POST OFFICE AUDIT, RISK AND COMPLIANCE COMMITTEE

Information Security and Data Asset Review

1. Purpose

The purpose of this paper is to:

1.1 Provide the Committee with an update on developments, progress and actions with the Information Security agenda for Post Office. It is for noting purposes only.

2. Background

2.1 Since our update to the Committee in November, we have been progressing three strands of Information Security activity, with the majority of actions completed and a new plan generated:

- Priority action plan: this covers a range of priority activities that are focused on improving our current Information Security controls and management;
- Data asset review: this is focused on producing an initial assessment of Post Office's top 13 supplier/partner contracts. These were categorised by potential for significant reputational risk should we encounter a loss of our business information;
- Independent review of Post Office's Information Security: this was to provide an independent view of Post Office's information security approach and a road map of improvement activity.

2.2 This paper provides an update and actions on each of the above areas.

3. Priority action plan

3.1 The following priority actions have been completed since November:

- Post Office staffs have been reminded about the importance of protecting information by Data Protection awareness communication.
- The Privacy / Data Protection Governance structure has been presented and approved by the Risk & Compliance Committee.
- The Major Incident Management process has been reviewed, and improvements have been implemented, to ensure an early alert mechanism for escalating potential security breaches to the attention of senior managers.
- The Clear Desk and Screen Policy has reviewed and communicated via the senior leadership team; assurance activity is in place to ensure compliance.
- Information Security training for new staff and annual refresher training for all staff has been finalised and will be rolled out in March.

- The Post Office Information Security Policy has been reviewed and will be published through the Risk & Compliance Committee.

- A Data Protection Handbook providing guidance and process has been drafted and will be rolled out to branches via Horizon and Branch Focus in Q1.

4. Data Asset Review

4.1 We have continued the review of our top ranked data assets held by third parties on behalf of Post Office. A model has been developed to enable a quantitative assessment to be carried out and this work has identified the top-13 risk areas which are viewed as having the highest risk of brand damage and customer privacy protection. The core contracts have been reviewed by our external law firm, and the Information Security risk has been assessed internally; other supplementary contracts in the chain are in the process of being reviewed. From the review the following points are noteworthy:

[redacted]

4.3 RAPP who manage and host the Marketing database for Post Office hold a significant amount of personal and account data. We understand their security architecture which is ISO 27001 certified and the measures they take to protect Post Office data. We are currently reviewing the amount of customer and account data being maintained, to ensure it is appropriate and further review of the contract is underway.

4.4 Our top 13 contracts have been reviewed with regard to Data Protection and understanding our position from an ICO (Information Commissioners Office) perspective, whether we are likely to be considered as controllers of the data or a processor. In the majority of cases the contracts are clear, however there are some exceptions which do require further investigation. Further work is required to clarify whether operational practices accurately reflect the contractual clauses (as the ICO takes both into consideration), and an action plan to address any gaps will be prepared.

4.5 Most third parties have capped their liability in relation to data issues and in some instances there are specific exclusions or limitations in addition to a cap. Where the core contract forms part of a larger chain (e.g. POCA) there are two instances where Bond Pearce have identified that our entitlement to recover from the third party is capped at a sum lower than our potential liability to the end customer (POCA / HP and DVLA / Cogent). In terms of indemnification for data issues, we benefit from indemnities in some but not all of the contracts reviewed; some of these indemnities are uncapped (e.g. Cogent) - which is in our favour.

4.6 The first stage of the review is scheduled to complete at the end of February, and the minimum Information Security standards will be implemented for all top 13 contracts and an action plan for our suppliers will be agreed during March.

5. Information Security – Independent Review Findings

5.1 Deloitte have been engaged to complete a review of Information Security within Post Office, covering a maturity and gap analysis against information security standards

(ISO27001/2)[1]. The high level findings have been agreed. The details are currently being reviewed by all key stakeholders within Post Office and a detailed plan encompassing the activities currently underway and future road map has been prepared.

5.2 The key findings from the review are as follows:

- The Information Security team is significantly under resourced and there is insufficient internal resource to provide appropriate security input into new and on-going projects; or assurance activities with our key suppliers/partners. The recruitment of a Head of Information Security is underway, and to support our recent separation from RMG additional security specialists are being recruited.

- We do not have a comprehensive view of the Information Security risk environment and the existing Information Security policy set is incomplete. There is a mixture of legacy RMG policies and gaps in the policy set.

- On-going training and awareness across Post Office is not currently proactively managed and there is no rolling security awareness campaign of Information Security policies.

- There is a need for greater oversight and a formal assurance programme of our third parties Information Security controls. Whilst there are some assurance activities such as PCI (Payments Card Industry) compliance testing and governance structures for our suppliers/partners, it is not consistent. A standard framework is required for the management of Information Security controls operated by third parties.

- There were gaps identified in the existing Information Security governance forums, it is recommended that an Executive level forum will be created which will report through to the Risk & Compliance Committee quarterly.

