks, their potential impact and how the Post Office manages them.

Risk Title	Impact	Mitigation
Risks to underperformance in profitable income Post Office faces both opportunities and threats to profitable income. The mails and parcels market remains intensely competitive and has seen some high profile market failures due to inadequate margins. Government Services are impacted by increased use of digital channels in an environment of reduced public spending.	Inability to reduce reliance on government subsidy.	The business strategy is customer focussed embracing new market and technological developments (a number of which feature in the Annual report) Focus developments are aligned to key business accelerator areas. Regular monitoring of business performance is undertaken by the General Executive and Board.
Business Transformation not delivered in full Savings may be delayed or not achieved, or overall service compromised due to inadequate capability, capacity and scale of change or withdrawal of support from stakeholders.	Project costs may have to be written off. Any major project issues would damage reputation.	A new programme management office is being established and assurance and oversight enhanced. There are detailed plans in place to manage the transformation and ensure it is delivered within budget and on time. A comprehensive engagement programme with unions, staff and postmasters is in place to engage our people in our vision and strategy.
IT development programmes not delivered in full IT replacements and	Project costs may have to be written off. Any major project issues	A new design framework is being created for the Front Office application, and will be subject to the

POL00423564

Risk Title	Impact	Mitigation
upgrades not timely leading to increased costs or infrastructure failure	would damage reputation	transformation assurance plan. Oversight will be embedded in the new programme management office.
Operational / Legal / Regulatory risks The Post Office operates under an extensive regulatory environment, including areas such as financial and postal services, procurement, competition law and data security. This environment continues to evolve, particularly in the financial services arena and we need to ensure that the changing requirements continue to be identified and met.	Customer losses and inconvenience. Fines, financial losses, regulatory censure or litigation. Loss of ability to trade in certain markets or products.	Our corporate services team works closely with the relevant business owners in identifying new requirements. Training and development of staff on the requirements. Regular compliance tests and monitoring are conducted. External review by regulatory principal for financial services business.
Market, macro-economic and environmental risks. Market developments, competitors' response and changing consumer needs are changing at a faster pace. The 2015 actuarial valuation of the RMPP is due to complete shortly and there is a risk, given market conditions, that the cost of the scheme will rise substantially	Parts of the strategic plan may become outdated and sub optimal.	Post Office is working closely with commercial partners to meet market and technological developments and to roll out an improved customer experience throughout all distribution channels. Business diversification gives Post Office different response options if there are significant threats to one business area.
Strategic development and sustainability Costs of social responsibilities impact the ability to create	Balancing conflicting purposes may impact operational efficiency and reduce our ability to become commercially	Communication of changes with stakeholders including investment case and identification of solvency requirements for

POL00423564

Risk Title	Impact	Mitigation
commercial sustainability. Stakeholders are unclear surrounding the limits to commercial sustainability for a public purpose Post Office; withdrawal of support from our staff or postmasters could cause delays and limit our ability to meet business objectives Ability to respond to evolving shareholder requests in a fluid macro-economic and market environment.	viable enterprise.	critical risk exposures. Comprehensive engagement programme with unions, staff and postmasters and events to involve our people in our vision and strategy.

POL00423564

RCC 1 MAY 2015 PAPER FOUR APPENDIX C

PO Annual Report 31 March 2015

Risk Management

Risk Governance

The Post Office Board is responsible for the risk management and internal control systems in the Post Office, and for determining the nature and extent of significant risk. Responsibility for day-to-day operations is delegated to the General Executive. The risk management and internal control systems are based upon what the board considers to be appropriate to the Post Office activities and are designed to manage rather than eliminate the risk of failure to achieve the Post Office strategic objectives and expansion in its chosen markets. The risk management and internal control systems provide reasonable, but not absolute, assurance against material misstatement or loss.

The board confirms there is an on-going process of identifying, evaluating and managing the significant risks face by the Post Office, and that this has been in place for the year under review and up to the date of approval of the annual report and accounts.

The year ahead will see further evolution of the framework to ensure it continues to meet requirements and support the aims of the strategic plan and transformation of the Post Office.

Risk Management Framework

In order to deliver its objectives the Post Office is required to identify, assess and manage a wide range of risks. These are managed through an overarching framework in order to apply consistency and transparency of risk management across the organisation. The framework identifies roles and responsibilities of key parties in the risk management process, the policies for how risks are managed, the tools and processes used and the reporting outputs that are generated.

Risk governance

Oversight of risk management is carried out by the Audit and Risk Committee on behalf of the Post Office Board. The Risk and Compliance Committee provides oversight on behalf of the Group Executive Committee over the risk management framework including the risk management policy and the management of the key risks for Post Office. This Committee is chaired by the General Counsel and reports to the Group Executive Committee. The Committee comprises members of the Group Executive Committee, including the Chief Executive and the Chief Financial Officer.

Progress

The Group Executive Committee has identified and manages the top risks in the organisation, focusing on those that affect the 2020 strategy. These risks, with their response plans, are reviewed at the Risk and Compliance Committee and the Audit and Risk Committee to assure the robustness of risk assessment and management.

POL00423564

Risk Appetite

The Post Office has articulated and agreed a series of risk appetite statements with associated metrics with a view to provide clarity to the organisation in terms of taking risks in managing new opportunities and/or the management of existing risks.

Business Continuity

As part of the Post Office approach to risk management, the Post Office brings together a wide range of business continuity arrangements throughout the Group under one central policy and governance framework to ensure that the business is capable of withstanding any significant threat to its on-going operations. The Post Office is committed to ensuring its business has adequate resilience and planning that protects its customers, clients, brand and reputation from business continuity threats, risks and incidents.

POL00423564

RCC 1 MAY 2015 **PAPER FOUR**

RISK AND COMPLIANCE COMMITTEE

Review of principal risks

1. Purpose

The purpose of this paper is to update the Risk & Compliance Committee (R&CC) on the review of Post Office's principal risks for the 2014/15 Annual Report.

2. Background

The principal risks which were first presented to the RCC meeting in March were substantially revised in line with members' feedback and discussed at the GE meeting on 16 April 2015. Further changes have been made after discussions with risk owners and an updated version of the principal risks is presented in Appendix A. POL's principal risks for inclusion in the 2014/15 Annual Report have been updated accordingly (see Appendix B) and a revised risk section for the Annual Report has been drafted (see Appendix C).

3. Action

The Committee is asked

1. To review the revised principal risks in Appendix A,
2. To review the proposed principal risks for the Annual Report in Appendix B
3. To review the proposed wording of the risk section for the Annual Report in Appendix C.

Steve Miller
1 May 2015

POL00423564

RCC 1 MAY 2015 PAPER FIVE

RISK AND COMPLIANCE COMMITTEE

Risk incident reporting process

1. Purpose

The purpose of this paper is to update the Risk & Compliance Committee (R&CC) on the proposed incident reporting process.

2. Background

Risk incident data can provide information on the effectiveness of controls and the likelihood that risks will materialise. Guidance on identifying and reporting risk incidents has been produced by the central risk team for use by front line risk champions (see Appendix A). This guidance was tested with a selection of front line risk champions and amended in response to their feedback.

A number of risk incidents were gathered by members of the central risk team and some examples are included in the guidance. Once the risk incident reporting guidance is embedded and operating risk champions will report incidents to the central risk team, and the most significant will be reported to the Risk and Compliance Committee. Risk incident owners may be requested to attend the RCC to discuss the actions taken as the result of an incident.

3. Action

The Committee is asked to approve the proposed incident reporting process.

Georgina Blair
1 May 2015

POL00423564

RCC 1 MAY 2015 PAPER FIVE

Appendix A

Risk Incident Reporting at Post Office

A Practical Guide

The purpose of this document is to provide:

- An explanation of how to identify a risk incident
- An outline of the risk incident reporting process

POL00423564

RCC 1 MAY 2015 PAPER FIVE

1.0 Introduction

Collecting risk incident data is an important part of understanding Post Office's risk profile. While a risk assessment helps to identify risks and the controls in place to manage them, risk incidents and indicators provide information on the effectiveness of controls and the likelihood that risks will materialise. When a risk incident occurs it is often because a control has failed or is absent. Identifying and discussing the causes of risk incidents is an important part of developing a proactive risk culture within Post Office.

'Toolbox' element	What it means
Risk assessment	Assessment of risk and mitigation (controls)
Risk incidents	Examples of individual risks materialising (quantitative data)
Key risk indicators (KRI)	Trend data about related indicators risks (quantitative data)

Key reasons for recording risk incidents

- To learn lessons from what has happened and to identify mitigating controls to help prevent a similar incident from happening again.
- To treat it as an opportunity to improve our processes and to reduce operational risk exposure and drive value for the Post Office.
- To understand the root causes and establish whether other areas of the organisation could have an exposure.

2.0 Definition of a risk incident

Post Office's risk management framework defines as risk incident as:

Any event which causes or may cause an interruption to or reduction in the quality of a service, or which causes financial loss, or any other operational failure.

Some examples of incidents are listed in the table in section 3 below. Not all risk incidents need to be reported to the central risk team. Once a number of incidents have been reported the central risk team will produce some guidance on de minimis limits but until then please report any incident you feel provides some information about missing or inadequate controls, or which may have implications for other areas of the business.

Note that reporting a risk incident is in addition to the normal management process for dealing with each type of incident; this process does not replace any existing reporting process.

POL00423564

3.0 Reporting a risk incident

Risk champions in each business unit are responsible for reporting risk incidents to the central risk team. When reporting an incident the following details should be included:

- nature of the incident
- impact (financial or otherwise)
- management action taken/planned
- details of the incident owner

The central risk team will review each report and determine whether the incident should be discussed at the next Risk and Compliance Committee (RCC) meeting. Risk incident owners may be invited to come to the RCC to explain the actions taken as the result of an incident and to help identify lessons which can be learnt in other parts of the business.

