FUJ00232652

FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)

Document Title:	Fujitsu Services Post Office Account Information Security Management System (ISMS) Manual
Document Reference:	SVM/SEC/MAN/0003
Document Type:	MANUAL
Release:	Not Applicable
Abstract:	An approach and framework to implementing, maintaining, monitoring and improving information security on the POA
Document Status:	APPROVED
Author & Dept:	CISO
External Distribution:	Mark Pearce, Head of Information Security [Post Office Limited]

Approval Authorities:

Name	Role	Signature	Date
Brad Warren	CISO	*n/a*	

©Copyright Fujitsu Services Ltd 2012

FUJ00232652

0 Document Control

TABLE OF CONTENTS

FUJ00232652

FUJ00232652

0.1 Document Control

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1		Initial Draft	
0.2	19/02/08	Updated with information from service description	
0.2	19/02/08	Issued for Review	
1.0	30/04/08	Issued for Approval after updating with review comments	
1.1	30/04/09	Review Amendments	
1.2.	14/12/09	Updates to reflect HNG-X	
1.3	16/12/09	Risk Approach updates	
1.4		Review and update	
1.5	8/04/10	Update following review following organisational changes. And initial meeting with BSI	
1.6	01/06/10	Changes arising from Document Review	
1.7	16/06/2010	Changes from Quality Review	
1.8	24/06/2010	Additional Risk Management Changes	
2.0	21/07/2010	Issued for Approval following review comments	
2.1	30/08/2011	Update after annual review	
2.2	26/05/2012	Review of ISMS Manual	
2.3	02/11/2012	Interim review of updated ISMS – draft	
2.4	04/12/2012	Following document review	
2.5	14/12/2012	Revised as per Bill Membery comments	
3.0	21-Dec-2012	Approval version	

0.2 Review Details

Review Comments by :	
Review Comments to :	Brad Warren
Mandatory Review	
Delivery Executive	James Davidson
Chief Information Security Officer (CISO)	Brad Warren
Quality and Compliance Manager	Bill Membery
Optional Review	
Client Executive	Gavin Bell
Commercial Director	Tim Healy
Security Operations Manager	Donna Munro
Issued for Information – Please restrict this distribution list to a minimum	

FUJ00232652

Head of Information Security, POL	Mark Pearce

(*) = Reviewers that returned comments

0.3 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)	2.0	16-03-07	POA HNG-X Generic Master Document Template	Dimensions
SVM/SEC/PRO/0033	2.0	14/06/10	Risk Management Procedures	Dimensions
SVM/SEC/MAN/0001	8.1	05/09/11	POA Statement of Applicability	Dimensions
SVM/SEC/POL/0003	6.0	08/09/11	POA Information Security Policy	Dimensions
CMP3	7.0	24/05/2012	Fujitsu Property and Physical Security Master Policy	CafeVik
CMP6	7.5	03/07/2012	Fujitsu Legal Compliance Master Policy	CafeVik
CMP20	2.2	26/06/2012	Fujitsu Security Master Policy	CafeVik
CMP21	3.4	03/10/2011	Fujitsu Intellectual Property Master Policy	CafeVik
CMP27	2.11	17/08/11	Fujitsu Risk Management Master Policy	CafeVik
CMP31	7.0	01/03/2012	Fujitsu Business Continuity Master Policy	CafeVik
Fujitsu (UK&I) Security Policy Manual	1.0	11/05/12	Fujitsu Services Security Manual	CafeVik

Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.

0.4 Abbreviations

Abbreviation	Definition
IG	Information Governance
ISMR	Information Security Management Review
ISMS	Information Security Management System
NCN	Non-Conformity Notice
POA	Post Office Account
ToR	Terms of Reference
Fujitsu	Fujitsu Services POA,
CISO	Chief Information Security Officer
RTP	Risk Treatment Plan

©Copyright Fujitsu Services Ltd 2012

FUJ00232652

ISP	Information Security Policy
SOA	Statement of Applicability
ARQ	Audit Request Query
SLA	Service Level Agreement
OLA	Operational Level Agreement

0.5 Glossary

Term	Definition

0.6 Changes Expected

Changes
Within 6-12 months re-issued following Information Security Management review [internal] audit.

0.7 Copyright

© Copyright Fujitsu Services Limited 2012. All rights reserved. No part of this document may be reproduced, stored or transmitted in any form without the prior written permission of Fujitsu Services.

FUJ00232652

1 Introduction

Information is an asset which, like other important business assets, has value to an organisation and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to safeguard customers and staff, ensure business continuity, minimise business damage and maximise operational efficiency.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected and is subject to the provisions of this policy document.

Information security is characterised here as the preservation of:

- *Confidentiality*: ensuring that information is accessible only to those authorised to have access;
- *Integrity*: safeguarding the accuracy and completeness of information and processing methods;
- *Availability*: ensuring that authorised users have access to information and associated assets when required.

Information security is achieved by implementing a suitable set of countermeasures, including policies, practices, procedures, organisational structures and technical measures. Therefore by using an Information Security Management System (ISMS), this provides a systematic approach to managing sensitive company information so that it remains secure. It also encompasses people, processes and IT systems

2 Information Security Policy

1. The purpose of this policy is to define how Information Security is managed, within the framework of this ISMS
2. The purpose of Information Security Management is to provide an appropriate level of protection for information assets from relevant threats, whether internal or external, deliberate or accidental. The implementation of this policy is important to maintain our integrity as a supplier of services to stakeholders.
3. It is the policy of the POA to ensure that:
    a. The requirements of ISO/IEC 27001:2005 are effectively addressed
    b. Information will be protected against unauthorised access.
    c. Confidentiality of information will be maintained.
    d. Information will not be disclosed to unauthorised persons through deliberate or careless action.
    e. Integrity of information is assured through protection from unauthorised modification.
    f. Information is available to authorised users when needed.
    g. Regulatory and legislative requirements will be met.
    h. Information security training will be provided to all staff.

