POL00302864

Risk & Compliance Committee Meeting
Room 505, 5th Floor, 148 Old Street, London, EC1V 9HQ
20th March 2014, 13.30pm – 15.30pm

Committee Members
Chris Aujard (Chair)
Paula Vennells
Chris Day
Alwen Lyons
Neil Hayward

To Attend
Dave Mason
Martin Edwards
Julie George
Julian DiMauro
Sara Hollingsbee
Adnan Killedar
David Epstein
Rob Bolton

Apologies:

	Agenda Item	Purpose	Timings	Papers	Owner
1.	**Risk Management Culture** i) Risk Management Strategy	**Agree strategy and recognise progress**	13.30 – 13.50 20 minutes	**Paper One plus Appendix**	Dave Mason
2.	**Top Business Risks** i) Update on the Top Risks ii) Deep Dive Session – Data Security iii) Network Transformation Financial Risk Assessments for Multiples	**Review risks and perform deep dive session**	13.50 – 14.40 50 minutes	**Verbal report** **Paper Two** **Paper Three**	Dave Mason Julie George NT Manager
3.	**Assessment** i) Risk Events and Near Misses ii) Assurance Activity iii) Risk Acceptance iv) BCM Report	**Review and agree recommendations**	14.40 – 15.00 20 minutes	**Paper Four** **Paper Five plus Appendix** **Paper Six plus Appendix** **Paper Seven**	Dave Mason Dave Mason Dave Mason David Epstein
4.	**Stewardship** i) Policy Approvals ii) Gifts & Hospitality Report	**Approve policies and receive report**	15.00 – 15.15 15 minutes	**Paper Eight** **Paper Nine**	Policy Owners Dave Mason
5.	**Committee minutes & matters arising** i) Agree meeting minutes of 20th January 2014 ii) Matters arising from 20th January 2014	**Agree minutes and review action updates**	15.15 – 15.25 10 minutes	**Paper Ten**	All
6.	**Meeting A.O.B** i) Annual Report	**Capture and review AOB items**	15.25 – 15.30 5 minutes		All

POL00302864

Strictly Confidential **PAPER ONE**

RISK AND COMPLIANCE COMMITTEE

Update on Risk Management Strategy

1. Purpose

The purpose of this paper is to:-

- Update the committee on the risk strategy, and
- Describe the approach to achieving the strategy.

2. Future state

Our objective is to create a culture within Post Office in which the management of risk (identification, assessment, treatment and reporting) is an integral part of decision making and sound risk-based decisions are encouraged.

3. Current state

Risk management across Post Office is still relatively immature. Consequently:-

- Risk ownership is being driven by risk and compliance, with most owners only beginning to understand and fulfil their responsibilities;
- Where risk management culture exists, it is generally limited to specialists and some senior leadership teams; and
- Governance and reporting of risk is limited to programme management and the senior leadership.

4. Strategy

Our strategy to move to the future state has a number of component parts; however the underlying theme is one of 'hearts and minds' rather than 'control and command'. To this end, the focus is on continually demonstrating the commercial and business value of risk-based decision making, not the introduction of processes and rules

Significant elements of the strategy are already operating:-

- The governance and resources required are in place;
- The roll out of a formal framework is under way; and
- Post office leadership have demonstrated a high level of commitment.

Details of the components of the strategy, their current status, the maturity roadmap and plans for 2014 – 2015 are included in appendix 1 of this paper.

POL00302864

5. Recommendation

The committee is asked to:-

- Agree the strategy for risk management at the Post Office; and
- Recognise the progress made to date in implementing the strategy.

.

Dave Mason
20th March 2014

POL00302864

Strictly Confidential **PAPER ONE APPENDIX**

RISK AND COMPLIANCE COMMITTEE

Update on Risk Management Strategy APPENDIX

1. Elements of the Strategy

The risk management strategy consists of the following components:-

- Acquiring risk professionals from outside the Post Office to supplement the existing business knowledge and skills in the risk management function;

- Developing the risk management function through the completion of professional risk qualifications to develop a common baseline of understanding and a common language for discussing risk management;

- Introducing a network of risk management business partners to share knowledge and expertise through the business and facilitate the deployment of the risk management framework;

- Designing a risk management framework that is practical in operation and relevant to the objectives and day-to-day management of Post Office, incorporating:

    - risk strategy (strategy, culture, appetite)
    - risk architecture (roles, responsibilities, reporting structures and governance)
    - risk management process (identification, assessment, treatment and reporting)
    - risk protocols (policies, procedures, tools and techniques)

- Supporting the business in using the above components to develop the cultural objective;

- Raising the awareness of the benefits of risk management through a comprehensive training and communication plan; and

- Conducting regular reviews to ensure the strategy matches the organisational need.

POL00302864

2. Current status

In support of this plan we have already:-

- Completed the recruitment process, the business partners are now all fully engaged with the directorates. All have, or are in the process of obtaining, professional recognition,

- Put in place the governance elements of the framework through R&CC, ExCo and ARC. Risk and Compliance are further incorporating risk governance into key business committees in conjunction with CoSec,

- Developed a 2014 to 2015 plan for the deployment of the risk framework, including communications and training needs, and

- Developed the new risk register tool which will be piloted in April.

Other "quick wins" have been:-

- Discussions with HR introducing 'risk thinking' into the induction process for new entrants and new managers;
- Engagement with HR introducing objectives which incorporate sound risk management;
- Integrating Business Partners with major programmes (Network, IT, Business, Sparrow);
- Scheduling briefing sessions by the Head of Risk and Compliance positioning risk management with directorate lead teams; and
- Implementing Anti Money Laundering product risk assessments.

Meanwhile, the risk business partners have been focussed on facilitating and supporting the risk owner's analysis and review of the "top nine" risks. The results to date were discussed at the most recent ARC and ExCo meetings.

POL00302864

Strictly Confidential **PAPER ONE APPENDIX**

. **Maturity Roadmap**

	13-14	14-15	15-16	16-17	17+
Risk strategy (strategy, culture, appetite)	Risk culture exists mainly in specialist functions e.g. Risk & Compliance, Internal Audit. Risk appetite is rarely identified and then only at a project specific level.	Risk culture exists at ExCo and directorate lead team level with regular review of risks Risk assessment is an integral part of investment decisions Risk appetite is discussed at enterprise level Risk management introduced into objective setting process	Board and ExCo set the 'tone from the top' Risk culture is evident at all senior management levels Review and reporting of risks is embedded within the governance structure of the business Risk appetite forms part of the planning process and is set across the business Risk management is embedded into objective setting process	Board and ExCo set the 'tone from the top' Risk culture is evident at all senior management levels Review and reporting of risks is embedded within the governance structure of the business Risk appetite forms part of the planning process and is set across the business Risk management is used pro-actively to set the business strategy	Board and ExCo set the 'tone from the top' Risk culture is evident at all senior management levels Review and reporting of risks is embedded within the governance structure of the business Risk appetite forms part of the planning process and is set across the business Risk management is used pro-actively to set the business strategy
Risk architecture (roles, responsibilities, structures and governance)	Ownership of risk management is driven by the specialist risk function Risk reporting is viewed as belonging to the specialist risk function	ExCo and lead teams regularly discuss enterprise and emerging risks, supported by business partners Escalation of significant new risks is commonplace R&CC is established as a value-add component of governance architecture	ExCo and lead teams discuss risks on a regular basis Lead teams and risk owners drive the content of risk reporting New initiatives or changes are critically evaluated from a risk perspective Risk reporting is firmly established Architecture reviewed against business design for the future	Management 'own' the review of risks and seek specialist support to enhance their risk management High risk areas of the business fully conversant and competent in risk management tools , techniques & practice	Common risk management architecture across all directorates & functions with common language of risk and shared tools & techniques deployed across the business

POL00302864

	13-14	14-15	15-16	16-17	17+
Risk management process (identification, assessment, treatment & reporting)	Key risks identified at enterprise level Directorates have reviewed risks at least once No formal risk management process other than in specialist areas e.g. Information Security	Risk management process is designed and deployed in limited areas of the business on a top-down basis	Risk management process is cascaded to the wider business Consideration is given to automating some reporting processes Process is reviewed to ensure fit with business	Risk management process transitions into integrated process within business planning Risk management process deployed in all high risk areas	Risk management process deployed throughout business
Risk protocols (policies, procedures, tools & techniques)	Introduction of basic tools to analyse critical risks Key reg risks have associated policies	Core risk management process defined and documented Training has been provided on basic tools and techniques to key individuals Induction training incorporates basic risk awareness All reg risk & some non-reg risks have associated policies A risk culture assessment framework is introduced to measure progress	Training has been extended to all senior management population Policy framework has been reveiwed and extended to cover all risk areas. A risk management handbook is available describing all processes, tools and techniques used in Post Office	All managers have been trained in risk management and how it applies to their day jobs Tools and techniques are widely used throughout the day to day activities of managers Consideration is given to registering fro accreditation against appropriate standard (e.g. ISO31000)	The use of risk management tools and techniques is commonplace throughout the business. Risk standard accreditation has been achieved.

POL00302864

4 Plan for 2014 -2015

The table below outlines the Risk and Compliance plan for the next year.

The individual risk framework components have already been identified and risk assessment guidelines noted as the first priority, including a standard for the formal acceptance of unmitigated risks. Other priority deliverables would include the definition and agreement of risk roles and responsibilities across Post Office as a whole and further process guidelines covering directorate level risk monitoring.

	Q4	Q1	Q2	Q3	Q4
Risk strategy (strategy, culture, appetite)	Risk strategy documented and approved	Quarterly comms plan designed and delivered Guidelines for risk-based objectives produced	Quarterly comms plan designed and delivered Director training delivered for significant risk areas e.g. FS compliance, AML, bribery and competition law etc	Quarterly comms plan designed and delivered Risk plan audited Risk based objectives introduced at SLT level and above 2015 plan confirmed and budgets submitted	Quarterly comms plan designed and delivered 2015 plan finalised
Risk architecture (roles, responsibilities, structures and governance)	Risk team all in post BP working with directorates Risk & compliance committee restructured	All major programmes have risk team member Revised committees and forums include risk team attendee TORs for revised governance architecture incorporate effective risk management	Gaps in risk governance identified and action plans developed Key risk policies identified and drafted for approval	Risk governance effectiveness review carried out and action plans developed	

POL00302864

Strictly Confidential **PAPER ONE APPENDIX**

	Q4	Q1	Q2	Q3	Q4
Risk management process (identification, assessment, treatment & reporting)	Monthly team planning sessions in place Risk framework defined Risk management process defined Top 10 risks identified and assessed Deep dive for FS mis-sell risk	New risk register introduced Deep dive for top 10 risk Bow-tie process extended to include evaluation and prioritisation of causes and controls	Deep dive for top 10 risk	Deep dive for top 10 risk Risk assessments factored in to planning process	Deep dive for top 10 risk
Risk protocols (policies, procedures, tools & techniques)	Risk management policy in place AML product risk assessment introduced	Risk management policy reviewed Risk assessment training for key individuals	Key individuals risk training Guide to assessing risk	Introduction of risk culture assessment tool Refresher risk training delivered	

POL00302864

Strictly Confidential

PAPER TWO

RISK AND COMPLIANCE COMMITTEE

Information Security and Assurance Group
Data Security Risk Update

1. Purpose

- The purpose of this paper is to provide the Committee with an update on the current unmitigated or partially mitigated risks for Data Security.

2. Background

- Data Security is acknowledged by the Board and ExCo as being one of the top 10 risks to the business. It is reported on under the heading of 'Cyber Security and Information Assurance' to the ExCo and the Post Office Board on a monthly basis, including a summary of incidents/breaches.

- The Information Security and Assurance Group (ISAG), in line with all industry information security professionals, understand Data as being a component of information security and as such it is reported within the Risk Register in relation to Information Assets. An example of an Information Asset could be a Database containing sensitive personal data or a key Application. Conversely it could also be a piece of paper that has details of a potential company takeover.

- It is important to note that some risks will always feature in the Risk Register since they are subject to on-going analysis and management. Whilst a risk can be reduced through various controls it will always be a risk, however, it should always be measured with a view to 'impact' and 'likelihood' of threat.

3. Corporate Information Security

- Risk assessment, management and mitigation are core areas of on-going activity for ISAG. They are linked to Post Office's corporate information security, the maintenance of its Information Security Management System and the maintenance of related certifications (such as Payment Card Industry Data Security Standard (PCI/DSS), ISO27001[1], and HMG Information Assurance (IA) obligations).

- Post Office certifications are assessed annually, and sometimes more frequently, by external auditors to ensure risk assessments are fit-for-purpose and that suitable controls are in place to mitigate and manage risks. Where appropriate, Post Office has contractual obligations with its suppliers to allow their processes and systems to be audited.

- Regular vulnerability/penetration testing is undertaken on Post Office suppliers by third-party specialists with follow-up tests to ensure that mitigating actions are implemented when any vulnerabilities are identified.

[1] ISO27001: An International Standard covering the specification and management of an organisation's Information Security Management System. The guidelines and general principles for initiating, implementing, maintaining and improving information security management within an organisation.

POL00302864

Strictly Confidential

PAPER TWO

- Any risks that are wholly mitigated through on-going controls, Technology and Policy, or assurance activities are not raised to the Risk and Compliance Committee. Such risks are subject to external audit scrutiny on an annual basis.

4. Corporate Information Security Risks

Identity and Access Management:

- This risk has been subject to an internal audit and it is currently managed by the Information Security Training Awareness and Communications project. It is acknowledged that this method of mitigation cannot be relied upon for adequate control, nor does it address comprehensive Audit requirements.

- Work will be undertaken by ISAG to assist IT Colleagues in specifying and designing an Identity and Access Management System suitable for Post Office. This will be done in conjunction with guidance from HR to ensure that the Identity and Access Management System will address roles and responsibilities, based on individual job requirements.

- A suitable Identity and Access Management system will also provide an audit trail, essential when investigating internal incidents/breaches.

4.1 Network Security

- The security of the technical network will always be a risk; controls will always be subject to on-going reviews and scrutiny. Specific risks are discussed with suppliers at regular Information Security Management Forums, as are vulnerability/penetration testing schedules. Instances where the suppliers fail to address technical areas are escalated to the IT Service Managers for resolution.

- ISAG are currently looking at various threat monitoring systems to 'guard and monitor' Post Office's Cyber/Technical estate. Whilst this is in its early stages, it is expected that such a service would provide statistics and management reports on attempted breaches and importantly if any were successful. It would back-up our System Integrator/Manager Incident Reports and also highlight any gaps. The suppliers also provide useful intelligence regarding the risk and threat landscape.

4.2 Governance and Change

Post Office is a rapidly changing and evolving business, making strong Governance essential. ISAG participate in:

- Project Gating and Concurrence;
- Contract Due Diligence and Pre Contract Supplier Assurance;
- On-going supplier assurance;
- Service Integrator Governance and Assurance;
- Various IT Forums and Change Control Boards.

It should be noted that it isn't unheard of for Projects to 'Go Live' before Gating sign-off has been agreed. This risk has been raised by ISAG and the governance process is currently under review by Corporate Risk.

POL00302864

Strictly Confidential

PAPER TWO

- ISAG hold a cross business Information Security Committee and Working Group, which provides Governance across Information Security and Assurance activities. It is known that the Company Secretariat is currently reviewing the corporate governance structure to ensure that all Boards and Forums are delivering against set criteria. The Secretariat is aware of the Terms and Conditions of both the Information Security Committee and Working Group.

- Incidents/breaches, IT and non IT are currently managed via the Duty Manager/IT Service Desk. In future the IT related incidents will be picked up by the Service Desk function provided by Atos. Non IT incident management is covered by a Post Office internal process currently under development.