Figure 1 Examples of risk incidents

Event	Cause	Impact	Actions
Customer contacted to inform that after registering for Post Office Home Phone they received a confirmation email containing their full bank details.	Incorrect process within the service.	Moderate risk of regulator taking action.	ISAG investigation on-going with project team.
Post Office Money Website launch on 5 January contained numerous landing page errors	Sub optimal implementation plan. Incomplete UAT.	Key website errors fixed within 24 hours. Errors made some of the website FCA non-compliant for this period as well as being confusing for customers.	Digital team have met and undertaken a lessons learned exercise. They assess that lessons will be learnt prior to next major exercise (re-brand 30 July) with many of the changes already implemented .
Robbery by intruder who hid in branch and appeared after office closed. 6th Dec 1pm South Norwood	Failure to check office and retail area before closing the branch.	Loss of £103,764 Trauma to staff who were locked in the safe until released by police	Branch visited - security hardware failures found. Considered suspicious as similar to previous incident
Failure to meet the requirements of disabled customers at two separate Crown Offices	Unable to reach the pin pad/ unable to enter the branch due to lack of ramp. No clear business strategy on how to meet the needs of disabled customers	Brand & reputation damage as widely covered in the media including TV coverage Minister of State for Disabled People noted the event and wrote to CEO to raise concerns	Tethered pin pads to be installed in Crown branches/ possibility of installation of ramp being investigated Post Office diversity/disability strategy group to be established

POL00423564

Policy Governance in Post Office

1. Purpose

To define and explain the framework within which company policies are developed, approved, updated and communicated.

2. Scope

Applies to all company-wide policies which impact all or the majority of: management, staff, key operations and relationships with third parties.

3. Overall principles

Business areas (Directorates) are responsible for developing draft policy in areas they own. The Risk and Compliance Committee (R&CC) will review all finalised policies before submitting them to the Post Office Executive Committee (ExCo) for approval.

3.1 Policy development and drafting

Each business area is responsible for developing the policies required by their area. Each policy requires a senior policy owner who is able to affect and substantially influence the policy and take responsibility for its outcome.

Business areas must consult all key stakeholders (including Risk and Internal Audit) during the drafting process. A policy template is available from riskandcompliance@ GRO

Each policy should:

- Reflect a high level view
- Refer to supplementary documents for processes and detailed procedures
- Be subject to version control
- Include review dates and details of how to update the policy.

3.2 Approval of policies

All finalised draft policy documents should be submitted to the R&CC for approval.

The R&CC will review policies either in session or by e-mail and determine whether the ExCo needs to approve the policy overall or note it as approved by the R&CC.

3.3 Communication and publication of policies

Once approved, the policy owner is responsible for ensuring all relevant parts of the business are made aware of the policy by using appropriate communications channels and will be published on the Corporate Policies Sharepoint site. Policy owners should ensure there are processes in place to communicate policy to new joiners and contract staff where relevant.

3.4 Revision to policies

Minor changes or updates to approved policies after review should be notified to the R&CC. At each meeting the R&CC will receive a list of all policies that were notified during the preceding period.

Major re-writes to policies need to go through the draft approval process as for a new policy.

The Risk and Compliance Committee
August 2013

POL00423564

RCC 1 MAY 2015 **PAPER SIX Appendix B**

Appendix B

List of policies and other documents which should contain a reference to POL's risk appetite.

The risk team will work with each policy owner to determine a suitable timeframe for reviewing the policy, including appropriate consideration of risk appetite and reverting to the committee where appropriate.

Name of policy/ other documentation	Risk appetite category	Policy owner
Acceptable social media use guidance	Stakeholder	Martin George
Atos Service Management Report	Technology	Lesley Sewell
Audit reports (internal / external / third party)	Operations	Gary Hooton
Code of Business Standards	Legal & Regulatory; People; Stakeholders	Neil Hayward
Data security/management incidents (ISAG and Atos)	Operations	Julie George
Financial (credit, market, liquidity) risk standards	Financial	Alisdair Cameron
Information security policy	Technology; Operations	Julie George
Investment / new product assessment / project assessments	Customer; Market; Financial	David Ryan
ISAG Incident Register	Technology; Legal & Regulatory	Julie George
Outsourcing due diligence procedure	Technology; Operations	Alisdair Cameron
Outsourcing policy	Technology; Operations	Alisdair Cameron
Procurement policy	Financial; Technology; Operations	Alisdair Cameron
Recruitment policy (including staff vetting)	People	Neil Hayward
Security policy	Financial	Alisdair Cameron
AML Policy	Legal & Regulatory	John Scott

POL00423564

RCC 1 MAY 2015 **PAPER SIX**

RISK AND COMPLIANCE COMMITTEE

Review of policy approvals process

1. Purpose

The purpose of this paper is to update the Risk & Compliance Committee (R&CC) on the operation of the policy approvals process in Post Office over the past year and to suggest improvements to the process.

2. Background

The R&CC approved a policy governance framework in August 2013 (see Appendix A). The framework states that all policies are to be reviewed by the R&CC prior to submission to ExCo for approval or noting, and gives guidance on the content of policies.

3. Review of the process

In the year to 31 March 2015 only one policy was presented to the R&CC for approval (and it did not receive approval) and the Committee has not received updates of any minor revisions to policies during the year. Five policies have been submitted to this meeting.

4. Actions planned

In order to match the approach to the resources available the central risk team has identified a number of policies and other documentation in the business which should contain reference to risk appetite. Risk business partners will work with policy owners to review and update the policies and other documentation accordingly (see list of policies and other documentation in Appendix B).

There is a more substantive piece of work to be completed. This includes defining a suite of top-down policies for management of specific types of exposure (Legal, HR, Security etc.) and developing appropriate implementation, compliance and oversight arrangements. This includes communication of policy governance requirements to the wider business and a review of the existing policy suite. This will require dedicated resource from within Corporate Services which has currently not been identified.

5. Action

The Committee is asked

1. To approve the proposed approach to the review of policy governance,
2. To agree the policies submitted for approval
3. To approve the approach to phased implementation of risk appetite via the list of policies attached.

Steve Miller
1 May 2015

POL00423564

Post Office Internal Audit RCC Report – April 2015

1. What we will do - Next 3 Months

Audit	Sponsor	Comments	Fieldwork Timing	Completion
Management Information	**Alisdair Cameron**	• Integrity and reliability of information / data. • Date of initial planning meeting to be confirmed.	May	July
Drop and Go (Lessons)	**Martin George**	• Lessons learnt and NPD lifecycle review. • Initial planning meeting held with Mark Siviter.	May	June
Telecoms	**Martin George**	• Mobile offering readiness review to inform GE decision on launch. • Initial planning meeting held with the Head of Telecoms.	July	September
Assurance Framework	**Jane MacLeod**	• Assessment /review of the assurance providers within PO. • Terms of Reference drafted and shared with Risk team.	On-going	August
IT Towers delivery on-going assurance review	**Lesley Sewell**	• Cross towers governance and programme management. • Towers (EUC and potentially FO at the moment) programme governance, risk mng, obligations, etc. • Terms of Reference drafted.	On-going	-
Fujitsu exit	**Lesley Sewell**	• Controls and mechanisms in place to control Fujitsu services and minimize exit cost.	May	July

POL00423564

Post Office Internal Audit RCC Report – April 2015

2. Work in Progress.

Audit	Key Findings	Status (24/04)
Contract Management	• Supplier contract portfolio is not fully known. • Contract Management Framework (CMF) remains in draft (since its development in 2012) and requires further development, finalisation and implementation. • Staff have the ability to define their own roles and responsibilities. • Management are unable to effectively foresee and manage expiration of contracts. • Analysis and management of risks to drive contract management.	• Findings workshops held. • Draft report issued to Colin Stuart for management comment. • Wave 2 and changes in management have delayed responses.
Financial Crime	• Staff are not clear on where and how to report suspicions or concerns. • Effective mechanisms to prevent and detect fraud and corruption are not incorporated into policies, procedures and systems. • Focus of proactive / reactive activity is directed towards customers and customer facing areas of the business. • There is no corporate / PO wide approach. • Concerns regarding potential internal staff fraud have been flagged for further investigation (outside of the audit)	• Fieldwork complete and findings shared with management. • Drafting report. • To be reported to ARC in **May**.

POL00423564

Post Office Internal Audit RCC Report – April 2015

2. Work in Progress Cont.

Audit	Emerging Findings	Status
Conduct Risk (FS)	• There is no compliance (2nd line of defense) function over sighting the Financial Service operations. • Management have not developed a comprehensive Conduct Risk strategy covering all the customer touch points and selling channels.	1. Fieldwork in progress. 2. Audit team is working with PWC financial conduct / regulatory specialists under the co-source. 3. To be reported to ARC in **July**.
IT Towers Delivery On-going Assurance	• Fieldwork commenced	

POL00423564

Post Office Internal Audit RCC Report – April 2015

3. Other Matters.

Area	Comments
Treasury	Memo has been shared with Treasury management which summarises concerns relating to arrangements relating to bank accounts currently out of scope of Treasury identified during routine audit activity.
Change Management	An update has been shared on stakeholder management within the new Change process.
Travel	A significant number of staff are not yet using Capita for hotel and travel bookings. Instead they are claiming for these expenses through the SAP system. This is allowing the daily overnight rate to be exceeded (there are instances where this has exceeded £200). In February 2015, contrary to the Expenses Policy a total of £10K (380 claims) was claimed for train tickets and £3.2K (46 claims) on overnight accommodation via SAP. There is a concern that PO are not getting the best value out of travel bookings with repeated examples, where staff have reclaimed over £350 for daily travel. The Travel Manager (new) is looking into the reasons for this. The HRSC is also contacting travellers with over £50 spend. Ultimately, Line Managers are signing off on such claims inappropriately and encouraging the wrong behaviours. This could be a cultural issue which needs to be gripped.
Business Transformation	One FTE Internal Audit resource has been allocated to support independent Business Transformation Assurance activities (currently away sick). An approach to delivering independent assurance has been drafted and is in the process of being socialised and agreed with stakeholders. Additional short term Business Transformation assurance needs will be identified through engagement between the programme, Risk and Internal Audit during April.

POL00423564

High overdue actions (audits 2013-2015)

	Audit	Action	Assigned to	Forecast Completion Date	Progress
1	**Business continuity**	Prepare and issue BC guidelines to GE / Top management	Corporate Services –Risk Team	Nov 2014	Guidelines are ready for issue
2	**Identity and access**	Access rights review control needs to be deployed for all PO domain accounts	IT & Operations – Dave Hulbert	Jan 2015	Closed with condition agreed with Roger Middleton
3	**Identity and access**	Ensure there is an overview of all access rights per user.	IT& Operations – Dave Hulbert	Feb 2015	Closed with condition agreed with Roger Middleton
4	**Identity and access**	There is a plan to move to Category base assess rights linked to Role once the EUC tower is in place	IT & Operations – Dave Hulbert	June 2015	Still open- follow on-going
5	**Identity and access**	Movers access review control needs to be implemented	IT & Operations – Dave Hulbert	Feb 2015	Completed
6	**Software Licensing**	PO needs to define a Software Licensing management policy defining the roles and responsibilities for PO, SI and suppliers related to licenses	IT & Operations – Dave Hulbert	Jan 2015	Completed
7	**Software Licensing**	SISD will define a SLM process and procedures to manage the licenses on PO behalf	SISD	Feb 2015	Completed
8	**Software Licensing**	PO will define its assurance and governance process around the SISD SLM process. Clear key performance measurements on SLM process needs to be defined.	IT & Operations – Dave Hulbert	Feb 2015	Completed

POL00423564

RCC 1 MAY 2015 **PAPER EIGHT**

RISK AND COMPLIANCE COMMITTEE

Annual report on operation of the Gifts and Hospitality procedure

1. Purpose

The purpose of this paper is to update the Risk & Compliance Committee (R&CC) on the operation of the Gifts and Hospitality procedure in Post Office over the past year.