©Copyright Fujitsu Services Ltd 2012

FUJ00232652

4. This policy is set within the context of the ISMS and interfaces the following Fujitsu Services Master Policies:

   Property and Physical Security [CMP3]

   Legal Compliance [CMP6]

   Security Master Policy [CMP20]

   Property and Physical Security [CMP3]

   Legal Compliance [CMP6]

   Intellectual Property [CMP21]

   Risk Policy [CMMP27]

   Business Continuity [CMP31]

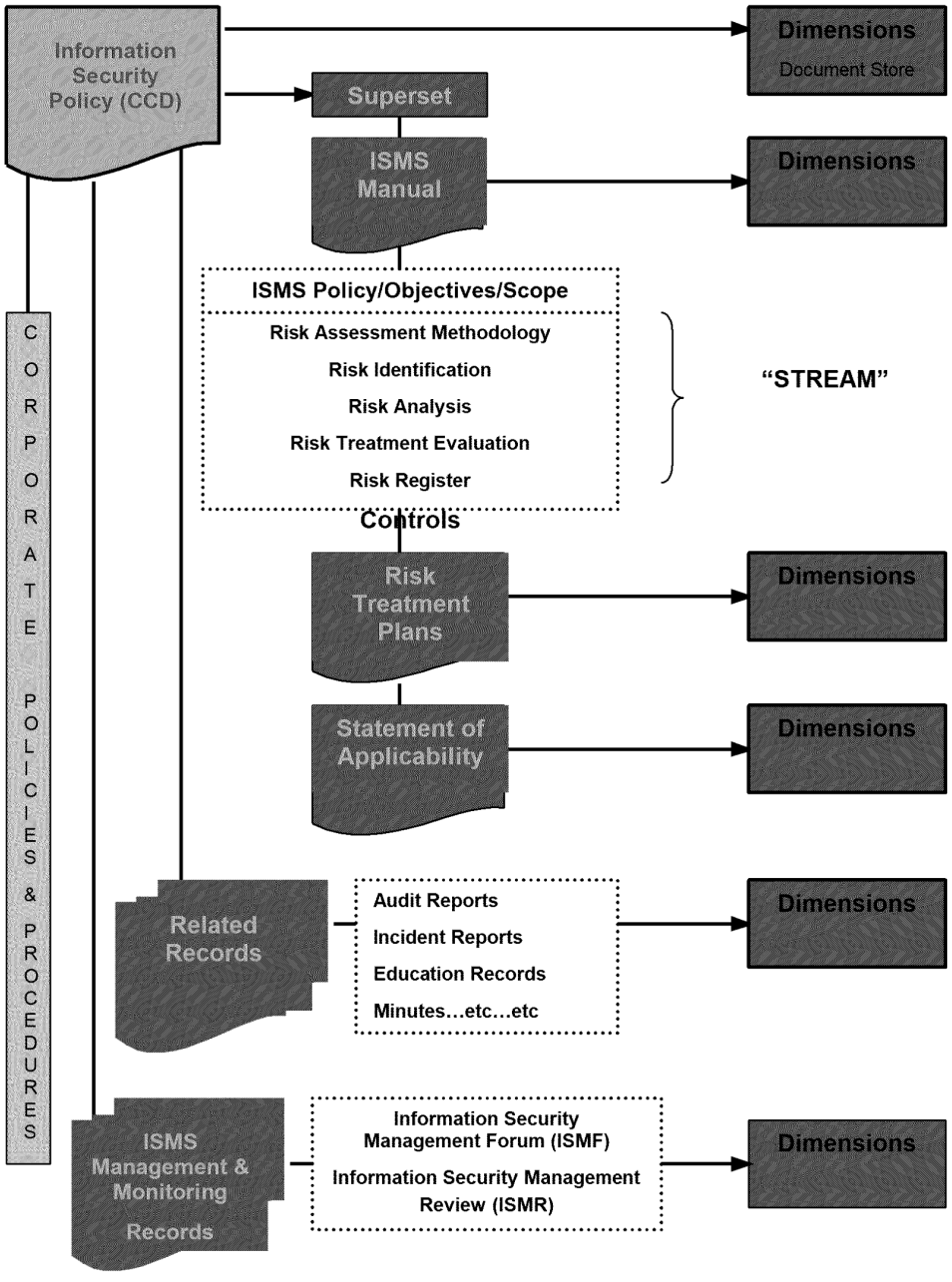
   Fujitsu (UK & I) Security Policy Manual

Any member of Staff failing to adhere to the Security Policy and associated procedures will render themselves liable to disciplinary action in accordance with Fujitsu Conduct Guidelines

©Copyright Fujitsu Services Ltd 2012

FUJ00232652

3 ISMS Document Structure



FUJ00232652

4 Objectives of the ISMS

The objectives of the ISMS are to:

1. Provide an information security framework within which the programme is developed, delivered and implemented to all relevant areas of the business;
2. Provide an organisational and responsibility framework for security activities and allocate security roles and responsibilities;
3. Identify risks associated with the provision of the POL Service, through formal risk assessment techniques, and prioritise and implement appropriate controls and security measures;
4. Ensure appropriate security and business continuity procedures and controls are in place to support Services provided;
5. Provide a basis for review, governance, assessment and improvement of the ISMS;
6. Ensure that information security controls are appropriate to the sensitivity of the information processed and stored;
7. Ensure contractual, legal & regulatory compliance across the scope of Service provision;
8. Identify the security awareness and education requirements for employees and subcontractors.