5.3 Deloitte have recommended an action plan, outlined in Appendix A. This has been reviewed by the project team to assess the level of resources and support required. In addition, we have aligned the plan with the activities currently underway. The plan includes:

- Mobilising the Information Security team to ensure that the POL Information Security objectives are met, with clear accountabilities and structure.

- Improve the Information Security risk control and review framework, which will be aligned to the wider risk activities across Post Office.

- Implement a high level Information Assurance Strategy and supporting policies, and wider monitoring and compliance to the Data Protection Act.

- Develop a framework of security management (including audit rights and clarity of contracts) for our suppliers, and implement controls to address the risks inherent in legacy contracts.

[1] **ISO27001/2:** An International Standards covering the specification of 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.

- Conduct a training and awareness programme, including the development of campaigns to address identified risks.

- Aligned to our Separation activities review the current security infrastructure protecting the key components such as our network and asset management.

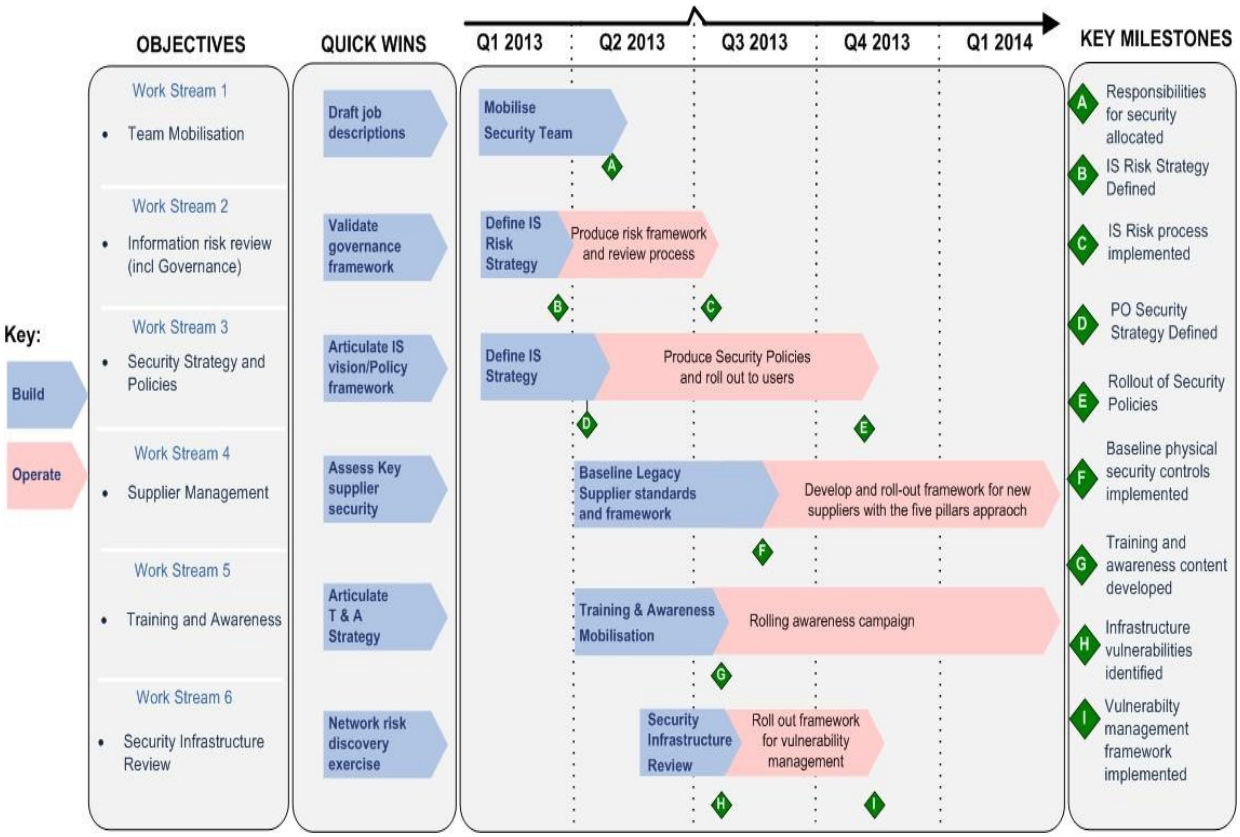
6. Summary

The Committee is asked to note the positive progress which has been made and it is proposed that quarterly updates are provided to ARC and the Risk and Compliance Committee on progress.

Lesley Sewell
February 2013

Appendix A – Deloitte proposed Information Security transformation roadmap

The Deloitte POL Information Security Review proposes the following Information Security roadmap:



1. Team Mobilisation is development of job descriptions and recruitment of the required Information Security staff.
2. Information Risk review includes definition of the underlying data relationship and baselined security controls.
3. Information Security Strategy and Policies includes a refreshed policy set, and Information Security minimum standards.
4. Information Security Supplier Management implements the minimum standards with the top 13 suppliers and ensures a consistent governance structure.
5. Training and Awareness is for both Head Office staff and the staff in the branches.
6. Security Infrastructure Review - to review the current security infrastructure for our network and implement where appropriate regular vulnerability assessment process. This will be aligned with our separation from RMG.

.