2. Background

Post Office has had a Gifts and Hospitality procedure in place as part of its anti-bribery procedures since June 2011. The Anti-Bribery Policy and associated gifts and hospitality procedure were reviewed and approved by the Risk & Compliance Committee in January 2014. Employees are required to provide details of all gifts over £25 and all instances of hospitality, accompanied by evidence of their line manager's approval, to the Risk team by e-mail to riskandcompliance@postoffice.co.uk.

3. Review of the register

In the year to 28 February 2015, 14 reports of gifts and 190 reports of hospitality received were made to the register. In the previous year, 23 reports of gifts received and 154 reports of hospitality were made (see appendix 1 for a breakdown by business unit). In 2014/15 Financial Services made the largest number of reports: 3 gifts and 85 reports of hospitality received. There was one report of hospitality declined during the year.

4. Need for Improvements and Actions planned

Preparation for this year's report appeared to reveal under reporting in some areas compared to last year. Financial Services and Commercial were asked to check their records for details of the gifts and hospitality received in the last financial year. Further reports were received from Financial Services but members of the Commercial team did not provide any further reports, and the number of incidents of gifts and hospitality reported by the Commercial team in the year remain low compared to last year.

Actions planned by the Risk team to improve reporting:

4.1 an e-mail reminder will be sent to colleagues to remind them of the gifts and hospitality reporting procedures

4.2 the information on the intranet will be refreshed.

5. Action

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

Georgina Blair
1 May 2015

POL00423564

RCC 1 MAY 2015 **PAPER EIGHT**

Appendix 1

Summary of reports to the Gifts and Hospitality register in the year to 28 February 2015 and a comparison for the year to 28 February 2014

Area	1 March 2014 to 28 Feb 2015				1 March 2013 to 28 Feb 2014			
Business Unit	Total Reports of gifts received	Total Reports of hospitality received	Reports of gifts received by GE members (incl in totals)	Reports of hospitality received by GE members (incl. in totals)	Total Reports of gifts received	Total Reports of hospitality received	Reports of gifts received by ExCo members (incl in totals)	Reports of hospitality received by ExCo members (incl. in totals)
Communications	1	0						
Commercial		3			3	16		
Corporate Services		27		2	2	18		
CoSec					3			
Finance	1	13	3	4	1	21		10
Financial Services	3	85	1	29		46		1
P&E					2	2		
IT and Change	2	25	2	14	5	15	5	14
Network & Sales	7	18		3	6	19		1
Office of the Chief Executive		19		19	1	17	1	17
Total	14	190	6	71	23	154	6	43

There were changes in some business units eg IT and Change[i] during the year and in the membership of ExCo to GE members[ii] as from 1 February 2015. The report reflects where the membership remained for most of the year.

[i] IT and Change reports include Information Security for the year
[ii] GE members' reports include the IT & Operations Director for the year

POL00423564

RCC 1 MAY 2015 **PAPER NINE**

Post Office ID Cards Policy

Document Control

Overview

Owner:	Head of Security	Enquiry point:	Head of Security
Version:	1.1	Effective from:	01 May 15
Last updated	09 Apr 15	Last review date:	
Review period:	Annually or major change		

Revision History

Version	Date	Author	Changes
0.1	21 Jan 14	Terry Folkman	Initial draft
0.2	30 Jan 14	Terry Folkman	Changes to para 4 & 10
1.0	11 Jun 14	Julian DiMauro	Approval received from Exco 22 April 14, version updated.
1.1	09 Apr 15	Diana Maddox	Inclusion of different colour ID cards for contractors and visitors

POL00423564

1 Purpose and Statement

The purpose of this Policy is to set out the framework for managing the use of Post Office ID cards within Post Office cash centres, stock centre, depots and central support sites.

2 Goals

The goals of this Policy are to:

- Protection and safeguard of people and assets.
- Define the management of ID Cards.
- Ensure that all Post Office employees, agents/SPMR and contractors are aware of the framework for the management of ID Cards.

3 Scope

This Policy applies to all areas of Post Office unless an exception is granted following the process explained in Section 7. This Policy does not apply to directly outsourced service providers or suppliers.

4 Roles and Responsibilities

The Head of Security has responsibility for ensuring the integrity of the physical security of Post Office. Day to day deployment will be via the operational line.

All employees and contractors employed within Post Office central support sites, cash centres and depots also have a responsibility to ensure that only bona fide individuals are permitted access to these locations and that all personnel display the correct ID card.

5 Policy Statement

ID cards are an integral part of the defence in depth approach that the Post Office employs in order to minimise crime and business loss, whilst protecting people and assets at its cash centres, depots and central support sites. To that end, every individual, whenever they are on Post Office property or part of a property that houses Post Office assets, must display a Post Office ID card. This card, if not handed back in when the individual leaves the Post Office property or property that houses Post Office assets, must be removed from public view.

There are three colours of ID cards:

- white photographic ID card for Post Office employees and white non-photographic ID card for "staff"
- lavender (lilac) photographic ID card for all contractors
- Post Office red non-photographic ID card for all visitors.

5.1 Service Provider

POL00423564

The Post Office will provide photographic ID cards for Post Office employees and contractors and non-photographic ID cards for visitors and visiting "staff". Appropriate electronic access rights will be granted to these cards as necessary in accordance with the Post Office ID Card management procedure and the Post Office Identity and Access Card Application Form and Contractor Access Card Application Form. Non-photographic ID cards for visitors will not have any electronic access rights whereas non-photographic visiting "staff" ID cards may afford limited electronic access rights.

The service provider is to contact Post Office line managers before employee and contractor ID cards expire. This will allow sufficient time for a new ID card application to be processed and will act as a form of ID card audit.

When ID cards are reported to the service provider as lost, stolen or destroyed, the service provider will immediately remove any electronic access rights and record the ID card as lost, stolen destroyed. Additionally, the service provider is to maintain records of all issued, destroyed or lost ID cards and is to provide Post Office with these details on a monthly report.

5.2 Cash Centres and Depots

All Post Office employees employed at a cash centre or depot are to be issued with a photographic ID card, which may also act as an electronic proximity access control card. Post Office employees are to display this ID card at all times whilst at the cash centre or depot.

All visitors to cash centres or depots, including individuals who visit in order to carry out work, but not including Post Office employees and contractors who ordinarily work at a different Post Office location to the cash centre or depot they are visiting, are to be issued with a Visitors ID card by the service provider at the access control point. This ID card carries no photograph but must still be displayed at all times when the visitor is at the cash centre or depot and must be handed back before the visitor leaves. Visitors are to be escorted at all times.

Visitor's hosts are responsible for the visitor whilst they are on Post Office property. Therefore, it is the host's responsibility to ensure visitor compliance with this Policy.

All Post Office employees and contractors who visit a Post Office cash centre or depot, but do not ordinarily work at that cash centre or depot, are to display their normal Post Office photographic ID card for the duration of their visit.

The loss of any type of Post Office ID card is to be reported immediately to the service provider.

5.3 Customer Support Centres

All Post Office employees and contractors are to be issued with a photographic ID card, which may also act as an electronic proximity access control card. Post Office employees and contractors are to display this ID card at all times whilst on Post Office property.

POL00423564

All visitors to customer support centres, including individuals who visit in order to carry out work, but not including Post Office employees and contractors who ordinarily work at a different Post Office location to the one they are visiting, are to be issued with a Visitors ID card by the service provider at the access control point to the individual properties or at the access control point to the Post Office area of the property. This ID card carries no photograph but must still be displayed at all times when the visitor is on Post Office property or in a Post Office area of a building and must be handed back before the visitor leaves the property or the area. Visitors are to be escorted at all times.

Visitor's hosts are responsible for the visitor whilst they are on Post Office property. Therefore, it is the host's responsibility to ensure visitor compliance with this Policy.

All Post Office employees and contractors who visit a different Post Office site to the one that they ordinarily work at are to be issued a "Staff" ID card. This ID card carries no photograph but must still be displayed at all times when the visitor is on Post Office property or in a Post Office area of a building and must be handed back before the visitor leaves the property or the area.

The loss of any type of Post Office ID card is to be reported immediately to the service provider.

5.4 Line Manager Responsibility

Line Managers are responsible for ensuring that all expired photographic ID cards and ID cards from all employees and contractors leaving Post Office employment are recovered and destroyed. These ID cards are to be recorded as returned and destroyed locally in accordance with the Post Office Leavers Checklist.[1] Line Managers' are responsible for informing the service provider that the ID cards have been destroyed. Line Managers' are also responsible for informing the service provider whenever an ID card is lost.

6 Compliance

Compliance with this Policy is mandatory and will be assessed as part of both internal and external audit and reported upon to the Post Office Security Governance Forum (SGF).

7 Exceptions

As per standard policy process, a policy exception must be obtained from the Head of Security. The appropriateness of these exceptions will be considered and reviewed by the Head of Security on an annual basis or other appropriate defined period. Evidence must be retained for the exception and the annual review.

8 Violations

[1] Post inception of Grapevine 2014 all expired/returned ID cards will be reconciled and destroyed by the service provider in order to provide a more accurate audit trail.

POL00423564

Failure to comply with this Policy or any documents referred to within this Policy constitutes a violation of this Policy.

9 Enforcement

The SGF will regularly assess for compliance against this Policy. Any violation of this Policy will be investigated and if the cause is found to be due to wilful disregard or negligence, it may be treated as a disciplinary offence. All disciplinary proceedings may be progressed in accordance with the Post Office Code of Conduct coordinated through HR.