4.1 Objective Measures & Effectiveness

No	Objective	Measures	Measurement
1	A management system, based on an information security risk approach, exists to establish, implement, operate, monitor, review, maintain and improve information security.	Demonstrated through the ongoing maintenance of the ISMS per registration to ISO27001:2005, under the auspices of the Plan, Do, Check Act cycle, and through the review of audit coverage & results; corrective actions; security incidents; risk assessment and reviews	Existing and management approved information security management system, based on a viable risk assessment methodology (STREAM), with attendant records
2	An organisational framework has been established, and approved by POA, to identify and allocate security roles and responsibilities.	Demonstrated through appointment of appropriately competent personnel identified; who are in post (with relevant and approved TORs) The organisational framework is under constant senior management review, with records maintained by PMO and security roles and responsibilities are subject to regular review & update by the ISMF and ISMR	• Information Security Policy, approved by Account Director (Version 5) • ISMR (Quarterly) and ISMF (Monthly) Minutes (8 senior managers invited) • PMO Records – 300+ Personnel on Account • Personal Terms of Reference
3	A formal risk management process has been established whereby relevant risks will have been identified, measured and appropriate controls and countermeasures implemented.	A fully documented risk management process including a control framework, risk registers and associated risk treatment/security improvement plans which are reviewed on a	• STREAM risk assessment tool and associated records. • STREAM Dashboard • Monthly risk assessment meeting

©Copyright Fujitsu Services Ltd 2012

FUJ00232652

		regular basis. Demonstrated through the risks being reviewed on a regular (at least monthly) basis as part of the Business Review Process and shown to be effective (+ risk mitigations closed off); linkage to managed change processes, incident management and audit; STREAM dashboard	
4	Controls relevant to the identified asset risks are in place	Demonstrated through, for example, the completeness of BC plans, together with associated review schedules/tests. Assigned asset owners, asset registers, test schedules and scripts which are subject to regular review and test (as applicable)	• ISMS Document set • Approved Risk Management Process (SVM/SEC/STD/0006); • STREAM Records in respect to asset classes, asset owners, risks etc
5	An Information Security Management Forum (ISMF) has been approved and established to oversee the review, governance, assessment and improvement of the ISMS	Demonstrated through schedule (at least monthly) of meetings;	• In POA top level forum is the Information Security Management Review – records/minutes of quarterly and weekly meetings; evidencing top management commitment and attendance. • ISMR Terms of Reference
6	A Statement of Applicability (SoA) has been prepared that describes the control objectives and controls that are relevant and applicable to the organisation	The SoA, which can be affected by changing business circumstances, is reviewed at a minimum on an annual basis, and updated where applicable.	SoA Version 1 (Dimensions); managed through STREAM updates
7	The handling of information will be in strict compliance with all relevant contractual, legislative and regulatory requirements.	Training, Awareness and Communication programs are established to ensure all stakeholders are apprised of the requirements. The requirements themselves are visited on a regular basis to ensure currency. Demonstrated throught audit results and incident reviews and records of those who have undergone Fujitsu services and POA training	• Fujitsu Corporate manages new mandatory Security Awareness Training Programme • All joiners/movers/leavers now managed through Operational Security. Re-introduction of Security at Induction, communications and briefings. [Ref Security Improvement Plan November 2012]
8	All personnel who are assigned responsibilities defined in the ISMS have documented records of training, skills, experience and qualifications.	Demonstrated through maintenance and regular review of staff records to ensure compliance with ISMS. Ongoing CBT training is monitored and reported, with relevant records maintained. Appraisal processes are designed to determine training/skills needs	• Staff Records (inc training and qualifications); skills database, appraisal system for training and developmental needs.

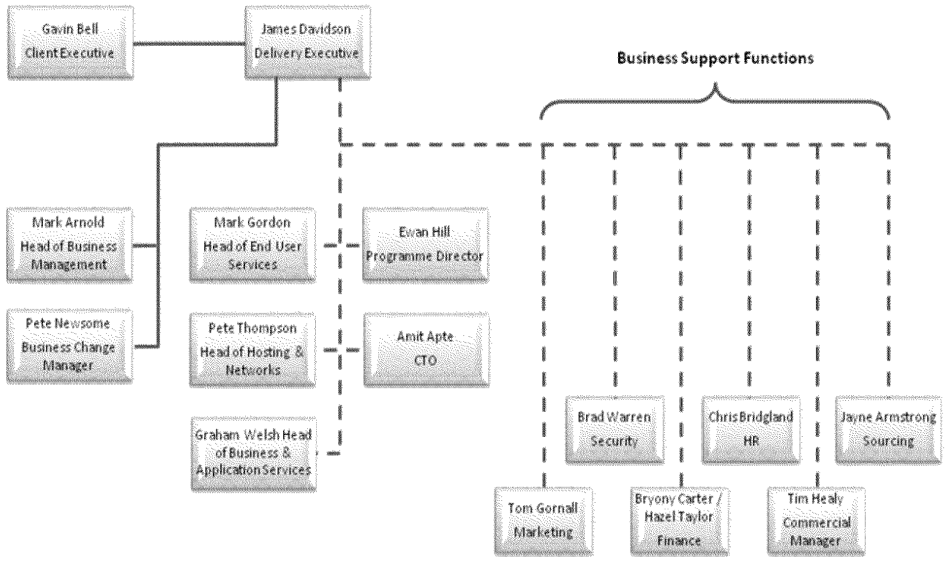
©Copyright Fujitsu Services Ltd 2012

FUJ00232652

5 Organisation and Scope

5.1 POA Organisation

The diagram below represents the POA Account organisation structure. Detailed organisation charts are maintained by PMO.