5. Summary

The Committee are asked to note that:

- Any failure to protect customer or corporate data could have a disproportionate reputational impact. This has the potential to prevent Post Office from achieving the growth necessary to deliver its strategic objectives.

- The integrity and security of Post Office data is reliant on a complex network of interrelated processes and controls.

- The number of potential threats, particularly of external attacks through the internet, is rapidly increasing.

- ISAG are aware that some elements of risk are not yet managed at an appropriate level. Examples are: data ownership, classification and business continuity. Many other controls are operating, giving assurance that the risk as a whole is being managed. Further assurance is obtained through third party reviews and certification audits.

- Risk mitigation is underway through on-going projects which are reviewing the controls and putting in place active measures to monitor the risks and their mitigation. These include implementation of a new GRC tool, appointment of a Data Protection Officer and procurement of a communications and training tool covering data protection and information security. An additional five resources have been proposed for the new financial year to increase the effectiveness of existing risk measures; this has yet to be confirmed.

Julie George/Lesley Sewell

20th March 2014

POL00302864

Strictly Confidential **PAPER THREE**

RISK AND COMPLIANCE COMMITTEE

Risk Assessments performed when working with Multiple Partners in the Network Transformation Programme

1. Purpose

The purpose of this paper is to update the Risk & Compliance Committee on the risk assessments which are performed when working with multiple partners in the Network Transformation (NT) programme.

2. Background

Multiple partners operate 1350 branches in the existing network and are being encouraged to convert their existing branches into the appropriate new model as part of the NT programme. The NT programme is also following a strategy of proactively engaging strategic multiple partners to take on new branches as existing agents leave the network. So far contracts have been signed with multiple partners to convert 640 branches.

Bulk contracts with multiples are often signed covering the conversion of tens of branches, which results in large upfront payments. A recent contract signed for 191 McColl's branches resulted in an upfront payment of approximately £6.8million. There is a risk that money advanced for transformation will be lost if a multiple partner ceases trading shortly after contract signing.

3. Approach to risk assessment – financial risk

There is a process in place to assess the risk of failure posed by a multiple partner at the time of contract signing. Prior to contract signing the Network Finance team completes a Financial Assessment (FA) on the relevant multiple partner, which includes a review of recent accounts, ratio analysis and commentary on performance and a review of the performance of any existing Post Office branches managed by that partner. An Experian credit check is carried out and if the partner is deemed to be above low risk as calculated by Experian the Network Finance team work with Legal to identify additional measures which can be taken to mitigate the risk. These vary depending on the level of risk and the structure of the partner, but can include a parent company guarantee or senior level discussions including provision of unpublished accounts to provide assurance of financial viability. Both these measures were used prior to signing the McColl's contract.

Financial Assessments have to be approved by the Network Finance team before contracts can be signed. All contracts where payments total £1million or more are reviewed by the Chief Financial Officer. In addition, any bulk contractual deal with a multiple partner is subject to our internal contract approval process requiring sign off from the Chief Financial Officer and Network and Sales Director in advance of contracts being issued.

4. Assurance

The Financial Assessment process has been reviewed as part of business process assurance work on financial controls on agency payments performed by Internal Audit in December 2012 and June 2013.

POL00302864

5. Recommendations

The committee is asked to note the update on risk assessments performed for multiple partners in the NT programme

Neil Ennis
20th March 2014

POL00302864

Strictly Confidential **PAPER FOUR**

RISK AND COMPLIANCE COMMITTEE

Risk Events and Near Misses

1. Purpose

The purpose of this paper is to:

- Advise the committee of any new events or near misses that could impact the risk profile of the entire organisation;
- Provide an update on events previously reported; and
- Advise the committee on events that have been closed.

2. New Events or Near misses since the last meeting

Internal Events

2.1 Southport PO – incorrect disposal of customer data.

Issue: A reporter from a local newspaper contacted Communications on 28 February 2014 to inform them that a number of documents containing client information had been found in a skip at the old Southport Crown Office, which was being cleared under the Crown franchise programme. The reporter had called the customers concerned using the phone numbers on the documents. Many had visited the newspaper to collect their personal information.

Impact: Whilst this incident has been managed locally with minimal disruption the controls in place within the Crown Transformation Programme to manage the destruction of data would not prevent this situation from happening again. This could lead to serious reputational damage or have a detrimental effect on our customers if personal information was leaked. There is also the possibility that further incidents may trigger the involvement of the Information Commissioners Office.

Actions: The crown transformation process communicated to the branch includes full instructions for the destruction of customer data. Whilst this is considered to be an isolated incident caused through either human error or a deliberate act by someone at the branch, the process did not prevent this situation from occurring. The controls around the destruction of customer data need to be reviewed and strengthened to prevent a similar event happening in the future. This is being considered as part of the post incident review being performed by Information Security and Crown Transformation.

POL00302864

2.2 Email disruption – Unavailability of email application March 2014.

Issue: Post Office Outlook became unavailable due to an issue at Microsoft. The core Microsoft application was impacted, Webmail and Blackberry were unaffected.

Impact: Post Office users were unable to use Microsoft Outlook and this incident has identified a reliance on a single email application in the business. Webmail and Blackberry may be sufficient as a short term fix however they may not be appropriate should an incident of this nature take longer to resolve.

Actions: It is still not clear what caused the issue at Microsoft, although this is an isolated incident, and this will be identified from the incident review. Whilst there was evidence of a level of resilience to this issue through the use of Webmail and Blackberry this was only appropriate due to the nature of the failure. The communication to all staff of the failure and the availability of Webmail was not effective and controls need to be strengthened in this area. Royal Mail hold the contract with Microsoft and therefore Post Office must ensure that resilience to this kind of incident is in place once the ownership of the contract is transferred from Royal Mail.

External Events

The following external events have happened recently. We have performed initial assessments of the potential for similar events happening at Post Office. Further reviews will be carried out, if required, to assess the risk and the outcomes reported to a future meeting.

We have not yet included the recent adverse press coverage of the Co-Operative Society and its possible effect on network transformation plans, but the programme team have undertaken an impact assessment and are closely monitoring the situation.

2.3 Tesco – Clubcard accounts data leakage Feb 2014

Issue: Details of 2,240 Tesco Clubcard accounts were published on a popular sharing website which has resulted in Tesco suspending the Clubcard accounts affected. It is believed that hackers compiled a list of customer details by taking data off the Internet and running it through the Tesco website to find matches. Account details were hacked where users used the same email addresses and passwords for their Tesco accounts.

Impact: An estimated 1.5 million Post Office online customers would be at risk to this kind of attack if they use the same user id/email and passwords across multiple online accounts or services.

Actions: It is recognised that there is insufficient control in place and identity and access management is therefore being addressed as part of the Information Security Training Awareness and Communications project. Data loss prevention communications will be rolled out from April 2014

POL00302864

2.4 Barclays Bank - customer data loss and Aviva - customer car insurance accident details stolen Feb 2014

Issue: Both Aviva and Barclays have suffered theft of customer information which was later sold or offered for sale to third parties.

Impact: Controls against data leakage in the Post Office are known to be weak and would not prevent a similar theft of client data.

Actions: These incidents reinforce the need to rapidly improve Post Office data security A programme is already under way to address data security. Specifically:-

- Existing policies are being revised, drafts are due for completion by July 2014;
- Data loss prevention communications and training software will be rolled out from April; and
- Internal Audit recommendations on user access controls are being implemented.

3. Update on Events previously reported.

3.1 BOI ATM's are not exempt from Business rate tax.

Issue: Valuation Office Agency's (VOA) decision is that BOI ATMs are not exempt from Business rate tax. The VOA action is backdated for up to 3 years with a potential impact of up to £11 million on the Post Office.

Update: VOA is currently seeking further clarification from BIS on their legal position. The risk remains that VOA will send out financial demand letters. These invoices would demand payment of full backdated amount within 30 days. The event is being closely monitored by the Banking Team within Financial Services.

3.2 Power Resilience Events

Issue: Two recent power disruptions at Dearne House and Swindon showed that power resilience plans were not effective.

Update: A Business Continuity (BC) third party site has been procured and a plan is being developed to secure appropriate recovery capability for NBSC post separation from Royal Mail.

Power resilience will be reviewed by the nominated supplier once separation is delivered and will include maintenance and testing. The project will appoint the supplier in September 14. Business Continuity has engaged Property to identify the current status of power resilience in advance of the September delivery.

3.3 Change of price and product provider for travel insurance

Issue: A number of errors occurred relating to the change of company and prices as from 1 January 2014. Post publication and distribution branch brochures were found to contain a price error significantly over stating the cost of one of the policy options (within Annual Multi trip cover).

Update: The lessons learned work has begun and FS is expected to complete investigations and report conclusions in March.

POL00302864

4 Closed Events

4.1 Outlook Mailing list misuse

Issue: On the 6th of December 2013, an employee from the Royal Mail Group (RMG) issued an email to the entire RMG and Post Office in error.

Update: Groups have been removed to reduce likelihood of further events. Business separation from Royal Mail will further reduce this risk. Royal Mail bore the cost of resolution as the principle contract holder.

4.2 Social Media misuse Dec 2013

Issue: Twitter -@Postofficenews posted a tweet relating to financial services that was non-compliant with the rigorous requirements set out by the Financial Conduct Authority (FCA) and had not been through the Financial Services marketing sign off process.

Update: There is now a work stream in place to agree use of social media and appropriate controls. Until these have been agreed, informed monitoring of @postoffice and @postofficenews is being carried out by Regulatory Risk and any non-compliant tweets asked to be taken down.

4.3 FCA enforcement notice and fine against Lloyds Banking Group for serious sales incentives failures Dec 2013.

Issue: The notice raises the importance and focus the FCA has currently on incentive schemes to ensure that these drive customer focussed and compliant behaviours in sales staff. It was fined £28m. The Lloyds scheme as described, by the FCA, was very aggressive, staff could be demoted or face salary reductions if they did not hit sales targets.

Update: Improvements to our incentive scheme governance are being implemented. We will respond to recent FCA feedback on our Mortgage Incentive Scheme following their Mortgage Deep Dive review.

POL00302864

4.4 Barclays Fine for record retention failure – Dec 2103

Issue: Barclays Plc. has been fined $3.75 million (£2.28 million) by a U.S. regulator over its alleged decade-long failure to properly keep electronic records, emails and instant messages.

Update: Whilst the Post Office has data retention policies and standards, they did not specifically cover emails or instant messages. Data Protection is now working on a wider data policy to cover email and instant messages. The target date for approval is July 14. They are also updating training awareness material as part of induction and continuing training. The target date for go-live is April 2014.

4.5 Homeserve – breach of FCA principles – Feb 2014

Issue: Homeserve, an insurance intermediary which arranges home emergency and repairs cover was fined £30.7m for breach of Financial Conduct Authority (FCA) principles. The breaches were in respect of sales practices, incentive schemes and complaints.

Impact: The enforcement case raised the importance of Board members being trained and giving requisite attention to Compliance issues.

Update: As part of our wider review of board training we will be including an update on compliance as well as our responsibilities as an appointed representative.

5 Recommendations

The Committee is asked to:

- Review the new events or near misses potentially impacting the risk profile of the organisation, consider the adequacy of the planned actions by Post Office and identify those requiring further monitoring;
- Note the updates on events previously reported; and
- Note the events that have been closed.

Dave Mason
20th March 2014

POL00302864

Strictly Confidential **PAPER FIVE**

RISK AND COMPLIANCE COMMITTEE

Assurance Activity Update

1. Purpose

The purpose of this paper is to provide the Risk and Compliance Committee with an update on assurance activity that is planned, in progress, or already completed.

2. Assurance Activity

2.1 Rainbow Update

Following the Rainbow incident Deloitte were commissioned in January 2013 to provide an assessment of the Information Security operating model within Post Office and its contrast with similar organisations. Following on from the Deloitte report the actions and recommendations were incorporated into a project called Buffalo.

The Buffalo project delivered a new Information Security staffing structure and Information Security policies and procedures were reviewed and developed. The outputs from the Buffalo project have now been incorporated into business as usual, however the remaining issues from the Deloitte report are:

- The implementation of an Information Security governance risk & compliance tool is going through the procurement process as the SISD tool does not meet the required criteria; and

- The shortfall in resource remains the same and has been raised as a risk.

Status The Information Security & Assurance Group are about to undertake a corporate wide, business impact assessment, to identify information / data assets and accountable owners within the Post Office. It is estimated this will be completed within two months.

2.2 Governance Update

A report of the findings from the review of the ExCo sub-committees was prepared for the General Counsel and this is attached as an appendix to this paper. The conclusions of the review were:-

- While certain sub-committees discuss risk in limited terms, there is no consistent, robust and effective risk management process adopted within the meetings to support ExCo in fulfilling their oversight of business risk; and

- The sub committees are not effective in reviewing their purpose, updating their terms of reference and evaluating their effectiveness.

Status Recommendations from the review along with improvements identified by the Company Secretary has initiated a sub-committee restructure. New terms of reference, membership and responsibilities including effective risk management oversight are currently being drafted.

POL00302864

2.3 Mortgage Market Review

As part of a regulatory review of the mortgage market following the financial crisis the FSA/FCA has tightened the rules in a number of areas including assessment of affordability and the requirement for face to face and interactive dialogue with customers to be on an advice basis only from 26 April 2014. A major project is in place for POL/BOI to become compliant with the revised requirements. This involves a significant recruitment, training and monitoring plan for advisors alongside improved infrastructure and controls.

Mortgage advised sales went live on 3 February 2014. Prior to launch Post Office and Bank of Ireland (BOI) performed a joint piece of assurance work to assess and review compliance preparedness which concluded that this was in place

Status The risk function will be undertaking a post implementation review in April 2014 to assess whether the regulatory requirements are in place for mortgage advice in Post Office branches..

2.4 Xanadu

Following the migration of Homephone and Broadband services from BT Worldwide to Fujitsu an assurance review was undertaken to assess whether the end to end process for identifying and implementing the new supplier had appropriate governance and employed the correct controls to manage the risks involved in the migration. Data has been gathered and is being evaluated and a report drafted.

Status A final report will be submitted to the Risk & Compliance Committee once discussed and agreed by the review sponsor, Martin George.

3. Recommendations

The committee is asked to note the update and status of assurance activity

Dave Mason
20th March 2014

POL00302864

PAPER FIVE - APPENDIX

Ex Co Sub -Committees Governance Performance Review

1. Purpose

The purpose of this paper is to:

1.1 Establish whether Post Office Ltd has robust and effective risk management reporting in place.

1.2 Identify if the sub-committees and boards are fulfilling their role, including risk as part of their role and evaluating their effectiveness.

2. Background

As part of the separation from Royal Mail and the introduction of Post Office as an independent company a defined board governance structure was agreed with accountabilities, decision making structures, escalation processes and delegated responsibilities.

To enable the Post Office Board and the ExCo in their decision making and oversight, a number of sub-committees and boards were set up to provide empowerment and enabling delegated responsibility across the business.

As an independent company Post Office is responsible for its own risk management framework and ensuring that risk management is an integral part of its strategic and key decision making processes.

This review was undertaken to gain an understanding of how sub-committees and boards include risk as part of their decision making process and consider the impact on the strategic objectives of the business.

3. Methodology

This review was carried out using the terms of reference, meeting notes and actions from the committees and boards, in addition to discussions with the board secretariat and Company Secretary's office staff.

It focuses on the sub-committees and boards reporting to ExCo only and does not include the committees reporting directly to Post Office Board.

4. Findings

4.1 Terms of Reference

- Terms of reference (TORs) are available for each of the boards but these vary in layout and content. Only 4 of the 12 examined included risk as part of their accountabilities.