10 References

Post Office ID and Access Card Application Form
Contractor Access Card Application Form
Post Office Leavers Checklist

POL00423564

POST OFFICE INFORMATION SECURITY ACCEPTABLE USE POLICY

POL00423564

Acceptable Use Policy

Document Control

Overview

Owner:	Head of Information Security and Assurance Group	**Enquiry point:**	ISAG
Approved by:		**Effective from:**	
Version:	0.5	**Last updated:**	

Revision History

Version	Date	Author	Changes
0.1	09/11/2014	Andrew Watson	Initial draft release
0.2	21/11/2014	Andrew Watson	Second release post ISAG review ad feedback
0.3	24/11/2014	Andrew Watson	Additional changes post feedback from DP team
0.4	26/11/2014	Andrew Watson	Changes post feedback from ISAG Senior Risk and Compliance Manager
0.5	11/02/2015	Andrew Watson	Changes made to reflect comments / feedback. A summary of which are provided in Policy Review Tracker and details provided back to ISWP through document mark-up
0.6	19/02/2015	Andrew Watson	As above

Reviewers

Version	Date	Reviewer	Comments
0.1		ISAG	Mark-up contained within document
0.2		DP Team	Mark-up contained within document
0.3	26/11/2014	Brian Harrison	Mark-up contained within document
0.4		ISWP	Feedback from ISWP contained within Policy review tracker
0.5		ISWP	Feedback from ISWP contained within Policy review tracker

Quality Control	Next review date
This document is subject to periodic review and will be reviewed at least annually or where there are significant changes to the business and/or its operating environment.	02/12/2015

POL00423564

Acceptable Use Policy

Table of Contents

POL00423564

Acceptable Use Policy

POL00423564

0. Terms and Abbreviations

Terms used throughout this document are described at the end of this document in Appendix A.

1. Introduction

The intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to supporting a culture of openness, trust and integrity. Post Office is committed to protecting its Employees, customers, Third Party Supply Chain and Information Assets from damaging or illegal actions by individuals, either knowingly or unknowingly. Post Office enables this through the development and deployment of Policies, Standards and Guidelines which are aligned to international best practices. Effective Cyber and Information Security is a team effort involving everyone in Post Office.

2. Purpose

The Information Security Acceptable Use Policy defines a set of business rules governing fair and acceptable use of Post Offices' Information Assets. This document is supported by the Information Security Handbook (##REF Handbook) which provides guidance for the effective implementation of this policy.

3. Scope

This policy applies to anyone working for or on behalf of Post Office, including, where applicable, Third Party Supply Chain.

Policy

4. Protection of Information Assets

4.1. Information Assets

4.1.1. Products purchased by an Employee then paid for by Post Office will be considered Post Office owned and are subject to Post Office policy.

4.1.2. Products purchased by an Employee which are approved for the processing, storage or transmission of Post Office Information and/or connection to Post Office Information Assets will be considered to be BYOD Devices (see 4.4) and are subject to Post Office policy.

4.1.3. Users remain responsible at all times for the protection of Post Office Information Assets and must not disclose corporate Information outside of approved agreements.

4.1.4. Users must adhere to the requirements of this policy and the Information Security Handbook (##REF Handbook).

4.2. Information Classification

4.2.1. Documented Information created for and on behalf of Post Office must follow the Control of Documents Procedure (##REF CoD).

4.2.2. All Information must be identified and classified in accordance with one of the following four classification levels. Strictly Confidential, Confidential, Internal or Public.

POL00423564

4.2.3. All Information must be handled and protected in line with its classification level as set out in the Information Security Handbook (##REF Handbook).

4.2.4. All Information classified above 'public' must be protected when transferred externally as set out in the Information Security Handbook (##REF Handbook).

4.3. Portable or Removable Media

4.3.1. Information stored on removable media must only be retained for as long as absolutely necessary and destroyed when no longer required (see 4.5).

4.3.2. Post Office Information must not be transferred to personal Removable media (see 4.4) without prior written authorisation.

4.3.3. Removable Media Devices must be protected against unauthorised access during transportation and must be sent using recorded delivery (i.e. a traceable service) as set out in the Information Security Handbook (##REF Handbook).

4.4. Bring Your Own Device (BYOD)

4.4.1. BYOD Devices may require software installation, configuration or other controls as set out in the BYOD standard (##REF BYOD standard).

4.4.2. BYOD Devices will be subject to auditing, logging and monitoring (see section 11) requirements as set out in the BYOD standard (##REF BYOD standard).

4.4.3. BYOD Devices are subject to Incident Response procedures, may be subject to digital forensics procedures and may be obtained by authorities if suspected of illegal activity.

4.4.4. End Users are liable for Post Office Information stored, processed or transmitted on BYOD Devices and must comply with this policy and the Information Security Handbook (##REF Handbook).

4.4.5. Post Office accepts no liability for loss, damage or corruption of BYOD Devices.

4.5. Information Retention and Destruction

4.5.1. All Post Office Information must be retained in accordance with the Information retention standard (##REF Post Office Data Retention Standard).

4.5.2. Information must be destroyed at the end of the retention period in line with their classification and corresponding destruction guidelines (##REF Handbook).

4.6. Clear Screen Policy

4.6.1. Information Assets must have the screen locked before leaving them unattended.

4.6.2. Privacy screens must be used when working in public areas.

4.6.3. Due care must be taken to protect the processing of confidential Information (see 4.2).

5. Access Management

5.1. Identity and Access Management

5.1.1. Post Office issues User ID's for the purpose of obtaining authorised access to Post Office Information Assets which must, at all times be unique to you (i.e. not shared with a group of Users) and must never be shared.

5.1.2. User ID's and passwords are confidential (see 4.2.2), must only be used for sanctioned activities and/or communications and must never be written down or stored either electronically or on paper, transmitted via email or another unsecured communication.

POL00423564

5.1.3. Any attempt made to obtain your User ID, password or Physical ID (see 6.1) either written or verbal must be reported (see 9.2).

5.2. Password Requirements

5.2.1. Strong passwords are required for securing Post Office Information Assets. Refer to the guidance (##REF Handbook) on creating strong passwords.

5.2.2. Post Office staff will never ask you for your password. Never reveal your password to anyone, even if they claim to be from Post Office or an authorised Third Party Supply Chain member.

5.2.3. Usernames and/or passwords used to access Post Office Information Assets must never be the same as those used for non-Post Office environments (for e.g. personal websites, Devices, email systems, social media).

5.3. Remote Working

Anyone wishing to work remotely (i.e. not in Post Office premises) must:

5.3.1. Adhere to the Information classification scheme and ensure that Post Office Information Assets are physically protected (see section 6).

5.3.2. Maintain discretion whilst conducting business voice communications (e.g. telephone calls) especially when the contents of the call are confidential.

5.3.3. Connect to Post Office's network using an approved method (##REF InfoSec Manual)

5.3.4. Never download, install or use any software (see 7.1.1 & 7.2.3), other than authorised software and/or security updates/patches on Post Office Information Assets when or if prompted to do so when working remotely.

5.4. Remote IT Support

IT support or service desk, will as required, need remote access to Post Office Information Assets to resolve issues, in all cases:

5.4.1. Users must ensure that all documents are saved and that all Information and applications are closed prior to allowing a remote IT connection, and;

5.4.2. Users must accept the incoming remote support request and remain with the Device throughout the duration of the connection.

6. Physical Security

6.1. Physical Access

6.1.1. Employees and where applicable Third Party Supply Chain members will be issued with Physical IDs which must be displayed at all times in line with the requirements set out in the (##REF ID Card Policy).

6.1.2. Post Office visitors and Third Party Supply Chain members must be escorted and issued with a temporary Physical ID, in line with the ID Card Policy (##REF ID Card Policy).

6.1.3. The sharing of Physical IDs is not permitted.

6.1.4. Employees and Third Party Supply Chain members are obliged to observe local security requirements and must not attempt to enter Post Office Premises by back doors, windows, service and goods entrances or any means, other than via the main Office entrance.

POL00423564

6.1.5. Unauthorised physical access to IT equipment within Post Office buildings, including but not limited to, wiring/network closets, server/computer rooms, wiring high rises, is strictly prohibited.

6.2. Clear Desk Policy

6.2.1. Classified documented Information must be kept clear of desks and working areas and locked away when not in use, or destroyed by shredding.

6.2.2. Devices must be stored securely or fastened to a desk using a Kensington lock (or similar lock).

7. Acceptable Use

End Users are required to read the Information Security Handbook which contains the required guidance to comply with this policy including the acceptable use of Post Office Information Assets (##REF Handbook).

7.1. Malicious Software

Websites (included trusted sources) can knowingly or unknowingly be harbouring malware which will attempt to trick the visitor into installing it onto the connecting Device. To protect Information Assets:

7.1.1. Users must never install, attempt to install software or modify software settings.

7.1.2. Users must never override or attempt to override any Post Office software running on the Device, e.g. anti-virus software.

7.2. Internet

7.2.1. Users must not visit websites that contain racist, pornographic, obscene, hateful or other objectionable material and must not make or post indecent remarks, proposals or materials on the Internet.

7.2.2. Users must not Anonymise (i.e. hide their identity or attempt to avoid detection or monitoring), bypass or attempt to bypass Post Office web content controls or intentionally interfere with the normal operation of Post Office Information Assets and will not take any steps that substantially hinder others in their use of Post Office Information Assets.

7.2.3. Users must not upload or download unauthorised software to or from the internet, infringe copyright (see 8.2) or execute or accept any software programs or other code from the internet (see 7.1).

7.3. Email and Instant Messaging

7.3.1. Users must not send, forward or store material and/or attachments containing images, video, sound, text or other materials considered indecent, pornographic, illicit obscene, defamatory or discriminatory or which is intended to annoy, harass, or intimidate another person and will not present personal opinions as those of Post Office.

7.3.2. Users must appropriately protect all Information with a security classification (see 4.2) above 'Public' (##REF InfoSec Handbook)

7.3.3. Users must not use personal e-mail systems (e.g. Gmail, Hotmail, Yahoo) for Post Office business; this includes forwarding business related emails to personal email addresses.

7.3.4. Emails sent or received are retained and stored as permanent records and instant messaging conversations may be stored as permanent records. Use of email and

POL00423564

instant messaging is logged and monitored (see Section 11) and all related records may be accessed by Post Office.

7.4. File Transfer and Storage

7.4.1. Post Office Information must be transferred using business sanctioned methods only. The use of unauthorised application/web/cloud based file transfer and/or file storage services are strictly prohibited (e.g. DropBox, SkyDrive, iCloud).