5.2 Management Commitment

POA management is committed to Information Security. This is demonstrated by:

- appointment of CISO to POA as a member of the Extended Leadership Team reporting directly to the Delivery Executive
- review and approval of this ISMS Manual which describes the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS;
- review and approval of the POA Information Security Policy
- the provision of resources and approval of roles and responsibilities for information security, including ensuring adequate skills and competencies;
- ongoing communications and awareness activity; and
- Inclusion of Security on both the Quarterly Quality Review and ELT and Programme Risk board.

FUJ00232652

5.3 Statement of Scope

The operation and maintenance of the Post Office Account (POA) on-shore and off-shore services provided by Fujitsu to Post Office Ltd (POL) and incorporating the Horizon on Line Service and POL Financial Systems (SAP and Management Information). In accordance with the Statement of Applicability Version 8

(*Associated asset types are recorded in Appendix A (15).*

5.3.1 Excluded from Scope:

Activities, processing, and management carried out by PO Ltd users, or non-Fujitsu assets (not managed by POA) located at PO Ltd sites, e.g. Post Office Branches, Mobile Offices or PO Ltd. 3rd party sites.

Communications to Post Office clients; where such connections are the responsibility of PO Ltd. or its clients as defined by the contract.

POA services provided to RMG (Royal Mail Group rather than PO Ltd),

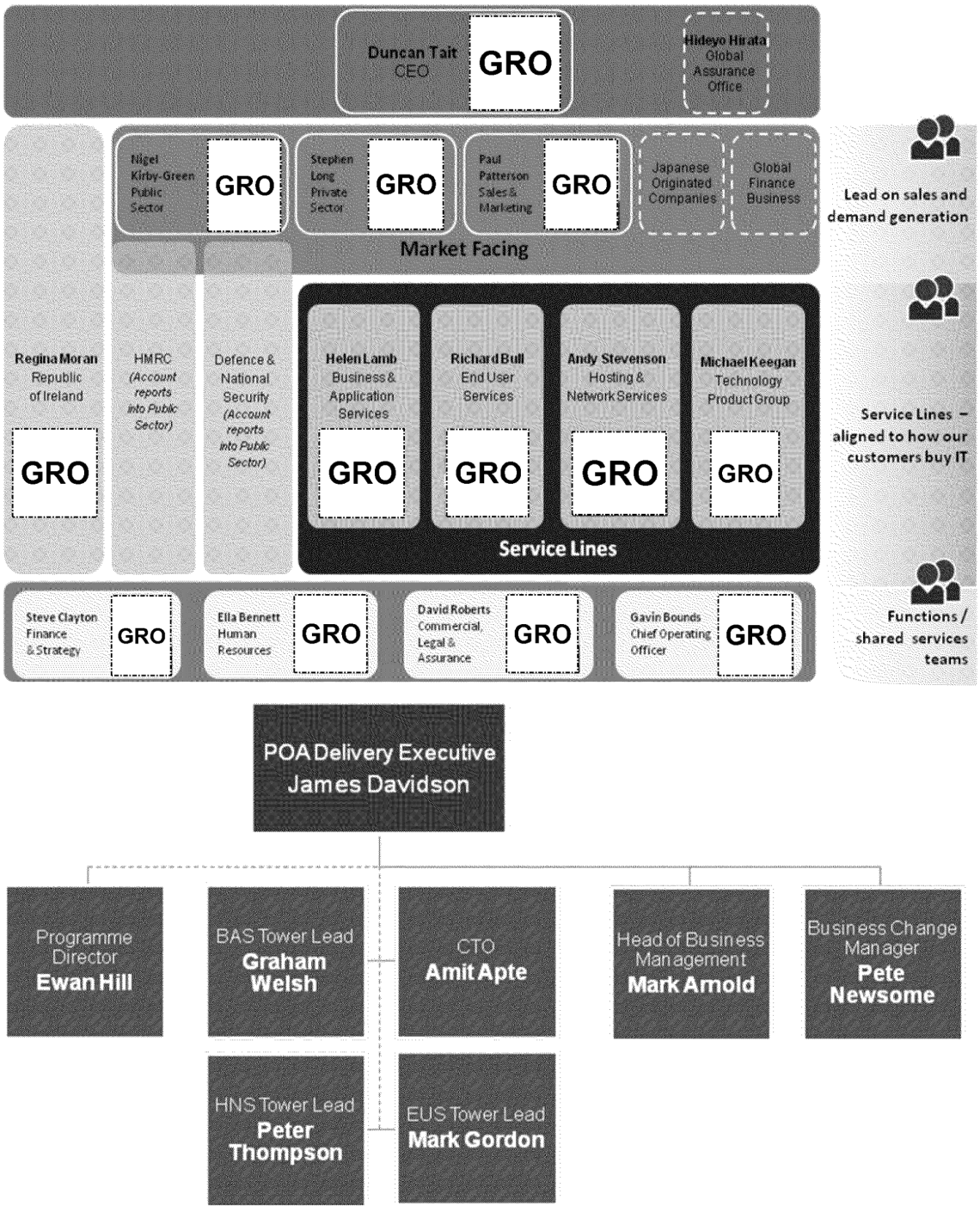
5.4 Boundaries and Interfaces

Fujitsu UK&I have recently reorganised to deliver its services more in line with our customer's needs. The top level Fujitsu organisation is shown below with the relevant Service Lines e.g. Business Application Services, Hosting & Network Services, End User Services and Technology Product Group. Fujitsu Post Office Account [POA] interfaces with these service lines to provide the services required to support delivery to Post Office. The Delivery Executive for POA reports into the head of Business Application Support service line – BAS – but interfaces with area of H&NS, TPG for delivery as well as the Functions that support Fujitsu UK&I delivery across the board as indicated in the POA org chart headed by the Delivery Executive.

©Copyright Fujitsu Services Ltd 2012

FUJ00232652

UK & Ireland Region



Key Dependencies

FUJ00232652