POL00302864

- It was unclear if a full review of the TORs and membership had been completed since the boards were set up. There is no date or version control included on the TORs therefore it was difficult to assess the latest version without confirming with the board secretariat.

4.2 Meeting Minutes and Actions

- Notes and actions are captured, these vary in level of content and detail and it is not clear how decisions are reached.
- There is no consistent approach to noting risk discussions or their impact on the wider business risks or business strategy.
- Actions are recorded and in general they are owned with a timescale and update provided at the next meeting.

4.3 Risk Reporting

There is no detail within the TORs how the boards report their discussions and decisions to ExCo.

The boards do not include risk reporting as an update to ExCo apart from the transformation board which includes risks to the delivery of programmes in their reporting pack but there is little evidence that decisions includes wider business risks and strategy.

4.4 Effectiveness Evaluation

- Some of the boards have reviewed their TORs for minor changes but there is no common approach taken to reviewing TORs and evaluating effectiveness of the board to confirm the purpose is still being met.

5. Conclusion

While certain boards discuss risk in limited terms, there is no consistent, robust and effective risk management process adopted within the meetings to support ExCo in fulfilling their oversight of business risk

The sub committees and boards are not effective in reviewing their purpose updating their terms of reference and evaluating their effectiveness.

6. Proposals

- Each board to review its terms of reference and include risk management as part of its accountability and risk discussion to be included on meeting agenda.
- Key decisions including risk management to be included in meeting notes.
- ExCo to review the purpose of each board to identify and agree what needs to be reported to them its format and frequency.

POL00302864

- A risk & compliance team member to attend the boards to facilitate risk discussions. This is in addition to the critical friend that is planned for future meetings
- TORs to be reviewed at least annually and the review to be included in the notes of the meeting.
- A central library of forum TORs to be maintained by the Risk& Compliance Team including dates for review and assurance methodology.

7 Activities already under way

In addition to the proposals listed above, the following activities are already in progress:

- Regular Ex Co reviews of enterprise level risks;
- Restructured and enhanced Risk & Compliance Committee;
- Risk business partners driving analysis of the enterprise level and directorate risks;
- Risk business partner engagement in programmes and directorate lead teams
- Working with the new Head of Strategic Programme Management Office.

POL00302864

Strictly Confidential **PAPER SIX**

RISK AND COMPLIANCE COMMITTEE

Risk Acceptance

1. Purpose

The purpose of this paper is to:-

- To update the committee on the acceptance of unmitigated risks; and
- To perform an after the fact review of the attached risk acceptance related to the implementation of self-service kiosks.

2. Background

In any risk management framework it is always an option for a firm to tolerate or accept any identified risk. This may be done for many reasons including: the cost of remediation, the perceived benefit to the organisation, the presence of a "hard" deadline that cannot be changed or simply that the impact and likelihood is considered to be within acceptable limits.

3. Action

A formal process for such acceptances is not yet implemented at the Post Office. The Head of Risk and Compliance is agreeing approach with the Company Secretary and the Head of Strategic Programme Office. A draft policy will be available before the next meeting of the committee.

The risk acceptance in appendix 1 was approved in February. Without pre-empting the action above, it is of sufficient significance to the organisation to require formal review by the committee.

4. Recommendation

The committee is asked to:-

- Agree the proposed approach to the acceptance of risk; and
- Review the attached, considering any further action to be taken.

Dave Mason
20th March 2014

POL00302864

PAPER 6 - APPENDIX 3

Confidential

Risk Acceptance Note

General Information

RAN reference	POL/RANXXX	Date of RAN	26th Feb 2014
System Name	Self Service Kiosk		
Risk Owner	*Kevin Gilliland, Lesley Sewell*		
Business Unit	Network, iT		
IT Custodian	Lesley Sewell		
Business Criticality Rating	CRITICAL	Information Classification	STRICTLY CONFIDENTIAL
Impact Value	HIGH	Likelihood Value	MEDIUM
Risk Status	HIGH		
Review Date	26th Feb 2014		

Risk Description

Background information

The Self Service Kiosk is an enabler for the Crown Transformation Programme supporting the requirement to bring the Crown branches into profit.

The first branch is planned to Go-live on 28th February 2014, as a soft launch. This will be Harpenden branch and is due to receive 2 Self Service kiosks.

A prerequisite for Go-live is the completion and acceptance of Penetration tests to the Self Service solution delivered. As a result of the system architecture employed, this Penetration Testing encompassed two elements:

1. A Penetration Test of the Fujitsu Horizon Business Service (HBS) application and the supporting network used by NCR and the Kiosk. This testing was performed by NCC on behalf of Fujitsu/POL, and found no significant issues. Remedial work has been undertaken and POL ISec have reviewed and accepted the results as fit for go-live.
2. A separate Penetration Test assessment, directed at the Kiosk hardware and application software, and its integration with the supporting network infrastructure was performed by Portcullis on behalf of NCR/POL and was aimed at determining the severity, impact and skill level required to exploit any vulnerabilities through realistic attack vectors. The initial output of this test was available on 25th February 2014 and has been reviewed and evaluated by POL ISec Subject Matter Experts.

The details of the findings are contained in the preliminary pen testing report which remains on restricted circulation due to the sensitive nature of the content. In summary, the test disclosed a total of 34 vulnerabilities as shown below:

Severity	Count
High	11
Medium	12
Low	8
Information	3

High Severity Vulnerabilities details are shown in Annex A attached.

NCR have reviewed the report. Annex A details vulnerabilities that have been fixed, regression tested and implemented into the latest kiosk build in readiness for rollout. The remaining items are listed with plans for

POL00302864

resolution. Penetration testing to be scheduled once all remedial activities are completed to establish closure of the vulnerabilities identified and a check that no new vulnerabilities have been introduced. Project team to own.

Normally POL would expect no "High" findings in a system going into production and that any "Medium" findings would be addressed within 7 to 30 days depending on their impact and the skill level required to exploit.

This assessment of the outstanding risks is based on the information available for the penetration test report and the response from NCR.

Based on the vulnerabilities discovered it would be possible for a miscreant of moderate skill level to perform a series attacks on the system through the software or hardware interfaces. (Refer to Annex A). These attacks could allow for the installation of physical devices or malicious code to cause the device to be modified to behave in an un-designed way (e.g. to log keyboard entries or capture other input; or to cause unexpected behaviour including denial of service). By the nature of the configuration of the system and application, management interfaces are not sufficiently secure to prevent remote access to the device from the network facilitating and attacker taking control or modifying behaviour in a similar way.

There are a number of system tools available which could be used to allow an attacker to control the behaviour of the device without installing any additional code. The use of the Solidcore security application may mitigate some of the ability of malicious code to run, but access to systems tools and the administrator account would not be prevented and could even be used to disable this feature.

The kiosk does not permanently store any product or customer data – this is all maintained by HBS in the centre.

In the event of a device being compromised, it could be possible to information, including cardholder data as covered by PCI-DSS, to be compromised and copied to a destination of the attacker's choice. Additionally, it would be possible for an attacker to cause the device to generate sufficient network traffic to cause a denial of service to the other devices connected to the same LAN. Should the traffic generated be sufficient to affect the performance of the branch router, it is possible Horizon traffic performance could be affected also.
As an attacker would be able to execute arbitrary code and commands, it is possible defacement of the interface could be caused, reference data modified or an entirely false application run without the knowledge of the user.
The ability to exploit the discovered vulnerabilities would require that an attacker has physical access to the device or the ability to connect to the LAN. The former would require some distraction technique (possibly by masquerading as an engineer) whilst the latter would be easier to achieve through the installation of a device in the network cable.

In summary, the risk in Harpenden from the vulnerabilities identified here would mean the loss of services from the two installed kiosks, and possibly a denial of the Horizon service if the network performance was affected. The likelihood is deemed to be low as there is no publicity around this kiosk go-live, and the operational staff in the branch will be attending these machines from switch-on.

The penetration testers were only permitted to show that a vulnerability existed as without running the risk of destruction or harm it is not possible to follow through on many of the exploits discovered.
The overall test shows that there are serious issues with the physical and logical security of the device.

Recommendation

It is recommended by InfoSec that the risk is owned at the appropriate executive level, while the remaining high issues are addressed in the immediate term, and a plan is in place to address the medium issues within agreed timescales not exceeding 30 days.

It is also recommended that no further branches are put live until a checkpoint is held to review the status of the remaining issues. Only once a go decision is obtained from that review meeting will the four branches planned w/c 10th March go ahead.

The recommendation that the go-live of any further of the NCR Self Service Kiosks be delayed until all the high issues have been fixed and retested and a plan is in place to address the medium issues within agreed timescales not exceeding 30 days.

Risk Mitigation Plan

Ref	Action	Responsible Party	Target Date
1			

POL00302864

2			
3			

Statement of Acceptance

I accept this risk and its implications for not implementing the stated recommendations within the appropriate timescale and will sponsor the activities within the Risk Mitigation Plan set out above.
Rationale for Risk Acceptance:

Signed: GRO

Name: H. CLARKE Date: 27/2/14

GRO Neil Wilkinson (DA for LJ Sewell) 27/2/14

Annex A – High Severity Vulnerabilities

Details of the high severity vulnerabilities are included in the attached spreadsheet.

MgtSummary
PenTest Highs v3

POL00302864

Severity	Impact	Likelihood	Skill Level Required	Title	Management Summary of Vulnerability	Management Summary of Impact	Planned Mitigation	Resolution Date
High	High	Low	Medium. As the vulnerabilities are documented in the public domain. The skill level required to exploit is high.	Oracle Java Multiple Vulnerabilities	Known vulnerabilities exist in the installed version of Java (programming language). Vulnerability could be exploited remotely or by direct access (eg. USB port).	A miscreant could use knowledge of these vulnerabilities to obtain full administrative control of the system PC giving opporunity to change or install software that could be used to collect information, alter displayed messages/images, and affect network performance within the branch only. There is a possibility that customer data may be intercepted.	Update to latest version of Java. For a single branch, ensuring the physical security of the kiosks is maintained by the branch staff reduces the risk likelihood	w/c 10/03
High	High	Low	Medium. An attacker would need to gain access to the system, and have sufficient technical knowledge to modify the services affected.	Insecure Windows Service Permissions	There are 16 Windows services running on the kiosk with permissions could permit a user to modify the executed code with arbitrary code, which would be executed the next time the service is started. Vulnerability could be exploited remotely or by direct access (eg. USB port).	A miscreant could escalate their permissions on the system, to permit them to undertake further activities on the system culminating in the same possible impact as described above.	Amend the user permissions on the services (protect the services); disable or remove the relevant services. For a single branch, ensuring the physical security of the kiosks is maintained by the branch staff reduces the risk likelihood	tbc
High	High	Low	High	Missing Security Patches	The latest Microsoft security patches were not applied to the build tested.	An attacked could exploit known Microsoft vulnerabilities not patched.	Apply all Microsoft security patches.	Fixed in Build 297; delivered xx/xx
High	High	Low	Medium	Insecurely Configured Service Path	The directory path description for some Services (9 instances) are not defined within quotes. Vulnerability could be exploited remotely or by direct access (eg. USB port).	By modifying the path description, an attacker could misdirect the system to a different executable, which could result in a number of possible outcomes, culminating in the same possible impact as described above.	All service paths are correctly quoted.	tbc

POL00302864

High	High	Low	Medium	Insecure Permissions On Program Files	Some programs and program files can be changed by non-administrative users. Vulnerability could be exploited remotely or by direct access (eg. USB port).	This could allow a miscreant to introduce malicious code into certain directories, or to replace existing programs with malicious ones, culminating in the same possible impact as described above.	Program and directories affected to be modifiable by users with administator privileges only. Where appropriate, write privileges for non-administrative users in the above programs and directories are revoked.	tbc
High	Critical	Low	High. An attacker with significant IT skills would be required.	Insecure TCP Service: Berkeley 'R' Services	The 'R' services (eg. 'rsh', 'rlogin', 'rexec') are running on the kiosk. With access to the kiosk, it is possible to logon and execute commands. Vulnerability could be exploited remotely or by direct access (eg. USB port).	This could allow a miscreant to establish control of the individual kiosk system targetted, which could result in a number of possible outcomes, culminating in the same possible impact as described above.	Disable these services or replace with secure alternatives (eg. SSH).	tbc
High	High	Low	High	Kiosk Application Excessive Execution Privilege	In the event that a user is able to break out of the kiosk application, a user could execute system commands	An attacker would have full administrative access to the system to permit an attacker to modify system components and configurations, culminating in the control of system with possible impact as described above.	Applications not executed with excessive user privileges.	Fixed in Build 297; delivered xx/xx
High	High	Low	High	Windows Kiosk Breakout (Unauthenticated)	An attacker that is able to break out of the kiosk application and execute arbitrary operating system functions with the privilege of the kiosk application.	An attacker would have the opportunity to perform, amongst other nefarious activities: • Execution of arbitrary applications • Escalation of privilege • Installation of malicious software • Modification of system and application configurations	Remove unnecessary Windows components and application that enable miscreant to break out of the application.	Fixed in Build 297; delivered xx/xx

POL00302864

High	High	Low	High	Exposed And Enabled USB Port	A USB port is exposed at the rear and base of the kiosk monitor, where the monitor is attached to the kiosk unit. Physical access to the kiosk is required.	The exposed port allows an individual to plug in a keyboard and access functionality in the Kiosk that is not normally available. The USB port permits the selection of the boot device menu, and allows for boot from an arbitrary USB storage device. Execution of arbitrary code could result in control of the kiosk culminating in the impact noted above.	Disable exposed/unused USB ports. Physcial barrier to be applied to the USB port for the single branch.	tbc
High	High	Low	Medium	Accessible Internal Enabled USB Port	A side panel may be unscrewed to provide an opening to the internals of the kiosk, including internal USB ports.	An attacker with an improvised tool and time could insert USB devices that may allow them to install malware on the system.	Secure the side panel so that it cannot be opened/removed.	27-Feb
High	Medium	Low	Medium	No BIOS Password Set	The BIOS password is used to control access to system hardware startup configuration.	Without a BIOS password, the device can be reconfigured to boot from an alternative boot media; such as a USB device or CDROM. By booting their own operating system, an attacker could gain access to the local drives as well as a potential stepping point within the network.	A suitably strong BIOS password is set	27-Feb

POL00302864

POL00302864

Strictly Confidential **PAPER SEVEN**

RISK AND COMPLIANCE COMMITTEE

Business Continuity Update

1. Purpose

The purpose of this paper is to provide the Risk and Compliance Committee with a brief update and synopsis with regards to business continuity in the Post Office.

2. Business continuity Update

2.1 Background

During previous external and internal audits in 2012, it was identified that a greater level of assurance of business continuity in the Post Office is required. There are a number of key drivers that support the requirement for business continuity capability and management in the Post Office:

- Business resilience and capability
- Protecting the Post Office brand and reputation
- Satisfying contractual requirements for Post Office clients
- Managing the Post Office's third party dependencies and supply chain
- Reducing impacts and costs of interruption
- Managing Business Continuity and Disaster Recovery risks
- Government obligations
- Business growth and change
- Separation, transformation, new bids, products, & services etc.

In response to the business continuity requirements, a programme of work has been initiated to develop a Business Continuity Management System (BCMS) framework, support business change and mature capability within the business.

2.2 Approach

The approach has been to deliver business owned business continuity in each directorate with the appropriate support and technical expertise in place to ensure effective delivery and on-going progress. This coupled with supporting critical projects, programmes, business change, emerging threats and incidents has both maximised the opportunity to deliver appropriate business continuity in real time activities and ensures the Post Office has the appropriate considerations and planning in place.

Based on the nature of current change, transformation and growth this approach is appropriate and effective for the current culture and direction of the organisation. This has significantly reduced potential business continuity risks, enables the successful delivery of the above activities and develops the business continuity culture within the Post Office.