7.4.2. Access to and/or use of known illegal file sharing applications/web sites or other services is strictly prohibited (e.g. warez sites, torrents, P2P/Darknet or streaming services).

7.5. Social Media

Social media sites, applications and technology including but not limited to: social networking websites, applications, blogs, community sites, integrated social media and chat forums are collectively referred to as 'Social Media' and are subject to the following requirements:

7.5.1. Users must follow Post Office guidance covering the appropriate use and best practices for using social media (##REF Handbook).

7.5.2. Users must not send or receive any material which is obscene, defamatory or discriminatory or which is intended to annoy, harass, or intimidate another person and will not present personal opinions as those of the Post Office.

7.5.3. Anyone publishing Post Office Information using Social Media, for or on behalf of Post Office, must be authorised and approved and may only publish Information classified as 'Public' (see 4.2).

7.5.4. Anyone publishing Post Office Information using Social Media, for or on behalf of Post Office, which is classified as 'Internal' (see 4.2) must be authorised and approved and the content of the Information must be controlled, approved and released by Post Office.

7.5.5. Information classified as 'Confidential' or 'Strictly Confidential' must never be published using Social Media.

7.5.6. Misuse, data leakage or any other contravention of this policy must be reported immediately following incident reporting procedures (see 9.2).

7.5.7. The use of Social Media is monitored by Post Office and authorised third parties (see section 11).

8. Software Use

8.1. Installing and Configuring Software

8.1.1. All requests for software and applications must be formally made through the service desk.

8.1.2. Users must not download, install or attempt to install unauthorised or unlicensed software or attempt to modify software or application settings.

8.2. Copyright

8.2.1. With the exception of personal data (as defined in the Data Protection Act 1998) Employees should not have any expectations of ownership or privacy in relation to Post Office Information.

8.2.2. Copying (including duplicating and any other variant of the copying concept) of anything (whether a document, digital asset, software, or anything else) other than in line with UK and international copyright law is explicitly forbidden.

POL00423564

8.2.3. Post Office Information Assets must not be used to store, process or transmit pirated materials, including but not limited to films, videos or music. Piracy is a breach of copyright law and is illegal.

9. Business Continuity

9.1. Backup

9.1.1. Post Office provides automated backups for Business Information Systems and Applications (for e.g. E-mail, SharePoint, Network / Shared Drives). Users must ensure they have a working backup of Information stored on Post Office Devices and/or approved BYOD Devices (see 4.4). Refer to the backup section of the Information Security Handbook for further guidance (##REF Handbook)

9.1.2. Backups of Post Office Information must only be performed to Post Office Information Assets (i.e. not personal computing equipment including but not limited to personal removable media)

9.2. Incident Management

9.2.1. Post Office maintains and manages incidents in accordance with the Incident Management framework (##REF ISIM FMWK). If anyone becomes aware or suspects that an incident is occurring, or has occurred, they must report it immediately to the Service Desk on 0330 123 0778.

9.2.2. An incident is defined as:

- Suspected, perceived, or actual loss, alteration or disclosure of Post Office Information Assets.
- Suspected, perceived or actual attacks on Post Office Information Assets whether or not an attack was successful in corrupting, deleting or stealing Information.
- Attempted or successful installation of malicious software on Post Office Information Assets.
- Accidental loss of Information Asset functionality, or any accidental event that leads to the loss of Availability or Integrity of Post Office Information.
- Any event that leads to the potential compromise of the Confidentiality of Post Office Information.

9.2.3. Everyone must support the activities and investigations of the Information Security Incident Response Team (IS-IRT).

9.2.4. User must not communicate any details concerning any past or ongoing incident to any person external to Post Office, without explicit instructions from Post Office (see 10.4).

9.3. Lost or Compromised Information Assets

Lost, stolen or compromised Information Assets, including but not limited to: Post Office Devices (see 4.1), Portable or Removable Media (see 4.3), BYOD (see 4.4), Physical IDs (see 6.1) or User IDs (see 5.1) present a risk to Post Office. If an Information Asset is lost or stolen or a User suspects it may have been used to gain unauthorised access then Users must:

9.3.1. Report it immediately (see 9.2).

9.3.2. Change all potentially impacted passwords.

9.3.3. Activate any available functionality to 'remote-wipe' the Device where such functions are available.

POL00423564

9.4. External Communications

9.4.1. Communications with external parties (e.g. press, media, news agencies, reporters, law enforcement, legal or regulatory bodies) must be authorised and approved by Post Office. Unauthorised external communications are strictly prohibited.

10. User Management

10.1. Acceptance of Information Assets

10.1.1. Users will be supplied with Information Assets (for e.g. Physical ID's, User ID's, laptop, desktop, BlackBerry, tablet, smart phone) required to perform their role.

10.2. Return of Information Assets

10.2.1. Users are required to return Information Assets upon termination of their employment or contract. Additionally, Post Office reserves the right to retrieve any asset at any time.

10.2.2. Users are required to remove all Post Office Information from BYOD Devices when requested and upon termination of employment or contract.

10.3. Information Security Training and Awareness

10.3.1. Post Office will periodically develop Information Security and Awareness training which must be completed by all Users.

10.3.2. Anyone involved in the processing or personal data or card holder data must complete Information Security and Awareness training prior to handling this Information.

11. Monitoring

11.1.1. Post Office monitors the use of and access to or from its Information Assets.

11.1.2. Unauthorised monitoring of Post Office Information Assets, communications or personnel is strictly prohibited.

11.1.3. Post Office reserves the right to access, read, review, modify, monitor and copy all Information and may access and/or disclose the contents of any Device including BYOD Devices (see 4.4).

11.1.4. Users accessing personal services (e.g. banking, shopping) do so at their own risk. Post Office Information Assets are monitored and Post Office accepts no liability for personal Information which might be obtained and/or corrupted as a consequence.

12. Compliance and Non-Compliance

12.1. Compliance

12.1.1. All Users have a duty of care to ensure compliance with corporate policies, contractual agreements and applicable laws or regulations.

12.1.2. Requests for personal data under the Data Protection Act 1998, known as Data Subject Access Requests, must be directed to Post Office's Information Rights Team foiteam GRO

12.1.3. Requests for Post Office Information under the Freedom of Information Act 2000 must be directed to Post Office's Information Rights Team foiteam GRO

12.1.4. Post Office may periodically audit any business areas against corporate policies, procedures or standards to ensure on-going commercial, legal or regulatory compliance.

POL00423564

12.1.5. Use of Post Office's Information Assets implies acceptance of these conditions and the conditions set out in this policy.

12.1.6. Use of BYOD Devices for processing, storing or transmitting Post Office Information and/or connecting to Post Office Systems or Applications implies acceptance of these conditions and the conditions set out in this policy.

12.2. Non-Compliance

12.2.1. Lost, stolen or compromised Information Assets must be actioned immediately, in accordance with the requirements set out at section 9.3 of this policy. Any delay will be treated as a breach of this policy.

12.2.2. Sharing of Physical IDs and/or User IDs is a breach of this policy.

12.2.3. Evidence of misuse and/or unauthorised activity is a breach of this policy.

12.2.4. All breaches or misuse cases will be logged and investigated and could lead to disciplinary action (see 15). Evidence of illegal activity will be reported to the appropriate authorities.

13. Exceptions

All policy exceptions must be obtained in writing from Post Office's Information Security and Assurance Group (ISAG). Exceptions will be considered by ISAG at the time requested and reviewed thereafter on an annual basis. Evidence must be retained for both the exception and the annual review. For further Information please contact: isag[redacted] GRO

14. Violations

Compliance with this policy is mandatory. Post Office provides Information Security and Awareness Training at Induction and at least annually thereafter and will regularly assess compliance against this policy.

Any violation of this policy will be treated as an incident. A breach of this Policy could lead to disciplinary action in accordance with the Code of Conduct (##REF CoC) with the possibility of termination of employment.

15. References

This document has the following references:

- Information Security Handbook
- Control of Documents Procedure
- ID Card Policy
- Code of Conduct

POL00423564

Appendix A - Terms and Definitions

ANONYMISE: is an attempt by a User to hide or obscure their identity or their use of Post Office Networks, Systems, Devices or Information in an attempt to avoid detection, monitoring or logging.

AVAILABILITY: necessitates that Information is accessible when it's needed.

BRING YOUR OWN DEVICE (BYOD): is any privately owned Device which has been sanctioned by Post Office for business use in accordance with policy.

CONFIDENTIALITY: necessitates that Information is not disclosed to individuals or systems that are not authorised to receive it.

CYBER SECURITY AND INFORMATION ASSURANCE (CSIA): is the overall approach to protecting Post Office's Information Assets from attack, loss, theft, compromise or damage. It comprises of policies, standards, procedures and control frameworks, typically referred to as a Management System, to enable the systematic management of Post Offices Information Assets in order to establish formal governance, manage business risks and ensure contractual, legal and regulatory compliance.

DEVICE: is any Device which is capable of connecting to Post Office Networks or Systems and can be used to store, process or transmit Post Office Information. Examples of Devices are: laptops, desktops, smartphones (iPhone, Blackberry), tablet computers (iPad).

EMPLOYEE: is anyone working for Post Office whether full-time or part-time and which for the purposes of this policy includes, but is not limited to, contractors, sub-contractors, postmasters or temporary staff.

END USER or *USER*: is anyone (excluding customers) who has been issued a Post Office User ID and/or has access to Post Office Networks, Systems, Devices or Information.

INFORMATION ASSET: is any asset with value and/or can present a risk to Post Office. Examples of Information Assets include people, processes, Networks, Systems, Devices or Information.

INFORMATION: is any data which is informative, organised for a purpose, has meaning and/or relevance to Post Office, its clients, consumers, customers, Employees and/or Third Party Supply Chain.

INFORMATON ASSURANCE: the practice of ensuring Information is adequately protected and managed in accordance with Post Office policy, frameworks, standards and contractual, legal and regulatory requirements.

INTEGRITY: necessitates that Information cannot be modified in an unauthorised manner.

NETWORK: typically described as either a wide area network (WAN) or a local area network (LAN) providing enterprise-wide connectivity for Post Office enabling voice, data or integrated communications that supports one or more business systems or inter-connected Devices.

PHYSICAL ID: is any hardware token which is used to identity a person and/or gain physical entry to Post Office premises.

REMOVABLE MEDIA: is any hardware Device which can be connected to and/or removed from another Device and can be used for transferring or storing Information. This includes but is not limited to: mobile phones, digital cameras, digital audio Devices, portable hard drives, CDs, DVDs, Blu-Rays, SD cards, memory sticks, flash drives or any similar Device.