H&NS provides Data Centres which are used to host, manages and operates business critical IT systems for Fujitsu corporate and customers' businesses.

Fujitsu Group Properties manage the secure building environment and the supporting sub components, such as the mechanical and electrical systems, resilience of the environment and the management of building security including media destruction services.

Fujitsu Group Security provides the systems for a) security vetting, and b) the processing, analysis and reporting of security incidents, including those pertaining to information security.

Human Resources provide the systems for ensuring starters and leavers are processed correctly thus ensuring all relevant aspects of security are fulfilled, e.g. passes, laptop etc, issued and recovered.

Supply and Lifecycle Services manage and control the relationships with our key services suppliers.

Engineering Services provide advice and guidance as well as incident management and resolution on servers, desktop and peripherals at a customer's site where such support cannot be provided remotely

5.5 External Parties

POA will create and maintain a register of external parties with connections to Services provided to PO Ltd.

In accordance with Section 6.4 of the POA Information Security Policy security requirements must be agreed, documented and defined in agreements with any external parties, who require access to POA information or processing facilities. This agreement may be in the form of an external contract or internal operational level agreement.

Audits will be carried out periodically by POA to confirm that compliance to POA security requirements. POA may accept ISAE 3402 or BSI ISO27001 registration as evidence of compliance all or part of the POA security requirements where the scope of the external audit includes all aspects of services provided to POA.

In addition Section 10.8 of the POA Information Security Policy provides the guidance and controls on the security requirements for exchange of information between external parties.

5.6 Other Fujitsu Business Units.

For the purpose of the POA ISMS other Fujitsu business units will be treated as external parties as per section 4.5 above.

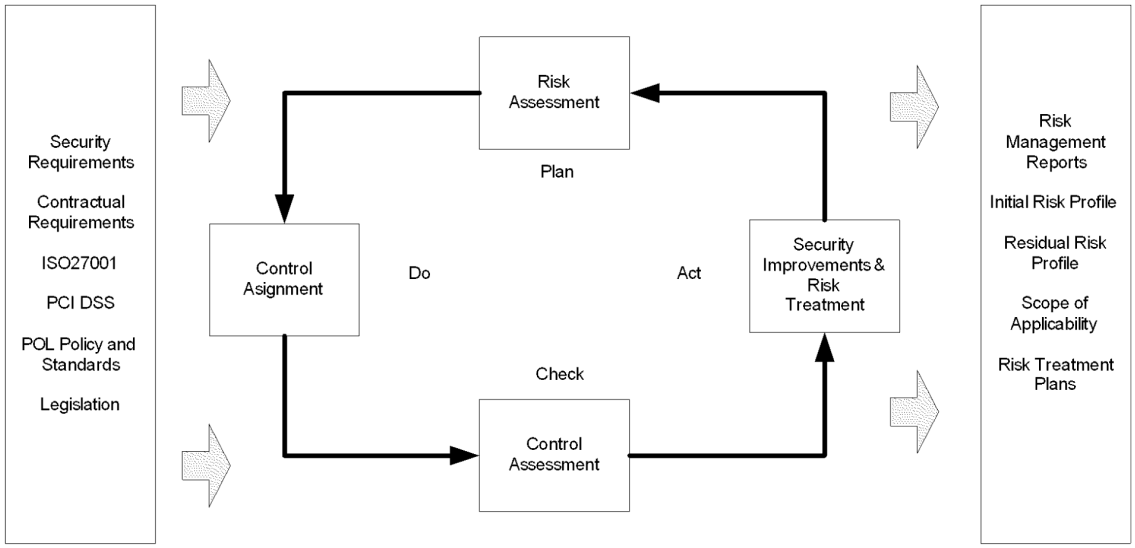
6 Information Security Risk Assessment

Risks shall be identified, assessed and reviewed as described below and shall be generally managed in accordance with the Fujitsu Services Business Management System (BMS) Risk Management Master Policy.