The Business Continuity Steering Group (BCSG) has been established with appropriate attendance and ownership from each of the directorates (nominated by each director). This group oversees activity and make the necessary business continuity decisions for their business area.

POL00302864

2.3 Current Progress

Business continuity is progressing well at the Post Office. There has been significant success and delivery with the BCMS Framework, support to business change and incidents that have impacted the business. A selection of deliverables and successes can be seen below:

BCMS Framework:

- Executive Sponsorship agreed with General Counsel and Chief Information Officer
- Gap analysis completed and BCMS development including governance structure within the Post Office
- Development and implementation of the BCSG including business continuity sponsors / ownership for each directorate
- Business impact analysis (BIA) underway, identifying critical activities, dependencies, suppliers and recovery strategies for Post Office activities
- Business continuity plan and disaster recovery plan templates completed
- Post Office plans and service plans for client assurance / new business bids
- Embedded business continuity in the project lifecycle i.e. gating process
- Successfully reduced Post Office obligations with Santander, BT, and FoOG
- Business continuity education and awareness across the Post Office
- Finance selected to pilot business continuity planning with initial plans in place and secondary planning in scope to implement required recovery strategies

Business Change:

- Support provided to multiple projects, products and business change ensuring appropriate business continuity considerations and reduced exposure for the Post Office i.e. Titan, Wave, FoOG, Rod Fishing, SISD transformation and a wide range of separation projects
- Delivering cost effective, lean and appropriate solutions i.e. Call Centre business continuity capability at 65% cost reduction with increased recovery capability options for additional Post Office critical sites such as Chesterfield and Bolton
- Providing business continuity assurance by generating business continuity planning for Post Office client services and meeting commercial requirements i.e. successful engagement with TFL, Bank of Ireland, and RBS etc.
- Completion of business continuity framework and planning for FoOG that achieved a flawless audit certification to ISO27001 and enabled the Post Office to meet challenging contractual obligations
- Delivering business continuity to ensure PCI compliance / certification
- Leading business continuity work stream in partnership with service management to ensure ATOS have appropriate planning, processes and capability in line with Post Office requirements and contractual schedules.

POL00302864

Incident Response:

- Managing and supporting key threats and risks within the Post Office including major incident management of industrial action throughout October to December
- Support to the business with bad weather, supplier failure, IT incidents and other emerging threats / incidents
- Developing the Post Office processes / incident response maturity

2.4 Next Steps

The section below demonstrates the key business continuity related activities and deliverables during the next 6 – 9 months

BCMS:

- Completion of the business impact analysis
- Prioritisation of critical activities and agreement of recovery requirements with BCSG
- Support business leads in generating business continuity plans
- Develop business recovery teams
- Exercise business continuity plans and recovery teams
- Deliver recovery solutions / strategies i.e. third party capability
- Develop processes and procedure that support delivery of business continuity
- Develop and deliver an enduring business continuity model at the Post Office
- Individual ExCo member updates throughout June and July
- Complete Finance pilot and deploy similar approach to the remaining directorates

Business Change:

Provide Business continuity expertise and guidance to critical projects / products / business change by:

- Ensuring appropriate considerations and deliveries for business continuity
- Lean and effective capability from both Post Office and its suppliers
- Cost effective solutions supported with comprehensive commercials
- Informed, accountable risk based decisions in line with developing Risk Framework
- Support separation and IT transformation to ensure supporting dependences and suppliers have appropriate business continuity capability that meets Post Office requirements, gives assurance in line with business continuity plans and reduces risk exposure / impacts of interruption
- Call Centre separation business continuity final delivery
- Implement updated BC incident management process / response, including supporting ATOS partnership and bridge between the two organisations.

3. Recommendations

The committee is requested to note the progress to date in Business continuity and agree that future updates will be provided to R&CC through 2014.

David Epstein
20th March 2014

POL00302864

Strictly Confidential

PAPER EIGHT

RISK AND COMPLIANCE COMMITTEE

Policies for Approval

1. Purpose

The committee is requested to approve the attached policies listed below.

2. List of policies for approval

The following ten policies are submitted to the Risk & Compliance Committee for approval as part of the policy governance process

- Post Office Closed Circuit Television (CCTV) Deployment
  This policy defines the standards and the framework for the deployment of CCTV throughout the Post Office including the CViT fleet. It ensures that all Post Office employees, agents/Sub-postmaster's (SPMR) and contractors are aware of the framework.

- Post Office Fraud and Loss Prevention
  This policy outlines the framework and the management of fraud and loss prevention within Post Office. It sets out roles and responsibilities for all Post Office employees, agents/Sub-postmaster's (SPMR) and contractor.

- Post Office ID Cards
  This policy identifies how the use of Post Office ID cards is managed within Post Office cash centres, depots and central support sites.

- Post Office Lone Worker
  This policy outlines the framework for the security protection of those employees and agents/SPMR that are at an increased security risk. It identifies who it applies to and how the risk to lone workers is managed.

- Post Office Overseas Travel Security
  This policy identifies the framework and raises the awareness of the security of all individuals whilst conducting business travel overseas.

- Post Office Physical Security
  This policy addresses the management of physical security risks and threats to Post Office and sets out the framework for how this is managed to ensure the security protection of the Post Office estate, its people, brand, products and reputation.

- Post Office Security Incident Management
  This policy lays out the framework for the management of security incidents in Post Office. It identifies the security role in the management of incidents and ensures that all Post Office employees, agents and contractors are aware of the requirements in the framework.

- Post Office Tiger Kidnap and Hostage
  This policy outlines the Post Office response and management of tiger kidnap and hostage incidents. It raises the awareness all Post Office employees and agents/SPMR of the management and aftercare of individuals who are subject to the threat of tiger kidnap or hostage.

POL00302864

Strictly Confidential

PAPER EIGHT

- Post Office Corporate Cards Purchasing
  This policy provides guidance on the issue, use and management of corporate purchasing cards. It outlines the framework for the cards including governance, roles and responsibilities and the expectations of cardholders and their line managers.

- Post Office Procurement
  This policy sets out how Post Office will procure goods and services and lays out the framework for all procurement and sourcing activities. It identifies the guiding principles for procurement activity to ensure that this provides the best possible value, is executed in a fair, objective and transparent way, is compliant with Public Procurement Legislation and uses best practice methods to achieve agreeable ethical standards.

3. Policy Governance

All new and updated policies are submitted to the R&CC for approval and then forwarded to the next available ExCo for final endorsement. Once policies have been through the full approval process they will be made available to the business via the intranet library.

4. Recommendation

The Risk & Compliance Committee is requested to approve the policies attached.

Dave Mason
20th March 2014

POL00302864

INTERNAL

Post Office Closed Circuit Television (CCTV) Deployment Policy

Document Control

Overview

Owner:	Head of Security	Enquiry point:	Head of Security
Version:	0.3	Effective from:	
Last updated	30 Jan 14	Last review date:	
Review period:	Annually or major change		

Revision History

Version	Date	Author	Changes
0.1	15 Jan 14	Terry Folkman	Initial draft
0.2	20 Jan 14	Terry Folkman	Inclusion of Compliance paragraph
0.3	30 Jan 14	Terry Folkman	Remove "Operating Board" from para 4

POL00302864

1 Purpose and Statement

The purpose of this policy is to define the standards and framework for CCTV deployment throughout the Post Office estate and its CViT fleet.

2 Goals

The goals of this Policy are to;

- Support the delivery of the Post Office Security Vision.
- Address the management of CCTV deployment throughout the Post Office estate and CViT fleet.
- Ensure that all Post Office employees, agents/Sub-postmaster's (SPMR) and contractors are aware of the framework for the deployment of CCTV.

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. This responsibility is devolved through the Head of Physical Security to the Physical Security Strand on a day-to-day basis.

All employees, agents/SPMR and contractors are strictly responsible for maintaining a standard of physical security sufficient to enable them to meet the obligations laid down for the safe keeping of cash, stock and all other Post Office property and documents, whether held in their care or that of their assistants, on a 24hr basis.

5 Policy Statement

5.1 Post Office Estate

CCTV deployment is determined by;

- Risk – If the perceived level of risk increases then CCTV may be installed
- Return on investment – Cost measured against potential financial benefit of loss reduction
- Response – Following an incident, where lack of CCTV may have been a contributory factor
- Crown Transformation Programme – All Crown offices are to have CCTV installed
- Network Transformation Programme – All main offices deemed to be at high risk of robbery are to have CCTV installed

CCTV is deployed in order to;

- Capture images of individuals committing criminal acts against Post Office during business hours.
- Gather evidence in the event of any criminal prosecution.
- To act as a visual deterrent to criminals.
- To assist in access control where face to face visual recognition cannot be achieved.

POL00302864

CCTV systems must not capture or view images of Personal Identification Number Pad operations, in accordance with Payment Card Industry Security Regulations and LINK Automated Teller Machine Banking Scheme.

5.2 Post Office CViT

Post Office CViT CCTV installation is determined by;

- Risk – If the perceived level of risk increases then CCTV may be installed
- Return on investment – Cost measured against potential financial benefit of loss reduction
- Age of vehicle – All new build vehicles will have CCTV as a standard specification

Post Office CViT CCTV is deployed in order to;

- To capture images of individuals committing criminal acts against Post Office CViT.
- Gather evidence in the event of any criminal prosecution.
- To act as a visual deterrent to criminals.
- To provide witness in the event of a road traffic accident.
- For crew protection in the event of suspicious activity, such as loose loading or unauthorised personnel on a vehicle.

5.3 CCTV General

All CCTV systems are to;

- Be installed in accordance with the relevant British Standard (except systems purchased and installed by the SPMR or Multiples partner)
- Be operated in accordance with the Data Protection Act 1998, the Human Rights Act 1998 and British Security Industry Association Codes of Practice.
- Undergo annual maintenance inspections (except still-shot systems).
- Be compliant with the Bank of England Security Standards for the Note Circulation Scheme, where applicable.

CCTV systems will not be;

- Continually monitored, except where it is used as part of the access control system or is installed within certain Depots or Cash Centres.
- Continually recorded and retained. Some CCTV systems only record after being triggered by an alarm. Retention periods will vary due to the purpose of the CCTV system.

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 SGF. The appropriateness of these exceptions will be considered and reviewed by the SGF on an annual basis. Evidence must be retained for the exception and the annual review.

POL00302864

8 Violations

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 will be treated as a disciplinary offence. All disciplinary proceedings will be progressed in accordance with the Post Office Code of Conduct coordinated through HR.

10 References

Data Protection Act 1998
Human Rights Act 1998
British Security Industry Association Codes of Practice
Payment Card Industry Security Requirements
LINK Automated Teller Machine Banking Scheme
Bank of England Security Standards of the Note Circulation Scheme

POL00302864

INTERNAL

Post Office Fraud and Loss Prevention Policy

Document Control

Overview

Owner:	Head of Security	Enquiry point:	Head of Security
Version:	0.3	Effective from:	
Last updated		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	24 Jan 14	Sally Smith	Changes to 5.2
0.3	27 Jan 14	Terry Folkman	5.2 Prevention – insert “mail”

POL00302864

1 Purpose and Statement

The purpose of this Policy is to outline the framework for the Post Office fraud and loss prevention measures.

Post Office is committed to preventing, detecting and reporting fraud and loss, and in co-operating with the police and other appropriate authorities in the investigation and prosecution of those responsible.

2 Goals

The goals of this Policy are to;

- Support the delivery of Strategy 2020 and the Post Office Security Vision.
- Address the management of fraud and loss prevention throughout Post Office.
- Ensure that all Post Office employees, agents/SPMR and contractors are aware of the framework for the prevention of fraud and loss in the Post Office.

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.

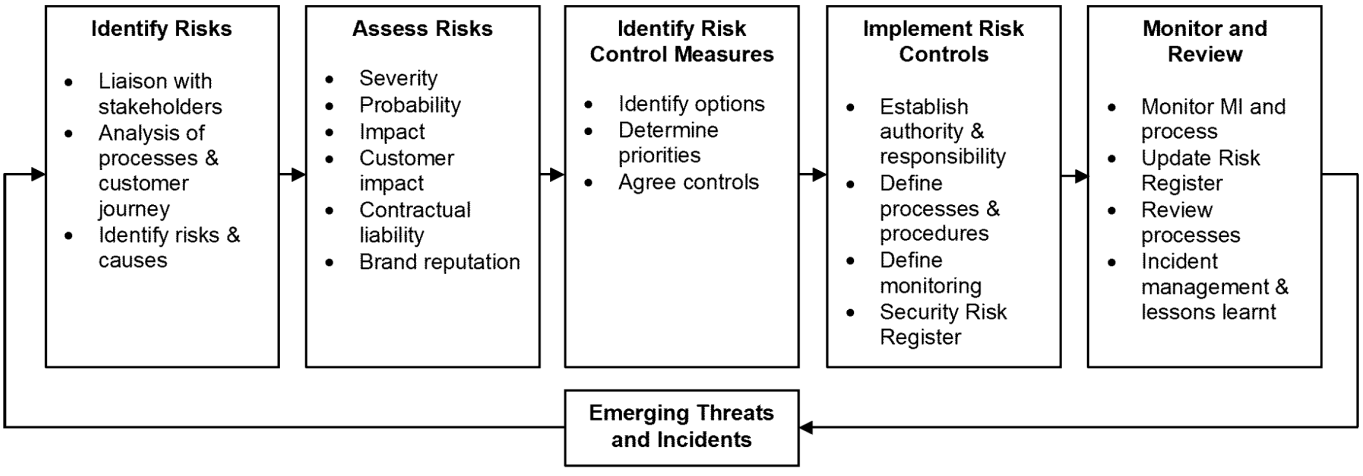
4 Roles and Responsibilities

Post Office Security are responsible for setting Fraud and Loss Prevention Policy, and establishing a risk-based framework of standards and controls. The Business is responsible for applying and following the Fraud and Loss Prevention Policy. Any exceptions to the Fraud and Loss Prevention Policy must be authorised by Security.

5 Policy Statement

5.1 Fraud Risk Management Cycle

The risk of fraud within the Post Office is managed using the following Fraud Risk Management Cycle.



POL00302864

5.2 Prevention, Detection, Investigation and Lessons Learnt:

- Prevention - Product and Service Fraud Risk Assessments; Post Office Security is responsible for establishing and deploying a framework of standards and controls across the business to ensure adequate fraud risk assessments for all new products and services deployed (Branch, Internet, Mail or Contact Centre) and any new/emerging threats identified for existing products and services. Fraud deterrent/loss reduction programme activity will be developed and deployed by Post Office Security to target high risk areas.
- Detection – Transaction and Event Monitoring; Post Office Security will undertake transaction and event/issue monitoring to detect internal and external fraud or loss across high risk modus operandi, working with key internal and external stakeholders to facilitate early intervention
- Investigation; in cases where fraud is uncovered and good evidence of criminality exists, a criminal investigation will be undertaken by Post Office Security. As a non-police prosecuting agency the Post Office is subject to the codes of practice and statutory requirements of the Police and Criminal Evidence Act 1998. In cases of monetary loss to Post Office, where it is assessed as appropriate to do so, a financial investigation will be undertaken to recover assets. Post Office Security will also investigate other incidents that may affect business brand or reputation, fraud cases raised by clients and suppliers, and certain cases arising from the employee grievance and disciplinary procedure.
- Lessons learnt; following incidents, cases and programmes, autopsies will be conducted by Post Office Security (in conjunction with internal and external stakeholders, where appropriate) to inform revised product and service process design, future analysis, data and transaction monitoring, investigation or fraud/loss reduction programme activity.

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 SGF. The appropriateness of these exceptions will be considered and reviewed by the SGF on an annual basis. Evidence must be retained for the exception and the annual review.