SYSTEM: is a logical grouping of hardware and software components (for e.g. Horizon, CFS, SharePoint) which is used in the storage, processing or transmission of Information. They may be owned and operated by Post Office or one or more Third Party Supply Chain.

THIRD PARTY SUPPLY CHAIN: any individual or company, along with its supply chain network that provides a product or service to Post Office.

USER ID: is any authentication or access credentials used to gain access to Post Office Networks, Systems, Devices or Information (for e.g. authentication tokens, computer or application usernames, wireless or network logons, Active Directory logins).

POL00423564

RCC 1 MAY 2015 PAPER 10B

POST OFFICE BUSINESS INFORMATION SYSTEMS POLICY

POL00423564

Business Information Systems Policy

Document Control

Overview

Owner:	Head of Information Security and Assurance Group	**Enquiry point:**	ISAG
Approved by:		**Effective from:**	
Version:	0.4	**Last updated:**	

Revision History

Version	Date	Author	Changes
0.1	09/11/2014	Andrew Watson	Initial draft release
0.2	20/11/2014	Andrew Watson	Second draft release post ISAG peer review
0.3	12/02/2015	Andrew Watson	Changes made to reflect comments / feedback. A summary of which are provided in Policy Review Tracker and details provided back to ISWP through document mark-up.
0.4	18/02/2015	Andrew Watson	As above

Reviewers

Version	Date	Reviewer	Comments
0.1	20/11/2014	ISAG	
0.2	10/02/2015	ISWP	Feedback from ISWP contained within Policy review tracker
0.3	18/02./2015	ISWP	Feedback from ISWP contained within Policy review tracker

Quality Control	Next review date
This document is subject to periodic review and will be reviewed at least annually or where there are significant changes to the business and/or its operating environment.	02/12/2015

POL00423564

Business Information Systems Policy

Contents

POL00423564

Business Information Systems Policy

0. Terms and Abbreviations

Terms used throughout this document are described at the end of this document in Appendix A.

1. Purpose

The purpose of the Business Information Systems (BIS) Policy is to support business requirements, provide adequate levels of protection for Post Office Information Assets.

2. Scope

The people, processes and technology used for the provision of services to and/or on behalf of Post Office throughout the enterprise, including Third Party Supply Chain are within the scope of this policy regardless of physical location.

3. Policy

3.1. BUSINESS APPLICATIONS

3.1.1. Applications must be protected using industry best practice security architecture principles and standards to ensure the use of consistent security functionality, aligned with the Post Office's Business Information Systems Framework (##REF BIS FMWK) and risk appetite (##REF RM FMWK).

3.2. IDENTITY AND ACCESS MANAGEMENT

3.2.1. Identity and Access Management (IAM) life-cycle arrangements must be established throughout the Post Office in line with risk appetite (##REF RM FMWK) as per the requirements set out in the Business Information Systems Standards Development Framework (##REF BIS FMWK).

3.3. SYSTEM MANAGEMENT

3.3.1. Business Information Systems must be protected using security controls that ensure they meet Post Office requirements (##REF BIS FMWK) and preserve the confidentiality, integrity and availability of Information in line with classification requirements (##REF IAP).

3.4. SECURITY INFRASTRUCTURE

3.4.1. An Enterprise Architecture framework that incorporates Post Office Information security principles and standards (##REF BIS FMWK) must be established to ensure a consistent risk based Information security management approach (##REF RM FMWK) across Post Office.

3.5. NETWORK MANAGEMENT

3.5.1. Networks must be protected and managed in accordance with Post Office Information security requirements (##REF BIS FMWK).

3.6. MOBILE COMPUTING

3.6.1. Mobile devices must be protected and managed in accordance with Post Office Information security requirements (##REF BIS FMWK).

POL00423564

3.7. ELECTRONIC COMMUNICATIONS

3.7.1. Electronic Communications must be protected using industry best practice security architecture principles and standards to ensure the use of consistent security functionality, aligned with the Post Office's Business Information Systems Framework (##REF BIS FMWK) and risk appetite (##REF RM FMWK) to ensure appropriate levels of protection.

3.8. SYSTEM DEVELOPMENT LIFE CYCLE

3.8.1. System Development Life Cycle activities must be secured in accordance with documented and assured methodologies and processes in line with the requirements set out in the Business Information Systems Framework (##REF BIS FMWK).

3.9. PHYSICAL AND ENVIRONMENTAL SECURITY

3.9.1. Facilities and access to those facilities must be protected against unauthorised access.

4. Exceptions

All policy exceptions must be obtained in writing from the Post Office Information Security and Assurance Group (ISAG). Exceptions will be considered by ISAG at the time requested and reviewed thereafter on an annual basis. Evidence must be retained for both the exception and the annual review. For further Information please contact: isag[GRO]

5. Enforcement

This policy will be supported by and enforced through Post Office frameworks and standards.

6. Violations

Compliance with this policy is mandatory. Post Office provides Information Security and Awareness Training at Induction and at least annually thereafter and will regularly assess compliance to this policy.

Any violation of this policy is an incident. Where incidents are attributed to an Employee, the individual(s) may be subject to the Code of Conduct (##REF CoC), similarly, Third Party Supply Chain incidents will be managed through corresponding contracts.

7. References

This document has the following references:

- Business Information Systems Framework
- Risk Management Framework
- Information Assurance Policy
- Code of Conduct

POL00423564

Business Information Systems Policy

Appendix A - Terms and Definitions

ANONYMISE: is an attempt by a User to hide or obscure their identity or their use of Post Office Networks, Systems, Devices or Information in an attempt to avoid detection, monitoring or logging.

AVAILABILITY: necessitates that Information is accessible when it's needed.

BRING YOUR OWN DEVICE (BYOD): is any privately owned Device which has been sanctioned by Post Office for business use in accordance with policy.

CONFIDENTIALITY: necessitates that Information is not disclosed to individuals or systems that are not authorised to receive it.

CYBER SECURITY AND INFORMATION ASSURANCE (CSIA): is the overall approach to protecting Post Office's Information Assets from attack, loss, theft, compromise or damage. It comprises of policies, standards, procedures and control frameworks, typically referred to as a Management System, to enable the systematic management of the Post Offices Information Assets in order to establish formal governance, manage business risks and ensure contractual, legal and regulatory compliance.

DEVICE: is any Device which is capable of connecting to Post Office Networks or Systems and can be used to store, process or transmit Post Office Information. Examples of Devices are: laptops, desktops, smartphones (iPhone, Blackberry), tablet computers (iPad).

EMPLOYEE: is anyone working for Post Office whether full-time or part-time and which for the purposes of this policy includes, but is not limited to, contractors, sub-contractors, postmasters or temporary staff.

END USER or *USER*: is anyone (excluding customers) who has been issued a Post Office User ID and/or has access to Post Office Networks, Systems, Devices or Information.

INFORMATION ASSET: is any asset with value and/or can present a risk to the Post Office. Examples of Information Assets include people, processes, Networks, Systems, Devices or Information.

INFORMATION: is any data which is informative, organised for a purpose, has meaning and/or relevance to Post Office, its clients, consumers, customers, Employees and/or Third Party Supply Chain.

INFORMATON ASSURANCE: the practice of ensuring Information is adequately protected and managed in accordance with Post Office policy, frameworks, standards and contractual, legal and regulatory requirements.

INTEGRITY: necessitates that Information cannot be modified in an unauthorised manner.

NETWORK: typically described as either a wide area network (WAN) or a local area network (LAN) providing enterprise-wide connectivity for Post Office enabling voice, data or integrated communications that supports one or more business systems or inter-connected Devices.

PHYSICAL ID: is any hardware token which is used to identity a person and/or gain physical entry to Post Office premises.

REMOVABLE MEDIA: is any hardware Device which can be connected to and/or removed from another Device and can be used for transferring or storing Information. This includes but is not limited to: mobile phones, digital cameras, digital audio devices, portable hard drives, CDs, DVDs, Blu-Rays, SD cards, memory sticks, flash drives or any similar device.

SYSTEM: is a logical grouping of hardware and software components (for e.g. Horizon, CFS, SharePoint) which is used in the storage, processing or transmission of Information. They may be owned and operated by Post Office or one or more Third Party Supply Chain.

THIRD PARTY SUPPLY CHAIN: any individual or company, along with its supply chain network that provides a product or service to Post Office.

USER ID: is any authentication or access credentials used to gain access to Post Office Networks, Systems, Devices or Information (for e.g. authentication tokens, computer or application usernames, wireless or network logons, Active Directory logins).

POL00423564

POST OFFICE
CYBER AND INFORMATION SECURITY POLICY

POL00423564

Cyber and Information Security Policy

Document Control

Overview

Owner:	Head of Information Security	**Enquiry point:**	ISAG
Approved by:		**Effective from:**	
Version:	0.7	**Last updated:**	

Revision History

Version	Date	Author	Changes
0.1	09/11/2014	Andrew Watson	Authored and initial Release
0.2	13/11/2014	Claire Davies	Peer Review
0.3	14/11/2014	Claire Davies	Lead Review
0.4	18/11/2014	Andrew Watson	Final mark-up following ISAG comments
0.5	20/11/2014	Andrew Watson	Updated definitions and minor content update
0.6	12/02/2015	Andrew Watson	Changes made to reflect comments / feedback. A summary provided in Policy Review Tracker and details provided back to ISWP through document mark-up.
0.7	18/02/2015	Andrew Watson	As above.

Reviewers

Version	Date	Reviewer	Comments
0.1	09/11/2014	ISAG	
0.2	13/11/2014	ISAG	
0.3	14/11/2014	Julie George	
0.4	19/11/2014	Julie George	
0.5	10/02/2015	ISWP	Feedback from ISWP contained within Policy review tracker
0.6	18/02/2015	ISWP	Feedback from ISWP contained within Policy review tracker

Quality Control	Next review date
This document is subject to periodic review and will be reviewed at least annually or where there are significant changes to the business and/or its operating environment.	02/12/2015

POL00423564

Cyber and Information Security Policy

Contents

POL00423564

Cyber and Information Security Policy

0. Terms and Definitions

The terms used within this document are located and described at Appendix A of this document.