6.1 Risk Management Approach (Methodology & Tools)

Risk management is a continuous and iterative process which underpins the ISO/IEC 27001

FUJ00232652



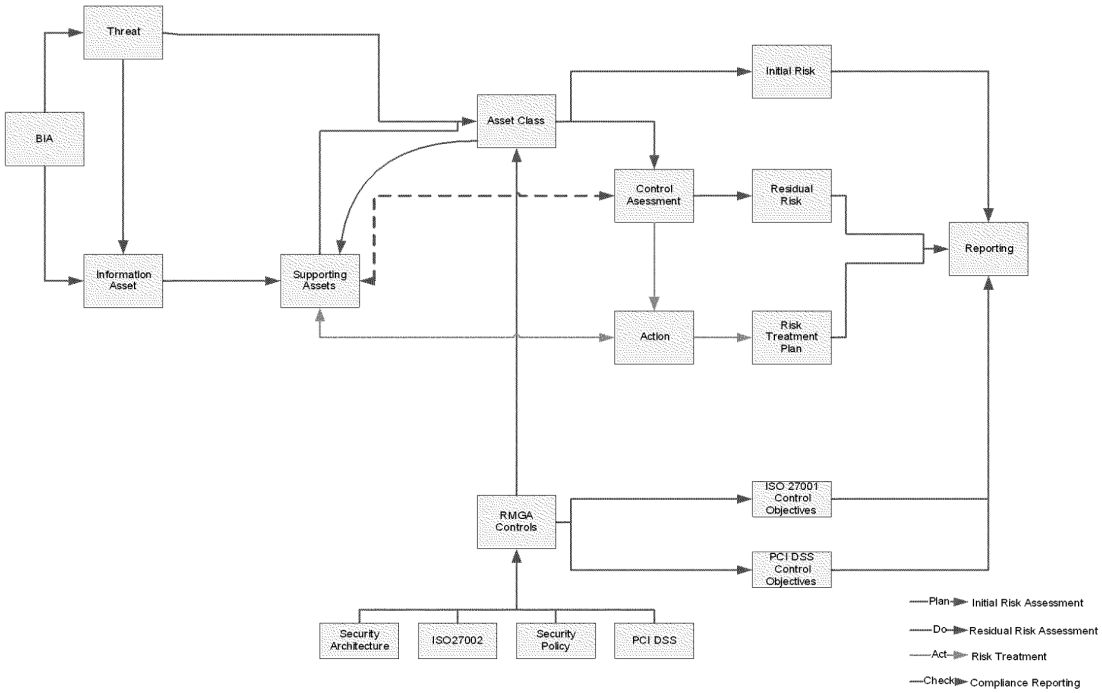
POA has selected the Acuity Stream risk management tool to manage:

- Risk Assessment;
- Control Assignment;
- Control Assessment;
- Security Improvements and Risk Treatment and
- Risk Management Reporting and Dashboard.

The workflow for Acuity Stream is demonstrated in the diagram below

©Copyright Fujitsu Services Ltd 2012

FUJ00232652



Information security risks are based upon the identified Information assets and supporting assets of the functions / services within scope. A list of the identified asset classes can be found in Schedule B.

6.2 Risk Treatment Plan

For all risks where the residual risk is identified within Acuity Stream as amber / red an action will be recorded, for further containment to reduce the residual risk to an acceptable level. These actions when consolidated into a report will be considered as the risk treatment plan (RTP).

The risk treatment report will identify for each risk requiring treatment:

- its pre-action data is recorded from the risk register;
- the risk option is decided
- risk treatment action[s] are determined and recorded;
- post action scoring is undertaken
- next review / milestone dates are documented

The RTP is subject to regular review by the POA CISO/ISMF, in conjunction with the risk owners.

6.3 Risk Treatment Options

FUJ00232652

There are several options available to senior management when considering what to do about identified risks. The chosen option (or mix of management techniques) will depend on the nature and level of the risk.

The key options are:

- **Risk Acceptance:**

  For low-frequency, low-impact risks, where the cost of control is greater than the potential risk, CU management will choose to accept such risks.

- **Risk Avoidance:**

  Where an activity generates a risk, and the CU has the option to cease the particular activity or to conduct the process in a different way, then they may choose to do so in order to avoid the risk concerned.

- **Risk Reduction/Mitigation:**

  Where the level of risk is unacceptable, management will employ controls in order to manage that risk down to acceptable levels, either by mitigating the impact, or reducing the vulnerability/likelihood. Lower impact risks will be kept under review to ensure that the trend is not increasing, or the cumulative impact is not unacceptable.

- **Risk Transfer:**

  In circumstance of potential catastrophic loss, with low probability (such as complete loss of data centre), management will opt to transfer the risk to other parties, facilities or services.

6.4 Statement of Applicability

The ISMS Statement of Applicability illustrates the:

1) control objectives and controls selected together with the reasons for their selection;