8 Violations

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 will be treated as a disciplinary offence. All disciplinary proceedings will be progressed in accordance with the Post Office Code of Conduct coordinated through HR.

10 References

Police and Criminal Evidence Act

POL00302864

INTERNAL

Post Office ID Cards Policy

Document Control

Overview

Owner:	Head of Security	Enquiry point:	Head of Security
Version:	0.2	Effective from:	
Last updated	30 Jan 14	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

POL00302864

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, depots and central support sites.

2 Goals

The goals of this Policy are to;

- Support the delivery of the Post Office Security Vision.
- Address 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. This responsibility is devolved through the Head of Physical Security to the Physical Security Strand on a day-to-day basis.

All employees and contractors employed within Post Office central support sites, cash centres and depots also have a responsibility to ensure that only bone 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.

5.1 Service Provider

The service provider will provide photographic ID cards for Post Office employees and contractors and non-photographic ID cards for visitors and "staff." Granting appropriate electronic access rights 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.

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.

POL00302864

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 a monthly report detailing this.

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 Central Support Sites

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.

All visitors to central support sites, 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.

POL00302864

5.4 Line Managers'

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 SGF. The appropriateness of these exceptions will be considered and reviewed by the SGF on an annual basis. Evidence must be retained for the exception and the annual review.

8 Violations

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 will be treated as a disciplinary offence. All disciplinary proceedings will be progressed in accordance with the Post Office Code of Conduct coordinated through HR.

10 References

Post Office ID Card Management Procedure
Post Office ID and Access Card Application Form
Post Office Leavers Checklist

[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.

POL00302864

INTERNAL

Post Office Lone Worker Policy

Document Control

Overview

Owner:	Head of Security	Enquiry point:	Head of Security
Version:	0.4	Effective from:	
Last updated	30 Jan 14	Last review date:	
Review period:	Annually or major change		

Revision History

Version	Date	Author	Changes
0.1	14 Jan 14	Terry Folkman	Initial Draft
0.2	20 Jan 14	Terry Folkman	Inclusion of Compliance paragraph
0.3	24 Jan 14	Terry Folkman	Change to Policy statement – delete "training" insert "user guide"
0.4	30 Jan 14	Terry Folkman	Para 10 remove "PO", insert "Post Office"

POL00302864

1 Purpose and Statement

The purpose of this Policy is to outline the framework for the security protection of those employees and agents/SPMR that are at an increased security risk.

2 Goals

The goals of this Policy are to;

- Support the delivery of the Post Office Security Vision.
- Address the management of risks to lone workers.
- Ensure that all Post Office employees, agents/SPMR and contractors are aware of the framework for the security of individuals who are subject to an increased security risk.

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

Accountability and responsibility for the security of those individuals issued with a Lone Worker Protection Device rests with the Head of Security.

5 Policy Statement

The safety and well-being of all Post Office employees and agents/SPMR is paramount and Post Office will do its utmost to ensure that it provides appropriate physical security measures to help achieve this.

Where a risk assessment dictates, individuals will be issued with a Lone Worker Protection Device and a user's guide. This device is to be operated in accordance with the instructions within the user guide.

All individuals who will operate a Lone Worker Protection Device are to complete a Personal Profile, which is to be securely despatched to Grapevine, who in turn will ensure that all personal data is stored securely in accordance with the Data Protection Act 1998.

All queries in relation to the issue, receipt or operation of a Lone Worker Protection device are to be addressed to Grapevine.

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).

POL00302864

7 Exceptions

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

8 Violations

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 will be treated as a disciplinary offence. All disciplinary proceedings will be progressed in accordance with the Post Office Code of Conduct coordinated through HR.

10 References

Post Office Security Operations Manual
Data Protection Act 1998

POL00302864

INTERNAL

Post Office Overseas Travel Security Policy

Document Control

Overview

Owner:	Head of Security	Enquiry point:	Head of Security
Version:	0.3	Effective from:	
Last updated	30 Jan 14	Last review date:	
Review period:	Annually or major change		

Revision History

Version	Date	Author	Changes
0.1	15 Jan 14	Terry Folkman	Initial draft
0.2	20 Jan 14	Terry Folkman	Inclusion of Compliance paragraph
0.3	30 Jan 14	Terry Folkman	Insert para 10

POL00302864

1 Purpose and Statement

The purpose of this Policy is to ensure that all Post Office employees, including contractors, are aware of the framework for security whilst conducting business travel overseas.

2 Goals

The goals of this Policy are to;

- Support the delivery of the Post Office Security Vision.
- Address the management of personnel security risks to overseas business travellers.
- Ensure that all Post Office employees, agents and contractors are aware of the framework for overseas travel security.

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 overall responsibility for ensuring the security of all Post Office employees and contractors who conduct business travel overseas on behalf of Post Office. This responsibility is devolved through the Head of Physical Security to the Physical Security Strand on a day-to-day basis.

All individuals who conduct business travel overseas on behalf of Post Office have a primary responsibility for their own personal security.

5 Policy Statement

Post Office is committed to maintaining the highest standards of security throughout its operations. It is the aim of the company to provide appropriate risk assessed security measures to protect all aspects of business in a cost effective, fit for purpose and proactive manner. This commitment extends to the security of all Post Office employees and contractors who travel overseas to conduct business on behalf of Post Office.

In order to highlight any increase in security risk to overseas business travellers and to correctly manage that risk, all Post Office employees and contractors must book their travel at the earliest opportunity.

CTE is the Post Office supplier of business travel services and as such it is incumbent on them to inform RMG Security of all intended overseas travel within 24hrs of notification. RMG Security will in turn inform Post Office Security within 24hrs of their notification.[i]

Post Office Security will supply the traveller with travel security advice specific to the intended destination(s). They will also supply a Request for Travel Details form that will be utilised in the event of an emergency. Security will safeguard the details supplied in accordance with the Data Protection

POL00302864

Act 1998 and Post Office Information Security guidelines and will ensure secure destruction of the details on return of the business traveller.

In the event of an emergency that affects business travellers, the travel details that have been supplied will be utilised to ensure that appropriate and timely contact with the business travellers is made and steps are taken to provide for their safety. This may include emergency medical assistance or even evacuation.

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 SGF. The appropriateness of these exceptions will be considered and reviewed by the SGF on an annual basis. Evidence must be retained for the exception and the annual review.

8 Violations

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 will be treated as a disciplinary offence. All disciplinary proceedings will be progressed in accordance with the Post Office Code of Conduct coordinated through HR.

10 References

Data Protection Act 1998

[i] Post CTE contract review in November 2014 the supplier of business travel services will inform Post Office Security directly within 24hrs.

POL00302864

INTERNAL

Post Office Physical Security Policy

Document Control

Overview

Owner:	Head of Security	Enquiry point:	Head of Security
Version:	0.3	Effective from:	
Last updated	30 Jan 14	Last review date:	
Review period:	Annually or major change		

Revision History

Version	Date	Author	Changes
0.1	14 Jan 14	Terry Folkman	Initial draft
0.2	20 Jan 14	Terry Folkman	Inclusion of Compliance paragraph
0.3	30 Jan 14	Terry Folkman	Minor changes to para 4, 5.2, 5.4, 5.5 & 10

POL00302864

1 Purpose and Statement

This Policy is to support the delivery of the Post Office security vision by setting the framework for the physical security protection of the Post Office estate, people, products, brand and reputation.

2 Goals

The goals of this Policy are to;

- Support the delivery of the Post Office Security Vision.
- Address the management of physical security risks and threats faced by Post Office.
- Ensure that all Post Office employees, agents/SPMR and contractors are aware of the framework for the physical security protection of the Post Office.

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. This responsibility is devolved through the Head of Physical Security to the Physical Security Strand on a day-to-day basis.

5 Policy Statement

The Post Office has an eight point framework for the physical security of its employees, agents/SPMR, property, information, brand and reputation;

5.1 Operational Security Management

The extent to which branches and other premises are protected by physical security measures is dictated by contractual requirements, governmental security requirements, legal obligations, risk assessments, business continuity, crisis management and industry best practice.

Physical security procedures and instructions are written in order to assist SPMR, operators and staff in the operational security management of their branches or premises. As such, these procedures and instructions are to be adhered to at all times.

5.2 CCTV Management

Post Office has installed CCTV systems at various branches across the estate. These systems must be managed and operated in accordance with the instructions within the Post Office CCTV Deployment Policy and the Security Operations Manual.

POL00302864

Non-Post Office installed CCTV systems and CCTV systems installed in central support and supply chain locations must be managed and operated in accordance with the Post Office CCTV Deployment Policy and a written local procedure,

All CCTV systems and their subsequent recordings, regardless of location or installation source, are to be operated in accordance with the DPA, the Human Rights Act 1998, PCI Security Requirements and the LINK ATM Banking Scheme.

5.3 Burglar Alarm Management

In accordance with the Security Operations Manual, burglar alarms are installed at various Post Office premises. Each branch with an alarm must have a set of operating instructions specific to the type of alarm that has been installed and these instructions are to be adhered to at all times.

All alarm installations must comply with the relevant British Standard.

5.4 Access Control Management

Access to branch secure areas will only be given to formally identified and authorised persons, whether Post Office employees, contractors or visitors. Access must be controlled in accordance with the Post Office Security Operations Manual.

Access to central support and supply chain locations must be controlled in accordance with a written local policy, which must include a formal authorisation and identification procedure. Furthermore, a procedure must be deployed to ensure that all staff, contractors and visitors shall at all times be recognisable by the wearing of a photographic identity card (staff and contractors) or a visitor's badge.

A procedure must be deployed to ensure that all Post Office employees, agents/SPMR and contractors must at all times observe the access control arrangements of any building in which they are working or visiting. Employees and contractors have a duty to maintain this security process in a robust and continuous manner.

5.5 Branch Format Management

The security format of a branch is defined by risk. Risk assessments are conducted by the Security Analytical Team and the format of individual branches is defined by the outcome of this assessment and in accordance with the guidance within the Design Manual documentation. Thereafter, any changes to branch format will only occur following an updated branch risk assessment.

5.6 ATM Protection Management

The Bank of Ireland has installed ATMs at many branches across the Post Office estate; some of these ATMs are serviced directly by CViT, whilst others are serviced by branches themselves following delivery of cash by CViT. To ensure the physical security of each ATM across the Post Office estate, branches must adhere to the security instructions within the Post Office Security Operations Manual.

POL00302864

5.7 Safe Management

Regardless of safe type it is incumbent on Branch Managers and all operators to ensure that the safe(s) that they have installed operate correctly and are used for their designated purpose. To ensure the physical security of each safe, branches must adhere to the security instructions within the Post Office Security Operations Manual.

5.8 Other Physical Security Tools Management

All other security tools are installed as a result of the risk assessment process. It is incumbent on Branch Managers and all operators to ensure that, the tools function correctly, they are used for their designated purposes and are operated in accordance with the security instructions within the Post Office Security Operations Manual.

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 SGF. The appropriateness of these exceptions will be considered and reviewed by the SGF on an annual basis. Evidence must be retained for the exception and the annual review.

8 Violations

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

9 Enforcement

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

10 References

This Policy has the following references;

- Post Office Security Operations Manual.
- Post Office Design Manual
- Data Protection Act 1998
- Payment Card Industry Security Requirements
- LINK ATM Banking Scheme
- Human Rights Act 1998

POL00302864

INTERNAL

Post Office Security Incident Management Policy

Document Control

Overview

Owner:	Head of Security	Enquiry point:	Head of Security
Version:	0.3	Effective from:	
Last updated	30 Jan 14	Last review date:	
Review period:	Annually or major change		

Revision History

Version	Date	Author	Changes
0.1	15 Jan 14	Terry Folkman	Initial draft
0.2	20 Jan 14	Terry Folkman	Inclusion of Compliance paragraph
0.3	30 Jan 14	Terry Folkman	Para 10 remove "PO", insert "Post Office"

POL00302864

1 Purpose and Statement

The purpose of this policy is to set out the framework for security incident management within Post Office.

2 Goals

The goals of this Policy are to;

- Support the delivery of the Post Office Security Vision.
- Address the management of security incidents.
- Ensure that all Post Office employees, agents/SPMR and contractors are aware of the framework for the management of security incidents.

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

Post Office accountability and responsibility for security management during incidents rests with the Head of Security, who is also a member of the Business Protection Team (BPT). Depending on the type and scale of the incident, overall responsibility may rest with the emergency services or even a governmental department/agency.

The Crisis Management Team (CMT) is responsible for coordinating the handling of security incidents on behalf of Post Office and will ensure full and timely cooperation with emergency services. The Head of Security is the CMT lead, a Senior Security Manager will act as Log Keeper and other CMT members will be nominated by the CMT Lead as necessary.

5 Policy Statement

Incidents that impact on business may also have an impact on security. Therefore security has a role to play in the formulation of any business continuity or crisis management plans and in the provision of advice to the business.

The Post Office Business Continuity and Crisis Management Policy details the major incident management process which defines key responsibilities and accountabilities. There are three levels of response dependent on the severity of the incident;

- Level 1 – Live Service Continuity Team control and manage all incidents.
- Level 2 – Business Protection Team support with the management of a medium/high severity incident.
- Level 3 – Major Incident Escalation Group support with the management of a medium/high severity incident.

It is likely that a security response will only be required for level 2 and level 3 incidents.
The underlying principles for responding to and managing an incident which impacts on the security of Post Office are;

POL00302864

- Preservation of life – The safety and welfare of all employees, agents/SPMR, their immediate families and customers during an incident is paramount. Post Office will take all appropriate steps to ensure this.

- Preservation of assets – Second only to personnel security is the Post Office emphasis on the security of its property, brand and reputation.

- Emergency services primacy – In the event of any incident that involves the emergency services the Post Office will cooperate fully with any requests made upon them in a timely manner.

As security incidents may manifest themselves in many forms, so the response to them will be equally varied. This response may utilise one individual within Security or it may utilise the CMT and a number of individuals as directed by the CMT. Decisions on the appropriateness of response will be taken as and when security incidents occur and will be in accordance with the Critical Threat and Serious Incident Escalation Management Process and other Post Office Security Policies.

Post Office will not always receive warning prior to an incident. However, when any warning or threat increase is received, either through business or emergency service/government liaison, then this warning will be disseminated throughout the business, as appropriate, by the BPT or by Security under the direction of the Head of Security, as the CMT Lead.

In the event of an incident which impacts on the security of the Post Office there is to be no unauthorised contact with the media by any Post Office employees, agents/SPMR or contractors. All media enquiries must be co-ordinated by the CMT lead.

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 SGF. The appropriateness of these exceptions will be considered and reviewed by the SGF on an annual basis. Evidence must be retained for the exception and the annual review.

8 Violations

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 will be treated as a disciplinary offence. All disciplinary proceedings will be progressed in accordance with the Post Office Code of Conduct coordinated through HR.

10 References

Post Office Business Continuity and Crisis Management Policy
Post Office Critical Threat and Serious Incident Response Management Process

POL00302864

INTERNAL

Post Office Tiger Kidnap and Hostage Policy

Document Control

Overview

Owner:	Head of Security	Enquiry point:	Head of Security
Version:	0.3	Effective from:	
Last updated	30 Jan 14	Last review date:	
Review period:	Annually or major change		

Revision History

Version	Date	Author	Changes
0.1	14 Jan 14	Terry Folkman	Initial draft
0.2	20 Jan 14	Terry Folkman	Inclusion of Compliance paragraph
0.3	03 Feb 14	Terry Folkman	Delete "aftercare" para insert "ransom payment" para

POL00302864

1 Purpose and Statement

There are two broad groups of kidnap threats. Conventional kidnap involves the taking and protracted holding of a person, against a demand for ransom, usually from the victim's family or employer. The second type involves the short-term hostage taking of family members of someone who has immediate access to cash or valuables. The captives are frequently held overnight and the aim of the criminals is to frighten their victims to such a degree that they will not contact the Police, even when, as often happens, they have an opportunity to do so. This is referred to as a tiger kidnapping.