1. Executive Statement

Post Office's Board and Executive Committee (ExCo) recognise that Cyber and Information Security threats present significant commercial and operational risk to Post Office and to those of its subsidiaries (Post Office). ExCo are committed to developing a strategic response to current and emerging Cyber and Information Security threats as an enabling mechanism for Post Office to achieve its growth, modernisation, customer focus and Employee engagement objectives whilst preserving Post Office's brand, commercial image, reputation, competitive advantage, revenues, profitability, legal, regulatory and contractual compliance.

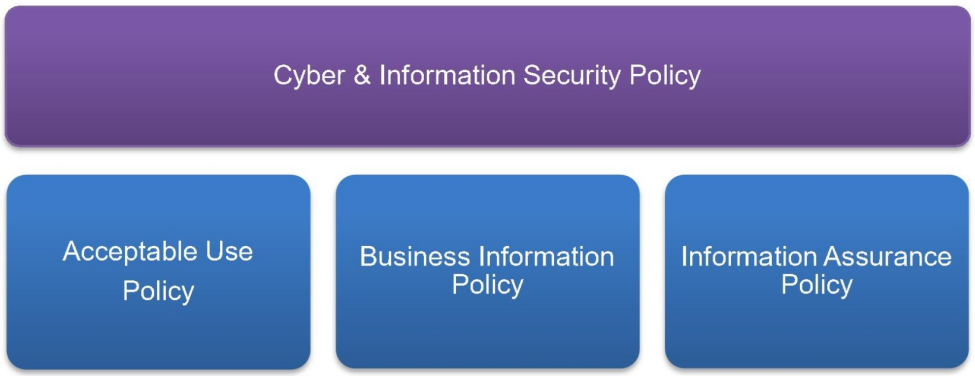
This policy sets out the agenda for the establishment, implementation, maintenance and continual improvement of Post Office's Cyber Security and Information Assurance (CSIA) Management System. These requirements will continue to be improved and aligned to any changes in Post Office's strategic objectives, operating environment, risk profile, legal or regulatory compliance and/or in response to incidents or emerging cyber threats.

2. Introduction

CSIA refers to the principles and implementation of defending Post Office against, unauthorised or unintended access, destruction, disruption or tampering of its Information Assets. The Cyber and Information Security Policy is a key component of the CSIA programme, which:

- Sets out Post Office's Cyber and Information Security Governance, Risk and Compliance (GRC) structure;
- Enables people, processes and technology to operate in a risk controlled environment; and
- Validates commercial, contractual, legal and regulatory compliance.

This Policy informs three sub-ordinate policies as defined below:



POL00423564

Cyber and Information Security Policy

3. Purpose

The purposes of the policy are to:

- Enable Post Offices' strategic objectives whilst maintaining a level of control and acceptable risk proportionate to the Board and ExCo's risk appetite.
- Structure CSIA activities within the business's Information Security GRC framework which covers all Post Office people, processes and technology.
- Protect Post Office's Information Assets from risks associated with the theft, loss, misuse, damage or abuse whether intentional or unintentional by preserving their Confidentiality, Integrity and Availability.
- Enable the development and maintenance of Post Office's CSIA capability including leadership and organisational responsibilities, while ensuring that everyone remains aware of their responsibilities and understands and adheres to Post Office's CSIA policies.
- Provide corporate policies, standards and guidelines as an enabler for Information; exchange, security operations, e-commerce, risk management and incident management throughout Post Office and its Third Party Supply Chain.
- Ensure on-going threat awareness, compliance and continual improvement of CSIA within Post Offices' programmes and management systems.

4. Scope

The people, processes and technology used for the provision of services to and/or on behalf of Post Office throughout the enterprise, including Third Party Supply Chain are within the scope of this policy regardless of physical location.

5. Policy

5.1. Information Security Governance

5.1.1. The Board of Directors and ExCo under the stewardship of the General Council (GC) bestow custodianship of CSIA for Post Office to the Head of Information Security and Assurance Group (ISAG).

5.1.2. ISAG is responsible for Post Offices CSIA strategy (##REF CSIA Strategy), Cyber and Information GRC frameworks, tactical CSIA programmes, controls, assurance and countermeasures across the enterprise.

5.1.3. In support of 5.1.2 (above) the Head of ISAG will establish a governing body known as the Information Security Committee (ISC) attended by members of the Senior Leadership Team (SLT) from each major business function. The ISC responsibilities are set out in ISC Terms of Reference (##REF ToR ISC). A subordinate Information Security Working Party (ISWP) will be established whose responsibilities are set out in the ISWP Terms of Reference (##REF ISWP ToR).

5.2. Information Risk Management

5.2.1. Information risk assessments must be performed and/or approved by ISAG for all Information Assets in order to identify the key Information risks, evaluate them, and determine treatment options.

5.2.2. The Information Risk Management Framework (##REF IS RM FMWK) provides the context for identifying, assessing and prioritising Information-related risks, alignment to the Enterprise Risk Management framework.

POL00423564

5.2.3. Risk Registers must be managed to include Information risks. Where an identified risk is above the acceptable level of tolerance a Risk Acceptance Notice (RAN) must be completed and where appropriate include ISAG guidance. (##REF RAN procedure)

5.3. Business Information Systems

5.3.1. The Business Information Systems Policy (##REF BIS Policy) will set out the technical framework for the protection of Post Office's Information Assets.

5.4. Information Assurance

5.4.1. The Information Assurance Policy (IAP) will set out the framework for monitoring, protecting, auditing, compliance, assurance and continual improvement of Information throughout its life-cycle (##REF IAP) including but not limited to any contractual, legal or regulatory requirements.

5.5. Acceptable Use

5.5.1. Post Offices CSIA policies will be supported by a detailed Acceptable Use Policy (##REF AUP) and handbook (##REF handbook) that define the way in which everyone is expected to comply with the use of Information technology and Information throughout Post Office.

5.6. Human Resources Security

5.6.1. Human Resources (HR) will complete standard background checks on Employees following the latest HR policies and guidance on the intranet.

5.6.2. Induction processes will incorporate Information security requirements, including but not limited to: deployment of Information assets and user ID's, acceptance of the Acceptable Usage Policy (##REF AUP) and the completion of regular Information security awareness training (##REF IAP).

5.7. Information Security Management

5.7.1. Cyber Security activities and Information assurance requirements must be incorporated into all business processes (for example business transformation programmes, change and project management). This will be achieved by integrating Information security requirements into planning decisions and budgeting activities and will include Information risk (see 5.2) in business decisions, meetings and audits (##REF IAP).

5.8. Incident Management

5.8.1. In support of this policy an Information Security Incident Management (ISIM) framework (##REF ISIM FMWK), owned by the Head of ISAG will be developed, deployed and maintained throughout Post Office and the Third Party Supply Chain. The ISIM framework sets out the requirements for incident management, incident handling and incident response in line with the Post Offices risk appetite (see 5.2).

5.8.2. Incidents and/or breaches impacting Post Office Information Assets must be notified to ISAG immediately in line with the requirements set out in the ISIM framework (##REF ISIM FMWK).

5.9. Third Party Supply Chain Management

5.9.1. CSIA requirements set out in Post Office's policies, frameworks and standards will be extended to all third parties through procurement and contractual management processes which must include the requirements set out in the ISAG House Position (##REF ISAG House Position)

5.9.2. New and updated CSIA policies will be issued to the Third Party Supply Chain immediately after they are approved by Post Office, at which point they will supersede

POL00423564

as appropriate (a) previous versions of the policy (b) current contractual requirements. Third Party Supply Chain must inform the Head of ISAG within 30 days of being issued a new or updated policy, if they are unable to meet any of the new requirements so appropriate action(s) can be agreed.

5.9.3. Third Party Supply Chain must obtain and maintain certification to the current version of ISO27001 and PCI DSS with a scope agreed by ISAG for the term of the contract. In line with 5.2.3 (above), any concession, without exception requires the completion of a risk acceptance notice (RAN).

5.9.4. Third Party Supply Chain service provisions must be monitored, measured, audited and are subject to continual improvement as set out in the IAP (##REF IAP) and the Cyber Security and Information Assurance Compliance Framework (##REF CSIA Compliance FMWK).

5.10. Business Continuity Management

5.10.1. CSIA controls must be resilient before, during or following any incident, breach, crisis or disaster and Post Office's Business Continuity Management (BCM) and Disaster Recovery (DR) planning and/or testing activities must incorporate Post Office's Information security requirements.

6. Exceptions

All policy exceptions must be obtained in writing from Post Office ISAG. Exceptions will be considered by ISAG at the time requested and reviewed thereafter on an annual basis. Evidence must be retained for both the exception and the annual review. For further Information please contact: isag@ GRO

7. Violations

Compliance with this policy and/or any subordinate policy is mandatory. Post Office provides Information Security and Awareness Training at Induction and at least annually thereafter and will regularly assess compliance to this policy.

Any violation of this policy is an incident. Where incidents are attributed to an Employee, the individual(s) may be subject to the Code of Conduct (##REF CoC), similarly, Third Party Supply Chain incidents will be managed through corresponding contracts.

8. References

This document has the following references:

- Cyber Security and Information Assurance Strategy
- Terms of Reference - Information Security Committee
- Terms of Reference - Information Security Working Party
- Information Security Risk Management Framework
- Risk Acceptance Notice procedure
- Business Information Systems Policy
- Information Assurance Policy
- Acceptable Use Policy
- Information Security Handbook
- Information Security Incident Management Framework
- ISAG House Position
- HR - Code of Conduct

POL00423564

Appendix A: Terms and Definitions

ANONYMISE: is an attempt by a User to hide or obscure their identity or their use of Post Office Networks, Systems, Devices or Information in an attempt to avoid detection, monitoring or logging.

AVAILABILITY: necessitates that Information is accessible when it's needed.

BRING YOUR OWN DEVICE (BYOD): is any privately owned Device which has been sanctioned by Post Office for business use in accordance with policy.

CONFIDENTIALITY: necessitates that Information is not disclosed to individuals or systems that are not authorised to receive it.

CYBER SECURITY AND INFORMATION ASSURANCE (CSIA): is the overall approach to protecting Post Office's Information Assets from attack, loss, theft, compromise or damage. It comprises of policies, standards, procedures and control frameworks, typically referred to as a Management System, to enable the systematic management of the Post Offices Information Assets in order to establish formal governance, manage business risks and ensure contractual, legal and regulatory compliance.

DEVICE: is any Device which is capable of connecting to Post Office Networks or Systems and can be used to store, process or transmit Post Office Information. Examples of Devices are: laptops, desktops, smartphones (iPhone, Blackberry), tablet computers (iPad).