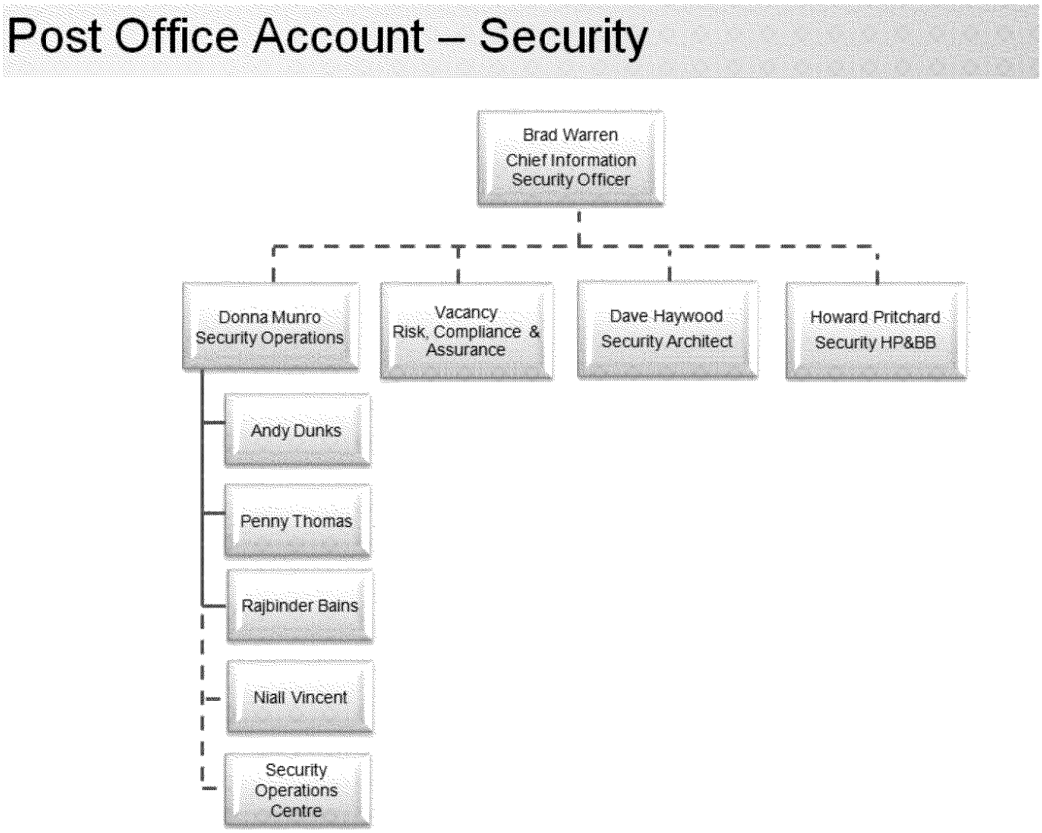
2) control objectives and controls currently implemented; and

3) exclusion of any control objectives and controls and the justification for their exclusion.

FUJ00232652

7 Organising Information Security

The information security organisation within POA is, under the leadership of the CISO.



The CISO is accountable to the Delivery Executive for management of all information security matters within the Account and scope of this registration; The CISO is a member of the ELT and senior management level Risk and Quality review boards where he shall report on security, risk and compliance issues. The CISO is the senior account representative on the Post Office ISMF and maintains contact with the Fujitsu Security Management Forum (SMF) and Security Delivery practice and CISO through line management responsibilities in H&NS.

Information security liaison between Post Office Ltd and POA is conducted through the Information Security Management Forum (ISMF), whose core membership comprises the POA CISO, Security Operations Manager and Post Office Ltd Head of Information Security and other representatives.

At Both the POA Quality and Risk boards and ISMF information security reports, risks, metrics and incidents are considered. The Quarterly Quality and Security Review are considered the acceptance body for POA account security policies. Minutes are taken of actions and decision for both these forums and are stored on POA SharePoint.

The CISO is a member of both forums and as such acts as liaison between both of the information security oversight bodies.

FUJ00232652

7.1.1 Information Security Management Review

Management review of Information Security is undertaken by the CISO and through reporting and review of RISK and associated Policies and Documentation through the monthly ELT meetings and the Quarterly Quality and Security Board. Senior management attendance is mandated and must be achieved in order for the board's activities to be authorised.

Terms of Reference for the Quarterly Quality and Security Board are detailed in RMGA/PGM/MGT/STD/2066

The POA Senior Management Team is responsible for:

- Approval for strategies and master policies supporting the Objectives.
- Identifying and reviewing metrics measuring the effectiveness of Security activities across the POA
- Ownership of Security Policy, ISMS and sign off of any other relevant CCDs e.g. for compliance etc

7.1.2 Information Security Service Review

Regular reviews of the POA Information Security Service are conducted through the ISMF, which is attended both by the POA CISO and the PO Ltd. Security Manager. Document and Record Management

All documents required by the ISMS are controlled through the Fujitsu Control of Documents Policy

Records are established and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS.

7.2 Key ISMS Documents and Records

The following key documents support the ISMS:

Document Description	Location	Retention
ISMS Manual (this document)	Dimensions	Life of the ISMS
Statement of Applicability	Dimensions	Life of the ISMS
POA Information Security Management Forum TOR's	Dimensions	Life of the ISMS
Risk Registers	STREAM/Sharepoint	Life of the ISMS

FUJ00232652

Risk Treatment Plans	Dimensions/Sharepoint	Life of the ISMS
Integrated Assessment Schedule [IAS]	Sharepoint	Current year +1
Audit Reports	Sharepoint	7 years
Reports of Security Incidents	TfS	7 years
ISMF Minutes	SharePoint	Life of the ISMS
Information Security Monthly Report	Sharepoint: POA Secured Share	Life of the ISMS

8 Key Personnel

All staff have a responsibility to protect POA assets and some play a specific role in the running and management of its ISMS.

Full details of key Fujitsu Services POA Security responsibilities are contained within the Information Security Policy. In summary the key roles and associated responsibilities are as follows:

8.1.1 Fujitsu Services POA Delivery Executive

The information security-related responsibilities of the Fujitsu Services POA Director include:

- Overall control and assignment of information security responsibilities throughout the Fujitsu POA;
- Sponsor of adequate resources for information security;
- Assignment management for the Chief Information Security Officer; (CISO);
- Appointing an experienced security professional responsible for managing and coordinating security across the complete POA domain in the CISO role.