The purpose of this Policy is to outline the Post Office response to tiger kidnap and hostage incidents.

2 Goals

The goals of this Policy are to;

- Support the delivery of the Post Office Security Vision.
- Address the management of personnel security risks and threats faced by Post Office.
- Provide awareness to all Post Office employees and agents/SPMR of the management and aftercare of individuals who are subject to the threat of tiger kidnap or hostage.

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

Responsibility for the management of all tiger kidnap or hostage incidents rests with the relevant police authorities. Post Office accountability and responsibility rests with the Head of Security who will lead the Post Office response to an incident. The Crisis Management Team (CMT) is responsible for coordinating the handling of incidents on behalf of Post Office and will ensure full and timely cooperation with emergency services. A Senior Security Manager will act as Log Keeper and other CMT members will be nominated by the CMT Lead as necessary.

5 Policy Statement

The safety and welfare of all employees, agents/SPMR, their immediate families and any other individuals affected by a tiger kidnap or hostage incident is paramount. This principle is entirely consistent with police aims, who have primacy in all tiger kidnap or hostage incidents. Post Office will comply fully with kidnap demands, on police advice, if that is considered the best means of ensuring the safety of any individual involved in a tiger kidnap or hostage incident.

The primary principles of this Policy are the safety of any hostage that has been taken, the safety of anyone else who may be involved and the provision of adequate aftercare for all those directly or indirectly involved in a tiger kidnap or hostage incident. In satisfying these principles Post Office will;

- Ensure employees and agents/SPMR, Grapevine and CMT operatives are familiar with procedures to be used and are given appropriate training on a regular basis
- Ensure that employee and agent/SPMR Tiger Kidnap risk assessments are conducted on an annual basis in accordance with the Bank of England Security Standards for the Note Circulation Scheme

POL00302864

- Provide immediate essential information and give full cooperation to the police
- Provide immediate professional advice and support to employees, agents/SPMR and their immediate families both during and after a tiger kidnap or hostage incident

All Post Office employees and agents/SPMR are advised to consider the best course of action according to individual situations as they occur. Post Office encourages individuals to contact the appropriate emergency contact free phone numbers immediately they become aware of or have suspicion that a tiger kidnap or hostage incident has occurred or may occur. Details of the escalation process for tiger kidnap and hostage incidents are contained within the Critical Threat and Serious Incident Escalation Management Process document.

In the event of a tiger kidnap or hostage incident the Post Office CMT will be activated. They will coordinate with emergency services and make decisions on behalf of Post Office. If, on consultation with UK Law Enforcement, immediate monetary funding is required in extreme circumstances to support their activities, then authority to sanction this rests with the Post Office Chief Finance Officer or General Counsel. If time constraints do not permit this then the Head of Security can authorise a payment not exceeding £250k.

There is to be no contact with the media by any Post Office employees or agents/SPMR. All enquiries in relation to a tiger kidnap or hostage incident must be co-ordinated by the Head of Security as the CMT lead.

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 SGF. The appropriateness of these exceptions will be considered and reviewed by the SGF on an annual basis. Evidence must be retained for the exception and the annual review.

8 Violations

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 will be treated as a disciplinary offence. All disciplinary proceedings will be progressed in accordance with the Post Office Code of Conduct coordinated through HR.

10 References

This Policy has the following references;

- Critical Threat and Serious Incident Escalation Process
- Bank of England Security Standards of the Note Circulation Scheme

POL00302864

PP1 - Post Office Procurement Policy

The purpose of this policy is to set out the way in which the Post Office will procure goods and services.

POL00302864

1 Introduction

Post Office spent in the region of £500m on goods and services from third parties in the financial year 2012/2013. From an operational and commercial perspective, the management of this expenditure is critical in achieving the profitability.

1.1 Policy objective

The purpose of this policy is to ensure all procurement and sourcing activities carried out by POL provide the best possible value, are executed in a fair, objective and transparent way, are compliant with Public Procurement Legislation, use best practice methods to achieve agreeable ethical standards and are aligned and support POL's Business-wide Strategies.

Compliance with the policy is mandatory for all directorates in Post Office.

1.2 Procurement definition

This policy addresses the principles of Procurement; Sourcing and Selecting Vendors; Authority to Contract, Authority to Order, Contract Management and managing excellent Vendor Performance at Post Office.

1.3 Scope of application

Only employees with delegated procurement authority are allowed to commit expenditure to third parties. Any other employee must not conduct any procurement activities unless specifically instructed by the Head of Procurement. In particular, employees who maybe engaged in procurement activities are required to familiarise themselves with the content of this policy and the other related documents PP2-PP4.

In the case of agencies and consultancies all contracted personnel working on behalf of POL shall be made aware of this policy and shall comply.

This policy does not apply directly to outsourced service providers or to suppliers; however, it does seek to ensure our outsourced service providers and suppliers must: support the governance of POL; mitigate the risks faced by POL; and support the quality of service we provide to our customers.

1.4 Compliance with this Policy

Compliance with this policy will be assessed by the Best Practice Procurement Team and reported annually to the Risk & Compliance Committee, and the Audit & Risk Committee as requested.

1.5 Policy Owner

The policy owner for this policy is the Best Practice Procurement Manager, who has:

- overall accountability and responsibility for setting and maintaining the Policy and for monitoring compliance with the Policy;

POL00302864

- responsibility for ensuring that the Policy remains up to date and relevant for the Post Office

1.6 Policy Revision

This policy must be reviewed and approved by the Post Office ExCo via the Risk & Compliance Committee on an annual basis. All revisions must be fully documented in the 'modification history' section of this document.

Relevant procedures must be updated to conform to the policy and updated within three months from the date of approval by the Post Office Board, and changes to the policy must be communicated to all relevant staff and those listed in the distribution section of this document.

2 Procurement Policy

2.1 Guiding Principles

Procurement shall be driven by the following Guiding Principles. In all procurement activities, POL shall:

- **Apply a Commercial Approach**; actively seek to promote competition in respect to goods & services purchased from third party vendors, and conduct purchasing activities in an objective manner, providing transparency and documentation as required.

- **Promote the adoption of performance specifications**, ensuring that goods and services are fit for purpose and provide effective and efficient commercial arrangements for standard products and services across the business.

- **Achieve sustained value** by achieving the best possible value and seeking continuous improvement

- **Establish effective governance and control** in the supply chain by conducting procurement activities in a manner that satisfies the requirements of internal control, fulfils POL's legal and financial obligations and effectively manages commercial risk

- **Create and maintain good supplier relationships** with key stakeholders recognising that to achieve the best possible value, strong relationships must be developed and managed with suppliers.

- **Meet the obligations of corporate social responsibility,** by considering social, ethical and environmental impact, promoting the adoption of appropriate HS&E standards and in writing specifications for the purchase, handling and disposal of goods.

POL00302864

2.2 Roles & Responsibilities

Procurement shall drive the procurement process, negotiate commercial arrangements, and govern the means by which procured solutions are delivered.

The Head of Procurement has the authority to delegate Procurement Authority to named individuals; the decision to proceed with expenditure shall be made by a responsible manager or committee under delegated authority. Overall, the authority to commit the company to purchase goods and services from a specific vendor rests with Procurement.

Procurement and its stakeholders shall undertake vendor selection in a manner that is fair, rigorous, transparent, objective, and in accordance with the strategy for the category of such spend. Competitive tenders shall be the vendor selection method of choice. Competition shall be administrated in an open manner with contracts awarded on the basis of criteria established prior to tendering. The evaluation process used to make contract award decisions shall balance quality against cost to provide the optimum value for money outcome.

The spend level below which a formal Procurement contract is not normally required is £50,000, and this is outlined in the delegated authority policy; Spend of this type shall be dealt with by issue of a purchase order except where purchases <£2000 and these can be acquired via a CPC transaction, as outlined in PP4 Corporate Purchasing Cards Policy.

Procurement Projects and Awards >£1m in value, must be approved by the Head of Procurement and the Head of Legal Services at the following key stages: Sourcing Strategy, Vendor Selection and Contract Award. Failure to do so shall result in recording the process as non-compliant and may be subject to disciplinary procedures.

Lead Team

Category Leads shall sign off vendor contracts in accordance with delegated authority. Any Procurement that proposes amendments to the standard POL terms and conditions must also have approval from the Category Lead, and any Procurement exceeding £50,000 that proposes entering into entire agreements as an alternative to POL standard terms and conditions, must be reviewed for risk and obtain sign-off from Legal Services.

Procurement Category Teams

Procurement shall identify opportunities to deliver benefits to POL and seek opportunities to generate revenue or reduce costs presenting these to the business with appropriate strategies.

Category Teams shall work with internal stakeholders to support the definition of requirements, evaluate potential sources of supply and develop sourcing strategies. Using a Category Management approach they will seek to engage and consult at project inception to optimise business performance and protect the interests of POL; where feasible, engagement shall be at the due diligence stage and provide assistance with business cases.

POL00302864

Category teams shall work with key vendors to develop stable, long-term partnerships that produce mutual benefits; taking responsibility for vendor performance management and ensuring vendors meet the required standards of the contracts. In all instances, VPM or contract management undertaken by stakeholders, outside of procurement, shall be agreed by the relevant Category Lead, and in such cases stakeholders shall be responsible for providing feedback on performance and delivery at an operational level.

Category teams shall identify the level of management required for each vendor relationship to protect commercial interest, and include appropriate exit strategies. The eSourcing application shall be the mandatory system for VPM carried out within Procurement, and for providing performance statistics and analytics.

FSC Buyers

eProcurement is the mandatory system for ordering goods or services at POL. Irrespective of the technical solution available, requisitions shall be approved by Finance in line with the delegated authority limits and subsequently by Procurement. FSC Buyers shall be responsible for converting approved requisitions into purchase orders and sending these to the vendor, resulting in a contractual commitment.

2.3 Measurement and Monitoring

Compliance shall be collated periodically using spend and sourcing analytics extracted from POLs eSourcing and eProcurement systems and the sourcing council minutes, by the Best Practice team and reported to the relevant category leads and line managers. It shall be the responsibility of the line managers to deal with the instances of non-compliance within their category teams and raise any disciplinary actions.

2.4 Control

2.4.1 Delegation of Authority

POL shall maintain a documented delegation of authority for Procurement and only employees with delegated procurement authority shall be permitted to make a third party commitment on behalf of the Business.

.

2.4.2 Internal Controls

POL has internal controls in place over procurement activities that ensure there is:

- more than one person involved in and responsible for a transaction end to end
- transparency in the procurement process
- a clearly documented audit trail exists
- appropriate authorisations are obtained and documented

These internal controls are documented in PP2 Authority to Requisition, Procure and Pay Policy, Sourcing Council Delegated Authorities V3.0 and within the workflows in the mandatory eSourcing system.

POL00302864

POL is committed to upholding ethical and responsible business, and this principle shall be reflected in POL's relationship with its vendors. Procurement activities shall support handling of commercially sensitive or confidential information and ensure it is acquired, stored, processed and published appropriately, and in accordance with POLs Data Protection Policy V3 and Guidance on the Freedom of Information Act 2000.

In line with the Code of Business Standards & Post Office Anti-Bribery Policy, under no circumstances should a decision maker involved in a procurement decision, or a close family member, have a financial interest in the selected vendor, unless such involvement is disclosed and explicitly approved by the Head of Procurement. A conflict of interest may be real or perceived, but nonetheless should be managed to ensure that POL is and is seen to be, beyond reproach.

Reciprocal trading shall be strictly prohibited. Whilst contracts may be placed with vendors who are also customers, the decision to award a contract must be taken based purely on the commercial merit of each individual contract.

2.5 Risk Management

All procurement activities shall adhere to the Post Office Regulatory Risk (Compliance) Policy. Procurement shall ensure that risk management is appropriately applied at all stages of procurement activities. Guidance shall be made available to enable the Procurement team to employ POLs risk management principles.

Procurement activities shall be properly planned and carried out in a manner that will enhance POLs capability to prevent, withstand and recover from interruption to the supply of goods and services where commercially viable.

2.6 Subordinate policies

Subordinate policies may be required to ensure compliance with this overarching policy and should be drafted by the Best Practice Procurement Manager. Any such policies must be consistent with this overarching policy.

2.7 Governance

The overall governance of the policy sits with Procurement, with a regular audit from the IA team.

3 Accessibility

This policy and any subordinate policies are available on the Post Office intranet.

POL00302864

4 References

In this section, all the references to other documents should be mentioned, including:

Ref.	Document Name	Description	Location
1	Business Code of Conduct	Code of practice for sound management of businesses	Post Office Intranet /HR Advice & Guidance
2	PP2 – Authority to Requisition, Procure & Pay	Authorities within the process of acquiring goods & services on behalf of POL	Post Office Intranet /Policies & Guidelines
3	PP4 – Corporate Purchasing Cards Policy	Responsibilities & processes for card holders	Not issued
4	Sourcing Council Delegated Authorities V3.0	Authorities to enter in external agreements & approval of papers	Procurement
5	POLs Data Protection Policy V3	Supporting Data protection legislation in practice	Post Office Intranet /Policies & Guidelines
6	POL's Anti-Bribery Policy	Processes for avoiding fraud in the working practices	Post Office Intranet /Policies & Guidelines
7	Post Office Regulatory Risk (Compliance) Policy	Managing Risk at POL	Post Office Intranet /Policies & Guidelines

5 Glossary

The following table contains definitions for acronyms and terms used in (and specifically in the context of) this document:

Acronym	Definition	Term
eProcurement	The Core Finance System namely P2P	
eSourcing	The Sourcing System that provides eTendering capabilities	
ExCo	Post Office Executive Committee	
FSC	Finance Service Centre	
HS&E	Health, Safety & Environmental	HS&E Standards
IA	Internal Audit	IA Team
POL	Post Office Limited	
RCC	Risk & Compliance Committee	
VPM	Vendor Performance Management	

POL00302864

Version History

Date	Version	Updated by	Change summary
19/02/2014	0.1	Sara Hollingsbee	Initial draft
26/02/2014	0.2	Sara Hollingsbee	Draft for comments
04/03/2014	1.0	Sara Hollingsbee	Revision of Section 2

Document Location

Unissued.

Distribution

For Sign-off - This document has been reviewed by the following people:

Name	Title – Department	Date of Sign off
Colin Stuart	Head of Commercial Finance & Procurement	05/03/2014
Sujai Jayaram	Procurement Best Practice Lead	27/02/2014
Risk & Compliance Committee		
Executive Committee		

POL00302864

PP4 Post Office Corporate Purchasing Cards Policy

POL00302864

1 Introduction

The purpose of the Corporate Purchasing Card is to establish a more efficient and cost effective method for the purchasing and payment of low value transactions; it aims to eliminate petty cash purchases, low value cheques and low value purchase orders being issued.

The cards shall also be used where national and local call-off contracts are in place, and it has been determined as the payment method.

1.1 Policy objective

The purpose of this policy is to provide guidance to: cardholders; line managers of cardholders; and custodians of company policy involved with the issue, use and management of cards and card transactions. It aims to define policy on governance, ownership and process. The CPC works as a credit card and is as widely accepted, therefore it is imperative that people are responsible in the way they use it and what they are spending.

Compliance with the policy is mandatory for *all directorates* in Post Office.