EMPLOYEE: is anyone working for Post Office whether full-time or part-time and which for the purposes of this policy includes, but is not limited to, contractors, sub-contractors, postmasters or temporary staff.

END USER or *USER*: is anyone (excluding customers) who has been issued a Post Office User ID and/or has access to Post Office Networks, Systems, Devices or Information.

INFORMATION ASSET: is any asset with value and/or can present a risk to Post Office. Examples of Information Assets include people, processes, Networks, Systems, Devices or Information.

INFORMATION: is any data which is informative, organised for a purpose, has meaning and/or relevance to Post Office, its clients, consumers, customers, Employees and/or Third Party Supply Chain.

INFORMATON ASSURANCE: the practice of ensuring Information is adequately protected and managed in accordance with Post Office policy, frameworks, standards and contractual, legal and regulatory requirements.

INTEGRITY: necessitates that Information cannot be modified in an unauthorised manner.

NETWORK: typically described as either a wide area network (WAN) or a local area network (LAN) providing enterprise-wide connectivity for Post Office enabling voice, data or integrated communications that supports one or more business systems or inter-connected Devices.

PHYSICAL ID: is any hardware token which is used to identify a person and/or gain physical entry to Post Office premises.

REMOVABLE MEDIA: is any hardware Device which can be connected to and/or removed from another Device and can be used for transferring or storing Information. This includes but is not limited to: mobile phones, digital cameras, digital audio devices, portable hard drives, CDs, DVDs, Blu-Rays, SD cards, memory sticks, flash drives or any similar device.

SYSTEM: is a logical grouping of hardware and software components (for e.g. Horizon, CFS, SharePoint) which is used in the storage, processing or transmission of Information. They may be owned and operated by Post Office or one or more Third Party Supply Chain.

THIRD PARTY SUPPLY CHAIN: any individual or company, along with its supply chain network that provides a product or service to Post Office.

USER ID: is any authentication or access credentials used to gain access to Post Office Networks, Systems, Devices or Information (for e.g. authentication tokens, computer or application usernames, wireless or network logons, Active Directory logins).

POL00423564

POST OFFICE INFORMATION ASSURANCE POLICY

POL00423564

Business Information Systems Policy

Document Control

Overview

Owner:	Head of Information Security and Assurance Group	**Enquiry point:**	ISAG
Approved by:		**Effective from:**	
Version:	0.4	**Last updated:**	

Revision History

Version	Date	Author	Changes
0.1	09/11/2014	Andrew Watson	Initial draft release
0.2	20/11/2014	Andrew Watson	Second release post ISAG peer review
0.3	12/02/2015	Andrew Watson	Changes made to reflect comments / feedback. A summary of which are provided in Policy Review Tracker and details provided back to ISWP through document mark-up.
0.4	19/02/2015	Andrew Watson	As above.

Reviewers

Version	Date	Reviewer	Comments
0.1	20/11/2014	ISAG	
0.2	10/02/2015	ISWP	Feedback from ISWP contained within Policy review tracker
0.3		ISWP	Feedback from ISWP contained within Policy review tracker

Quality Control	Next review date
This document is subject to periodic review and will be reviewed at least annually or where there are significant changes to the business and/or its operating environment.	02/12/2015

POL00423564

Business Information Systems Policy

Contents

POL00423564

Business Information Systems Policy

0. Terms and Definitions

Terms used throughout this document are described at the end of this document in Appendix A.

1. Purpose

The purpose of the Information Assurance Policy (IAP) is to support business requirements and provide adequate levels of assurance to Post Office Information Assets.

2. Scope

The people, processes and technology used for the provision of services to and/or on behalf of Post Office throughout the enterprise, including Third Party Supply Chain are within the scope of this policy regardless of physical location.

3. Policy

3.1. INFORMATION ASSET MANAGEMENT

3.1.1. Information Assets must be identified, owned, risk assessed (##REF RISK MGT FMWK), and protected in line with the requirements set out in the Asset Management Framework (##REF Asset MGT FMWK).

3.2. INFORMATION CLASSIFICATION

3.2.1. An Information classification scheme will be established and must be observed throughout Post Office to ensure the appropriate level of protection is applied to all Information, this includes but is not limited to Information that is: communicated verbally, stored in physical or electronic form and electronic communications (##REF INFO CLASSIFICATION STD).

3.3. INFORMATION ASSET LIFECYCLE

3.3.1. Information will be managed throughout its life cycle in line with the Data Management Life Cycle (##REF DATA MGT LIFECYCLE).

3.4. INTELLECTUAL PROPERTY RIGHTS (IPR)

3.4.1. Software and other third party copyrighted items must only be obtained through legitimate sources, and only on the basis that the software or copyright licence terms will be complied with and will ensure that copyright ownership of documents or software is established through the granting of a license, contract and/or employment agreements.

3.5. INFORMATION SECURITY AWARENESS PROGRAMME

3.5.1. A security awareness programme must be established throughout Post Office and tailored security messages must be communicated to End Users.

3.5.2. The effectiveness of security awareness programmes must be monitored and evaluated.

POL00423564

3.6. INFORMATION SECURITY MONITORING AND IMPROVEMENT

3.6.1. The Information security status of Post Office is subject to regular monitoring, reporting (##REF CSIA M&R STD), audit (##REF AUDIT FMRK) and performance review to assess Post Office's Cyber Security and Information Assurance programmes, policies, frameworks, standards, controls, risks and Third Party Supply Chain and will make continual improvement decisions aligned with business risk (##REF RISK MGT FMWK) and objectives as set out in the CSIA Compliance Framework (##REF CSIA Compliance FMWK).

3.6.2. Post Office and Third Party Supply Chain members must continually monitor the external environment for events and threats outside of its control which may adversely impact Post Office operations and/or capabilities.

3.7. COMPLIANCE

3.7.1. Post Office will protect the rights and privacy of individuals whose Information Post Office collects and/or processes and will comply with UK & EU legislation, and where appropriate, international laws. Post Office's Data Protection and Privacy standard, owned by the Data Protection Officer (DPO) (##REF DPA & Privacy STD) sets out the requirements for legal and regulatory compliance.

4. Exceptions

All policy exceptions must be obtained in writing from Post Office's Information Security and Assurance Group (ISAG). Exceptions will be considered by ISAG at the time requested and reviewed thereafter on an annual basis. Evidence must be retained for both the exception and the annual review. For further information please contact: isag GRO

5. Violations

Compliance with this policy is mandatory. Post Office provides Information Security and Awareness Training at Induction and at least annually thereafter and will regularly assess compliance to this policy.

Any violation of this policy is an incident. Where incidents are attributed to an Employee, the individual(s) may be subject to the Code of Conduct (##REF CoC), similarly, Third Party Supply Chain incidents will be managed through corresponding contracts.

6. References

This document has the following references:

- Risk Management Framework
- Asset Management Framework
- Data Life Cycle Management Standard
- CSIA Monitoring and Reporting Standard
- CSIA Audit Framework
- CSIA Compliance Framework
- Data Protection and Privacy Standard
- Information Classification Standard
- Code of Conduct

POL00423564

Appendix A - Terms and Definitions

ANONYMISE: is an attempt by a User to hide or obscure their identity or their use of Post Office Networks, Systems, Devices or Information in an attempt to avoid detection, monitoring or logging.

AVAILABILITY: necessitates that Information is accessible when it's needed.

BRING YOUR OWN DEVICE (BYOD): is any privately owned Device which has been sanctioned by Post Office for business use in accordance with policy.

CONFIDENTIALITY: necessitates that Information is not disclosed to individuals or systems that are not authorised to receive it.

CYBER SECURITY AND INFORMATION ASSURANCE (CSIA): is the overall approach to protecting Post Office's Information Assets from attack, loss, theft, compromise or damage. It comprises of policies, standards, procedures and control frameworks, typically referred to as a Management System, to enable the systematic management of the Post Offices Information Assets in order to establish formal governance, manage business risks and ensure contractual, legal and regulatory compliance.

DEVICE: is any Device which is capable of connecting to Post Office Networks or Systems and can be used to store, process or transmit Post Office Information. Examples of Devices are: laptops, desktops, smartphones (iPhone, Blackberry), tablet computers (iPad).

EMPLOYEE: is anyone working for Post Office whether full-time or part-time and which for the purposes of this policy includes, but is not limited to, contractors, sub-contractors, postmasters or temporary staff.

END USER or *USER*: is anyone (excluding customers) who has been issued a Post Office User ID and/or has access to Post Office Networks, Systems, Devices or Information.

INFORMATION ASSET: is any asset with value and/or can present a risk to Post Office. Examples of Information Assets include people, processes, Networks, Systems, Devices or Information.

INFORMATION: is any data which is informative, organised for a purpose, has meaning and/or relevance to Post Office, its clients, consumers, customers, Employees and/or Third Party Supply Chain.

INFORMATON ASSURANCE: the practice of ensuring Information is adequately protected and managed in accordance with Post Office policy, frameworks, standards and contractual, legal and regulatory requirements.

INTEGRITY: necessitates that Information cannot be modified in an unauthorised manner.

NETWORK: typically described as either a wide area network (WAN) or a local area network (LAN) providing enterprise-wide connectivity for Post Office enabling voice, data or integrated communications that supports one or more business systems or inter-connected Devices.

PHYSICAL ID: is any hardware token which is used to identify a person and/or gain physical entry to Post Office premises.

REMOVABLE MEDIA: is any hardware Device which can be connected to and/or removed from another Device and can be used for transferring or storing Information. This includes but is not limited to: mobile phones, digital cameras, digital audio devices, portable hard drives, CDs, DVDs, Blu-Rays, SD cards, memory sticks, flash drives or any similar device.

SYSTEM: is a logical grouping of hardware and software components (for e.g. Horizon, CFS, SharePoint) which is used in the storage, processing or transmission of Information. They may be owned and operated by Post Office or one or more Third Party Supply Chain.

THIRD PARTY SUPPLY CHAIN: any individual or company, along with its supply chain network that provides a product or service to Post Office.

USER ID: is any authentication or access credentials used to gain access to Post Office Networks, Systems, Devices or Information (for e.g. authentication tokens, computer or application usernames, wireless or network logons, Active Directory logins).

POL00423564

Post Office Ltd
Risk & Compliance Committee Meeting
1 May 2015

Location:

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

ATTENDANCE LIST

ATTENDEES	SIGNATURE
MacLeod, Jane	
Alwen, Lyons	
Cameron, Alisdair	
Hayward, Neil	
Lambert, Gavin	
Nick, Kennett	
Paula, Vennells	