1.2 Corporate Cards Principles

- Cards are intended for Business use only; for low value, ad-hoc purchases up to £2000
- Goods and Services should be delivered to a POL business office address, where possible
- The card is non-transferable
- The card shall not be used for cash withdrawals.
- Employees must be authorised by their Budget Holder before becoming a card holder
- Transaction and monthly credit limits shall be established for each card issued.
- Budget holders may change the card limit by applying for an increase or decrease via the CPC Co-ordinator
- The Card is not for use for travel related expenses
- Use of the Card for any purpose which is not in accordance with company policy may result in disciplinary action.

1.3 Scope of application

This policy covers the following: when to use a corporate card, spending limits; card maintenance; card security; roles and responsibilities; acceptable purchases; unacceptable purchases; and misuse and abuse of cards.

This policy does not cover corporate policy on Travel and Subsistence.

1.4 Compliance with this Policy

Compliance with this policy will be assessed by the Best Practice Procurement Manager annually and reported to the Risk & Compliance Committee, and the Audit & Risk Committee as requested.

POL00302864

1.5 Policy Owner

The policy owner for this policy is the Best Practice Procurement Manager, who has: overall accountability and responsibility for setting and maintaining the policy and for monitoring compliance with the policy; and responsibility for ensuring that the policy remains up to date and is relevant to the Post Office.

1.6 Policy Revision

This policy must be reviewed and approved by the Best Practice Procurement Manager and the FSC Client Settlements Manager on an annual basis, except where a significant change in policy requires the review and approval of POL ExCo. All consequent revisions must be fully documented in the modification history section of this document.

Relevant procedures must be updated to conform to the policy and updated following approval by the Post Office ExCo. Changes to the policy must be communicated to all relevant staff, noted in Section 4 of this policy document. Those staff listed must, in turn, ensure that the changes are cascaded to staff and/or 3rd parties as appropriate.

2 Corporate Purchasing Cards Policy

2.1 The Corporate Card Process Summary

The card process does not require competitive quotations, since all purchases shall be under £2000 and, where the requirements change to regular use, the requirement shall be referred to Procurement.

2.2 Roles & Responsibilities

Budget holders and line managers shall be accountable and liable for the integrity of everything charged to the Card, and for all transactions and proper controlled use of the CPC.

Cardholders shall be responsible for the integrity of everything charged to the Card, and for all transactions and proper controlled use of the CPC. In the instance an audit is conducted they must be able to produce receipts and invoices or proof that the transaction has occurred; where an error is discovered, cardholders shall also be responsible for showing that the error or dispute resolution has been initiated.

The CPC Co-ordinator shall be the point of contact at POL, liaise with the card provider, internally manage the account and manage the relationship with the card provider in an operational capacity.

2.3 Measurement and Monitoring

2.3.1 Card Maintenance

Name changes; card replacements, cancellations or reinstatements; cost centre changes; and department changes shall be maintained by the CPC Co-ordinator via approvals and verification from the FSC team.

POL00302864

2.3.2 Card Security

Cards, PINs and accounts shall be issued to individual employees on the basis that they take adequate responsibility for the security of the cards, never display or give their card number or PIN to anyone for the purpose of allowing anyone else to place an order with the card.

In the instance a cardholder loses or has their card stolen, they are responsible for informing the provider, as soon as they become aware of it.

2.3.3 Spending Limits

The cardholder transaction limit and monthly expenditure limits are set at either £100 or £500 on issue. Any increase to these limits shall be considered separately from the card holder application, except where this is a temporary increased limit for an ad-hoc purchase.

2.4 Control

Cards shall be assigned to one cost centre only and the number of cards per cost centre is the decision and preference of the cost centre owner. Each card is assigned a default cost centre and the cardholder can only place orders for that cost centre. All card purchases shall be recorded against a single GL code. Cards shall not be used for the purposes of withdrawing cash and purchases shall not be split resulting in a number of transactions below the threshold; such transactions shall be identifiable via the monthly MI reports.

2.4.1 Acceptable Purchases

Acceptable purchases are those purchases that will eliminate the use of petty cash, low value cheques and low value purchase orders.

- Externally arranged Seminars
- Advertisements in newspapers and magazines
- Journals, Business Periodicals and magazines
- General Stationery (low value, ad hoc, emergency purchases)
- Photographers
- Hire fees (e.g. costumes etc. for Public Relations purposes)
- Agreed Ad-hoc printing, laminating, binding jobs e.g. Prontaprint
- Courier services
- Street maps
- External Hospitality / Entertainment (Following the gifts and hospitality process published on the POL Intranet)
- Conference/Meeting <£500

Note: All conferences/meetings £500 < £2000 are to be sourced via business venue finder; payment is due directly to the venue via CPC. Conferences >£2000 require a Purchase Order via the Requisition process.

2.4.2 Unacceptable Purchases

Corporate Purchasing Cards shall not be used for Goods and Services where a Post Office Contract exists, for Travel & Subsistence i.e Train Tickets, Flights, Meals, Snacks, Petrol or Overnight Accommodation, and any of the following:

- Items exceeding the limit agreed by Budget Holder,

POL00302864

- Capital equipment
- T&S, personal travel, entertainment and group meals
- Personal items
- Consulting fees
- Lease contracts or long-term rental contracts.

2.4.3 Misuse or Abuse of Cards

Where Cards have been used for purposes which are not in accordance with company policy, the cardholder may be subject to investigation under the formal discipline procedure.

POL may investigate any fraudulent use of the Purchasing Card and where investigations uphold fraudulent use; POL shall treat this as a serious disciplinary offence, and proceed under the conduct code. Where fraudulent use of the card by the cardholder, or someone the cardholder has knowingly allowed to fraudulently use the card is detected, the card shall be cancelled immediately and necessary measures shall be taken. Fraudulent use shall be treated as gross misconduct and may result in summary dismissal.

Where a cardholder is found responsible for, or is party to the fraudulent use of the CPC, they will be required to repay the Business for any expenditure incurred. POL shall be entitled to recover the principle sum by way of a single deduction or a series of deductions from the cardholder's wages, including pay in lieu of notice or any other payment due on the termination of the employment.

POL may withdraw the cardholder's permission to use a card, at any time, whereby the card must be returned it immediately.

2.5 Subordinate policies

Subordinate policies may be required to ensure compliance with this overarching policy and should be drafted by the Best Practice Procurement Manager. Any such policies must be consistent with this overarching policy.

2.6 Governance

The overall governance of the policy sits with Procurement, with a regular monitoring from the FSC and regular auditing from the IA team.

3 Accessibility

This policy and any subordinate policies are available on the Post Office intranet.

POL00302864

4 References

In this section, all the references to other documents should be mentioned, including:

Ref.	Document Name	Description	Location
1	The Hospitality and Entertainment Approval Process	Approval Process and approval email addresses available on the POL Intranet Site.	Bribery Policy POL Intranet/ Policies & Guidance
2	Code of Conduct	HR policy providing guidance on acceptable behaviour	POL Intranet/ HR Advice & Guidance
3	Travel & Subsistence Policy	HR Policy providing guidance on booking travel and claiming expenses.	POL Intranet/ HR Advice & Guidance

5 Glossary

The following table contains definitions for acronyms and terms used in (and specifically in the context of) this document:

Acronym	Definition	Term
CPC	Corporate Purchasing Cards	
ExCo	Post Office Executive Committee	
FSC	Finance Service Centre	
GL Code	General Ledger Code	
POL	Post Office Limited	
PP4	Procurement Policy No.4	
T&S	Travel and Subsistence	

6 Version History

Date	Version	Updated by	Change summary
11/02/2014	0.1	Sara Hollingsbee	Initial draft
27/02/2014	0.2	Sara Hollingsbee	Final draft
04/03/2014	1.0	Sara Hollingsbee	Final

7 Document Location

Unissued.

POL00302864

8 Distribution

For Sign-off - This document has been reviewed by the following people:

Name	Title – Department	Date of Sign off
Rod Ismay	Head of FSC	03/03/2014
Kay Wilson	Client Settlements Manager	03/03/2014
Colin Stuart	Head of Commercial Finance & Procurement	27/02/2014
Sujai Jayaram	Procurement Best Practice Lead	27/02/2014
	Risk & Compliance Committee	
	Executive Committee	

POL00302864

Strictly Confidential

PAPER NINE

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. Employees are required to provide details of all gifts over £10 and all instances of hospitality, accompanied by evidence of their line manager's approval, to the Risk and Compliance team by e-mail (to GRO The Anti-Bribery policy and gifts and hospitality procedure has recently been reviewed and approved by the R&CC and the de minimis limit on gifts will be changed to £25.

3. Review of register

In the year to 28 February 2014, 23 reports of gifts received and 147 reports of hospitality received were made to the register (see appendix 4 for breakdown by directorate). The Financial Services directorate made the largest number of reports of hospitality received (46), of which 29 events were hosted by the Bank of Ireland.

A brief review of gift and hospitality reporting by other organisations, and other anecdotal evidence, suggest that Post Office may be recording lower volumes than is typical.

4. Action

Risk and Compliance will remind colleagues of the gifts and hospitality policy to encourage compliance with the gifts and hospitality procedure at all levels.

Dave Mason
20h March 2014

POL00302864

Strictly Confidential

PAPER NINE

Appendix 4

Summary of reports to the Gifts and Hospitality register in the year to 28 February 2014

Directorate	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)
Commercial	3	16		
Corporate Services	2	18		
CoSec	3	0		
Finance	1	21		10
Financial Services	0	46		1
HR	2	2		
IT and Change	5	8	5	2
Network and Sales	6	19		1
Office of the Chief Executive	1	17	1	17
Total	23	147	6	31

POL00302864

Post Office Ltd – Strictly Confidential PAPER TEN

Risk and Compliance Committee (R&CC)		Reference: R&CC/MIN/JAN14
Date: 20th January 2014	**Venue: POL Boardroom, 148 Old Street, London**	**Time: 13.30 – 15.30**
Attending:		
Chris Aujard	General Counsel	Chair
Chris Day	Chief Financial Officer	Member
Alwen Lyons	Company Secretary	Member
Martin Edwards	Chief of Staff	Report (for Paula Vennells)
Dave Mason	Head of Risk & Compliance	Report
Jonathan Hill	Head of Financial Services Risk	Report (for Nick Kennett)
Julie George	Head of Information Security	Report
Rob Bolton	Assurance Adviser	Secretariat
Apologies:		
Paula Vennells	Chief Executive Officer	Member
Starting February 2014:		
Neil Hayward	Group People Director	Member

Agenda Item 1

Top Business Risks

Purpose

The committee was asked to endorse the risk management approach and methodology and to provide feedback on the content and structure of future risk reporting

Discussion

The overview of ExCo risks paper was discussed and the committee reviewed each risk considering whether :

- the ExCo view was an accurate reflection of the risk
- the governance structure was appropriate for the risks
- had there been enough progress in managing the risk

An overview of the risk management approach and progress to date was provided and the committee requested an interim update on progress every 4 weeks outside of the normal committee meeting schedule. The committee provided feedback on the structure and content of risk reporting and it was agreed that the name of the business partner and the risk owner be identified in future updates. The committee also requested that consideration be given to the use of a RAG status to more clearly identify the quantum of risk.

As a general point the committee asked that consideration be given to more clearly describing the top risks in the interests of clarity – this will be reflected in subsequent reports to the committee.

The top risks were discussed by exception and the following comments made, however no significant concerns were raised:

Integrity of Horizon System
It was agreed that, whilst this is more of an issue than a risk, the progress on managing Sparrow would continue to be reported to the committee. It was noted that assurance work was being planned on Sparrow, especially with regard to its dependency on the Business Improvement Programme.

Inadequate People Capability
The committee was concerned that the risk was too focused on the capability of those currently employed rather than the mix of people and skills we need to deliver the strategic plan and a sustainable business. It was agreed that this will be followed up with the risk owner.

Data Security / Cyber Security
It was confirmed that merging the two risks had been agreed with Lesley Sewell (Chief Information Officer) and Julie George (Head of Information Security).The committee expressed concern regarding the IT capability in the R&C team and it was confirmed that a new IT Business Partner with experience in this field was due to start in February

POL00302864

Post Office Ltd – Strictly Confidential PAPER TEN

Failure to Deliver Top Line Growth
The committee requested that, for future meetings, more information was required about how the risk was being managed and controlled.

Outcomes

The committee endorsed the risk management approach and methodology

The committee provided feedback on the structure and content of future risk reporting

Actions

Ref	Action	Lead
1557	Interim update on risk management progress to be provided to the committee every 4 weeks	Dave Mason

Agenda Item 2

FS Mis-selling Focus Session

Purpose

To conduct a "deep dive" session on the management of the FS mis-selling risk

Discussion

The committee received a presentation on the FS Mis-selling risk. The committee suggested that the appropriate Risk & Compliance business partner should attend future deep dive sessions to support the risk owner.

The committee asked for more detail regarding the training and development controls and the risk owner explained that 100 mortgage specialists would be in place by April 2014 together with training & development logs retained in a central admin team in London.

The committee requested details of the 'go-live' decision for Mortgage Market Review. The risk owner explained this was performed through the Mortgage Market Review Governance Board which would be confirmed. The risk owner also confirmed that the Financial Services Sub Committee was under review and that terms of reference would be provided in due course

The Key Risk Indicator (KRI) measures were reviewed and the committee asked for more detail on how the tolerances had been calculated. The risk owner provided an explanation of how the tolerances had been identified and agreed

Outcomes

The committee performed a deep dive session on the FS Mis-selling risk

Actions

Ref	Action	Lead
1558	Confirm that the MMR Governance Board provides final sign off for mortgage product	Jonathan Hill
1559	Provide the terms of reference for the Financial Services Sub Committee once review of this forum completed	Jonathan Hill

POL00302864

Post Office Ltd – Strictly Confidential PAPER TEN

Agenda Item 3

Business Policy Approvals

Purpose

The committee was asked to approve a number of business policies as part of the agreed governance process

Discussion

Four policies had been submitted to the meeting for approval by the committee:

- Anti-Bribery
- External Data Protection
- Data Sharing
- Acceptable Use

With the exception of Acceptable Use the policies were agreed and approved for further submission to ExCo for final endorsement

It was the view of the committee that the Acceptable Use policy could not be approved until further work had been performed and it was agreed that once this had been completed an updated policy be re-submitted to a future meeting

Outcomes

The committee approved the Anti-Bribery, External Data Protection and Data Sharing policies to be submitted to ExCo for final endorsement

Actions

Ref	Action	Lead
1560	Approved policies to be submitted to next available ExCo for final endorsement	Rob Bolton
1561	Re-submit updated Acceptable Use policy to a future Risk & Compliance Committee for approval	Julie George

Agenda Item 4

Risk Events and Near Misses

Purpose

The committee was asked to note the implications of risk events and near misses and agree any recommendations to reduce the impact of similar future events

Discussion

The risk events paper was discussed at the meeting and whilst the report was well received it was agreed by the committee that future reporting should include an impact assessment for each reported event.

The committee focused on the reported business continuity related events and the committee requested a full report on the status of business continuity to be provided to the next meeting

The committee did not reach a view on the recommendations in the risk events paper and the paper relating to assurance activity was not reviewed.

Outcomes

The committee agreed future risk event reporting to continue and that it include an impact assessment for each of the reported events

The committee requested a full BCM status report to be provided to the next meeting

The committee did not reach a view on the recommendations in the risk events paper or review the assurance activity paper

POL00302864

Post Office Ltd – Strictly Confidential PAPER TEN

Actions		
Ref	**Action**	**Lead**
1562	A full BCM status report to be provided to the next meeting	Dave Mason

Agenda Item 5

Action 1552 Update

Purpose

The committee was asked to review and agree the update on the outstanding Information Security action from the last meeting

Discussion

A full update had been provided in advance and it was explained that there was a risk that the Information Security team does not have enough resource to manage the required activity. The committee agreed that the risk needed to be quantified and requested a paper to be provided to this effect, including options for Post Office and identification of the residual risk under each option.

Outcomes

The committee asked that the Information Security resource risk to be quantified

Actions		
Ref	**Action**	**Lead**
1563	Paper to be submitted to the next meeting that quantifies the Information Security resource risk, including options for Post Office and the identification of residual risk under each option	Julie George

Agenda Item 6

Risk Management Culture

Purpose

The committee was asked to endorse the progress against risk plans and suggest any further recommendations

Discussion

The risk management update that had been provided was discussed. The committee queried the pace of progress against risk plans and it was explained that whilst there had been some good progress, this could have been quicker although now the Christmas period was over it was likely that this would improve. The committee agreed that the Risk & Compliance business partners should be more challenging in their discussions with risk owners and in any reporting to the committee

The committee also considered the profile of risk management and associated risk discussions and it was confirmed that a piece of assurance work was currently being performed, in the area of governance and terms of reference, that would focus on the profile of risk management. The results of this would be reported to the next committee meeting.

Outcomes

The committee agreed and endorsed progress against risk plans
The committee agreed a governance and terms of reference assurance report to be provided to the next meeting

Actions		
Ref	**Action**	**Lead**
1564	Results of assurance work on governance and terms of reference to be reported to the next meeting	Dave Mason

POL00302864

Post Office Ltd – Strictly Confidential PAPER TEN

Agenda Item 7

Minutes and Actions

Purpose

The committee was asked to agree the previous minutes and receive updates on actions to confirm they are completed

Discussion

The committee agreed the minutes from the last meeting in October 2013 and all actions were confirmed as completed

Outcomes

The committee agreed the minutes from the previous meeting as an accurate record
The committee agreed that all outstanding actions confirmed as closed

Actions

Ref	Action	Lead
None		

Agenda Item 8

Meeting Summary & AOB

Purpose

The committee was asked to consider any other business not captured in the agenda and agree any necessary actions

Discussion

Three AOB items had been identified:
National Measurement Office
McColls Multiple Partner
Terms of Reference

National Measurement Office (NMO):
It had been identified that the scales in use at self-service kiosks need to be certified together with the linked component of the Horizon system. This was being progressed via the Crown Transformation Programme. A review of the corresponding licence for counter scales has revealed that current certification expires in 2014 and this is being progressed with the NMO. The committee requested that confirmation be provided when this certification had been achieved

McColls Multiple Partner:
The Network Transformation Programme is currently engaging with this multiple partner to convert 192 branches to new models however it was suggested that this could lead to a concentration risk of too many branches operated by this partner. The committee queried what risk assessments are conducted when working with multiple partners in the NT Programme and that a representative from the NT Programme should attend the next meeting to explain

Terms of Reference:
The terms of reference had been re-drafted to reflect the recent changes in the committee focus and membership. The updated terms of reference to be circulated by email for agreement by the membership

Outcomes

The committee requested confirmation of the certification of scales required by the NMO
The committee requested confirmation of what risk assessments are performed when working with multiple partners in the NT programme
The committee agreed that the updated terms of reference be circulated to members for agreement

POL00302864

Post Office Ltd – Strictly Confidential PAPER TEN

Actions		
Ref	**Action**	**Lead**
1565	Report to be provided for the next meeting to explain what risk assessments are conducted when working with multiple partners in the NT Programme	Dave Mason
1566	Updated terms of reference to be circulated to members for agreement	Rob Bolton

Rob Bolton
Risk & Assurance Adviser

Action Summary and Updates			
Ref	**Action**	**Lead**	**Update**
1557	Interim update on risk management progress to be provided to the committee every 4 weeks	Dave Mason	Action closed
1558	Confirm that the MMR Governance Board provides final sign off for mortgage product	Jonathan Hill	The roll out of 100 Mortgage Specialist roles, from the original pilot of 2012, was approved under PID submission G206 in July 2013. This PID included approval to complete work to ensure compliance with the MMR regulations and the two initiatives were governed in parallel. The GO/NO GO approval to move to an advised model was given at the Post Office/BoI Joint MMR Steering (attended by Nick Kennett and Nick Fahy and Mike Joyce from BoI) on 29th January 2014. Further internal Post Office approval was provided by the Gating Forum on 5th February 2014. Individual Advisor suitability is provided by accreditation following the BoI approved training course and is subject to Fit and Proper checks. All advisors required to hold a professional qualification in Mortgages
1559	Provide the terms of reference for the Financial Services Sub Committee once review of this forum completed	Jonathan Hill	Terms of reference circulated with supporting papers for March meeting
1560	Approved policies to be submitted to next available ExCo for final endorsement	Rob Bolton	Action completed
1561	Re-submit updated Acceptable Use policy to a future Risk & Compliance Committee for approval	Julie George	Action Closed - Acceptable Use Policy was reported to ExCo following a request for a paper to be submitted. The policy has been agreed with exceptions – mainly with regard to Board members – activity is underway to engage with each Board Member via Alwen Lyons, Lesley Sewell and Julie George which will be documented and agreed in a risk acceptance paper. Currently discussions have been undertaken with Alice Perkins and Virginia Holmes.
1562	A full BCM status report to be provided to the next meeting	Dave Mason	On agenda for March meeting
1563	Paper to be submitted to the next meeting that quantifies the Information Security resource risk, including options for Post Office and the identification of residual risk under each option	Julie George	Action Closed - Paper submitted to meeting

POL00302864

Post Office Ltd – Strictly Confidential PAPER TEN

1564	Results of assurance work on governance and terms of reference to be reported to the next meeting	Dave Mason	Update included in Assurance Activity paper provided for March meeting
1565	Report to be provided for the next meeting to explain what risk assessments are conducted when working with multiple partners in the NT Programme	Dave Mason	On agenda for March meeting
1566	Updated terms of reference to be circulated to members for agreement	Rob Bolton	Terms of reference circulated on 17th February with the minutes from the January meeting

POL00302864

RISK AND COMPLIANCE COMMITTEE

The purpose of this paper is to provide the committee with an update on an action from the previous meeting in January 2014

1563	Quantify the Information Security resource risk, including options for Post Office and the identification of residual risk under each option	Julie George / Lesley Sewell

Consolidated Version

The Information Security and Assurance Group (ISAG), to meet its increasing responsibilities for Corporate Information Security and Assurance including Cyber Security and wider business support, require additional headcount. In addition to corporate responsibilities ISAG are responsible for the on-going Information Security due diligence of suppliers and partners to ensure that they protect Post Office information that is in their care. Currently the headcount is supplemented by 5 contractors (3 of which cover the main programmes of Transformation, Separation and Transition), where possible these Contractors are also utilised within BAU activities since there no other Information Security skills outside of ISAG within Post Office. Below is a summary table of the risk that ISAG permanent staffing shortfall creates, aside from the financial implication of the contractor overhead. The shortfall detailed on the next two tables equates to 6 FTE against the published organisation headcount shortfall of 4 (as referred to in the final perspective below).

Where possible Contractors will be replaced by full time employees providing a substantial saving to Post Office.

The comparison of Contractors versus Full time employees:

5 Contractors = (Average £850 per day x 22 days per month over 1 year) = £1,122,000
5 Full time Employees = (Average £110,000 per year inclusive of package) = £550,000

Savings £572,000 per year.

Risk Metrics based on Data protection fines, and Industry metrics of £100 per Data Record, also on overall risk of loss of business through non-certification to PCI/DSS (Payment Card Industry Data Security Standards)

Description	Information Risk Register	Role Required	Risk
Information unavailability due to IT service disruption or lack of system availability	Covering 6 Risks	1.5 ISA Technical Assurance Manager	£500K - £100M
Information integrity and confidentiality exposure	Covering 9 risks	0.25 ISA Senior Risk manager and 0.5 ISA Compliance Manager	£500K - £100M
Insufficient Information Security involvement in wider internal practices, projects and programs	covering 5 risks	0.5 ISA Senior Risk manager, 1 ISA Compliance manager and 1 ISA Technical Assurance Manager	£500K-£100M
Failure to conform to information security standards and compliance	covering 3 risks	0.25 ISA Senior Risk Manager and 1 ISA Compliance Manager	£500k - £100M

POL00302864

More Detailed Version			
Consolidated Risk Category	**Areas of Risk – Cause and Concern**	**ISAG Response**	**Staffing Shortfall**
Information unavailability due to IT service disruption or lack of system availability	• Communications interference • Degradation of critical services • External misuse and abuse • Insecure external communications • Loss or unavailability of premises or IT infrastructure • Malicious software	10 Penetration Tests and Vulnerability Scans undertaken annually against a projection of 30 to cover all main third parties. Whilst we do not undertake the testing ourselves there is liaison work with our suppliers as well as scoping work to ensure risks are managed appropriately	• 1.5 FTE Technical Assurance Managers
Information integrity and confidentiality exposure	• Incorrect Application Processing • Inappropriate Information Leakage • Human Error • Internal misuse and abuse • Repudiation of user action • Social engineering • Theft or loss of media • Unauthorised logical access	10 Security Reviews of significant third-parties undertaken, but at least 20 further secondary and tertiary suppliers and smaller third parties not reviewed. Review of Post Office and third party staff on internal systems only performed for privileged accounts	• 0.25 FTE Senior Risk Manager • 0.5 FTE Compliance Manager
Insufficient Information Security involvement in wider internal practices	• Inadequate third party management • Unauthorised hardware or software • Unauthorised physical access • Inadequate change management • Inadequate security awareness training(that is performed outside of ISAG) • Inadequate security incident management	ISAG is involved as : • Design Authority in contractual wording 'inclusion of 'House Position' • Licencing reviews • Physical security initiatives • IT changes • Security incidents • Maintaining the security awareness programme however gaps in coverage are apparent	• 0.5 FTE Senior Risk Manager • 1 FTE Compliance Manager • 1 FTE Technical Assurance Manager/Security Architect
Failure to conform to Information Security standards and compliance	Non-compliance to: • ISO27001 • PCI DSS • ISAE3402 • LASSIS • Third party audit and questionnaire response	Post Office manages and undertakes the contractually obligated compliance and certification activities but it is more reactive than proactive due to the increasing size of Post Office, the diversity of the business and intrusiveness of third party approaches	• 0.25 FTE Senior Risk Manager • 1 FTE Compliance Manager

POL00302864

Gaps viewed from Risk, Compliance and Technical Assurance perspective

Description	Cause	Consequence
Management of Information Risks	There was clear direction from the Buffalo exercise, Deloitte Information Security assessment review report, Internal Audit report and the PCI DSS audit the there is a significant shortfall in the way that information risks are managed. At present the area is only resourced as an interim position to cope with these activities and 1 associated extra ISA Senior Risk Manager is defined in Target Operating Model as announced on 17th Oct. There is also the growth issue of Cyber Threats which increases risk via Post Office online/digital services	This will result in ISAG team's inability to manage the new Target Operating Model defined information risk activities as they current stand. The Deloitte report stipulated "Senior Management do not have a comprehensive view on the information security risk environment" and to "plan what actions the organisation must take to reduce risk and enable Post Office to manage and monitor the threats they face effectively and proactively". The consequence of failure to attend to risks will invoke contractual and compliance penalties and sanctions
Third Parties Information Security governance	There was clear direction from the Buffalo exercise, Deloitte IS report and more importantly for on-going certification; the PCI DSS audit the there is a shortfall in the way that major third-parties are managed for assurance of their security response. Currently, there are 12 suppliers in this category, but significant others remain outside. Additionally, we need to further explore the second tier suppliers as well as complete the security review scheduled. At present the area is under resourced to cope with these activities and 1 associated extra Compliance Manager as defined Target Operating Model as announced on 17th Oct	This will result in ISAG team's inability to manage the new Target Operating Model defined compliance activities as they current stand. Furthermore both the new versions of both ISO27001:2013 and PCI DSS v3 both stipulate more requirements around the governance of third parties. The consequence of failure to attend to compliance will invoke contractual and compliance penalties and sanctions.
Information Security Technical Assurance	There was clear direction from the Buffalo exercise, Deloitte IS report and the PCI DSS audit the there is a shortfall in the way that information security technical assurance is maintained. At present the area is under resourced to cope with these activities and 2 associated extra Technical Assurance Managers as defined Target Operating Model as announced on 17th Oct	This will result in ISAG team's inability to manage the new Target Operating Model defined technical assurance activities as they current stand. Currently the management and review of vulnerability assessments, penetration testing, project technical involvement, as well as the security incident management response is under-resourced. The consequence of failure to attend to technical assurance will invoke contractual and compliance penalties and sanctions

POL00302864

Post Office Limited Board
Financial Services Sub-Committee
Terms of Reference

Summary

The Post Office Board Sub-Committee on Financial Services is a group, established by the Post Office Limited Board, to provide guidance on, oversight of and authorisation to the development of the Post Office's financial services programmes and activities, including those of First Rate Exchange Services Limited ("FRES"), a 50% joint venture with Bank of Ireland, within the strategic framework as agreed by the Post Office Limited Board.

The Sub-Committee has the delegated authority of the Post Office Limited Board for Financial Services matters.

1. Meeting Frequency:

- At least quarterly but can meet more frequently as required to facilitate effective and timely actions and decisions

2. Chair:

- The Chair should be a non-executive director of Post Office Limited.
- Tenure should be for an initial term of 2 years
- The Chair is responsible for reporting to the Post Office Limited Board, including any escalation of issues that require full Board approval

3. Members:

- Members of the Sub-Committee should be non-executive and executive members of the Post Office Limited Board
- It is proposed that the Sub-Committee consists of three members:
  - Virginia Holmes — non-executive Director (Chair)
  - Tim Franklin — non-executive Director
  - Chris Day — executive Director (CFO of the Post Office)
- It is expected that the Director – Financial Services and the General Counsel will both attend but will not be members
- Operational and finance management representatives may be invited to attend as required. Any ad hoc attendees to be approved by the Chair prior to the meeting.
- Secretary

4. Secretariat:

- The Secretary will be provided by the Company Secretariat.

5. Quorum:

- A minimum of 2 members
- Decisions need to be made by a majority of the members although it is not anticipated that matters will be taken to a vote.

POL00302864

6. **Delegated Authorities**

Planned Spend	Unplanned Spend	Value of Indemnities or Potential /Contractual Liabilities	Risk or brand impact
Value	Value	Potential cost	Description
> £20m	> £10m	> £20m	Carries significant risk (ERM score 4) Attracts public and media interest Risk of impact on brand value New product Is likely to attract the interest of the Shareholder

7. Core Responsibilities:

- Review key activities of the Financial Services strategic programme, including those activities of FRES, as presented and agreed at Post Office Limited Board
- Oversight of the Bank of Ireland (UK) plc capital and liquidity for Eagle Contract requirements
- Provide guidance to the Financial Services management team
- Consider Risk Management matters prior to consideration and decision by Audit, Risk & Compliance Committee
- Provide authorisation to proceed with contractual agreements for new products, services and suppliers and changes to existing agreements in accordance with the existing mandate and delegated authority limits of the Post Office Limited Board
- Receive a quarterly report on Financial Services, including a copy of the Risk Register – this will be noted at the Post Office Limited Board along with minutes and actions
- Annual Review of the Sub-Committee's effectiveness

8. Inputs:

- Business performance reports
- Focused papers from Financial Services management on key activities requiring approval to proceed

9. Outputs:

- Key decisions and actions from the meeting
- Report to the Post Office Limited Board on decisions/actions taken
- Quarterly report on Financial Services performance to the Post Office Limited Board
- Risk management matters to be referred to the Audit, Risk & Compliance Committee
- Issues/decisions to be referred to the Post Office Board.

Approved by the Financial Services Sub-Committee 27 January 2014