8.1.2 Chief Information Security Officer (CISO)

The CISO is accountable for design, implementation and delivery from within the POA Security function. This includes strategy, planning, resourcing and management of the security programme to support the ISMS and the other major security obligations in the POA. Responsibilities include:

- owner of the Fujitsu Services POA Information Security Policy;
- point of engagement and escalation for all areas of POA and Fujitsu's operations and management with regards to the POA security function

FUJ00232652

- overall design of risk management and assurance approach, including deciding the criteria for risk treatment and reporting/escalation where necessary;
- ensuring the security organisation and roles are properly structured and resourced;
- direction of security resources within the Security Operations, Risk Management and Governance activity;
- authority for approving POA Security Policies, Procedures and Risk Management documentation;
- managing and directing the security functions relationships with the Post Office;
- to ensure that compliance with all contractual and other obligations are maintained in conjunction with the Quality and Compliance function.

Also by co-ordinating Security Operations [through the Security Operations Manager] to:

- ensuring that security incidents are recorded and investigated;
- monitor compliance with the POA Information Security Policy;
- ensuring all POA Staff are screened in line with contractual requirements, FS Group Policy and this policy;
- ensure that security relevant events are recorded;
- ensure that system audit trails are analysed on a regular basis;
- analysis and evaluation of information security risks as presented through Change Management process; deliver security data, metrics and operational issues to / from the ISMF;
- manage delivery of Security Services to the Post Office and internally as described and/or amended by the contract and other agreements;
- audit and manage compliance with POA security policies and procedures;
- deliver security induction and awareness activities to the POA.

8.1.3 Quality & Compliance Manager

The information security-related responsibilities of the Fujitsu Services Quality & Compliance Manager include:

- Facilitate and support the introduction of new quality standards and/or regulatory requirements providing SME knowledge
- Support the Change Process through reviewing and impacting Change Proposals from a Quality and Compliance Perspective.
- Represent POA Quality and Compliance at the Joint Audit Board Meeting and ensure Fujitsu actions recorded, distributed to owners and cleared in a timely manner.
- Report to the ISMF on Quality & Compliance activities for POA. And provide advice and guidance relating to Quality and Compliance issues

FUJ00232652

- Facilitate the POA Quarterly Quality & Security Management Meetings. Ensure Stakeholders are aware, informed of progress and internal issues are resolved quickly
- Manage the network of POA Quality Leads/SME's to improve quality and embed standards and continuous improvement
- Ensure remediation plans are on track and report progress to POA Leadership Team
- Ensure all business proposals are impacted for Quality and Compliance perspective
- Owns and maintains the Integrated Audit Schedule

8.1.4 Staff Responsibilities

All POA Staff have an Information Security related objective to ensure awareness of their security responsibilities and security procedures. Security Induction Training ensures all staff know where to find security procedures, are familiar with their contents, and understand their own responsibilities for compliance.

The information about which staff should be aware includes:

- Physical security controls and visitor procedures
- Clear desk policy, careful communications and storage
- Protecting Fujitsu documents and media and protecting POA information
- Reporting security incidents
- Responsibilities for the protection of personal data
- Acceptable use of Fujitsu equipment, Internet and email
- Working at home and out of the office

8.1.5 Other Responsibilities

The following table identifies other key roles, responsibilities and, where appropriate, authority levels and training requirements:

ROLE	RESPONSIBILITIES	AUTHORITY	COMPETENCIES
Asset Owners	Management & control of the asset for which they have primary ownership	Executive & line management	General ISMS Awareness + BMS
Line Management	Commitment to ISMS Reporting and investigation of security incidents, contribution to BC plans, testing and lessons learnt	Executive & line management	General ISMS Awareness + BMS.

9 Compliance and Reporting

FUJ00232652

9.1 ISO/IEC 27001 Compliance Audits

In support of the ISO/IEC 27001 compliance requirements, and to provide ongoing assurance of compliance, regular compliance audits (Health Checks) will be conducted. As directed by the CISO, the scope and terms of reference for each of these audits will be determined in advance and agreed with the manager of the area(s) to be audited.

For each ISO/IEC 27001 control within the scope of the ISMS the following is reviewed:

Clear, accepted responsibility for the aspect of Information Security which is subject to that control;

Confirmation from the organisation that the relevant control is in place, documented and effective;

Documentary evidence (records/logs etc. in either electronic or hardcopy format), which can be inspected to confirm the controls are in place and functioning as intended. Inspection is on a sampling basis.

All findings are logged on the Fujitsu Services Assessment Database and updated as action is taken.

All audits will be carried out by suitably trained auditors with auditing qualifications e.g. /ISO/IEC 27001 Lead Auditor/ Auditor.

Audits are carried out as part of the POA Integrated Audit Schedule, managed by the Quality and Compliance function. Additional audits are carried out on a regular basis by the FS Manage Information Security Process Champion and Fujitsu Services Business Assurance. As part of ISO/IEC 27001 registration, independent external audits will be conducted as determined by the audit body.

9.2 Reporting

Monthly security reports are produced for the ISMF which include data and details in relations to security services and Operational Security issues, incidents, events and data. In addition the CISO reports on a monthly basis to the ELT and Quarterly Quality and Security Board on issues of Business and Security Risk and any issues with security organisation and effectiveness.

A subset of data will also be represented in the POA Dashboard.

9.3 Supporting Post Office Ltd Compliance

The POA CISO is responsible for supporting Post Office Ltd in its compliance to information security regulatory and contractual information security requirements, through:

- Ensuring agreed information security controls are managed and effective
- Completing security questionnaires from POL and any of its clients e.g. LINK
- Participating, following a formal written request from POL, in routine audits such as those conducted by POL's Internal Audit team or as part of an overall audit of POL's PCI compliance.

©Copyright Fujitsu Services Ltd 2012

FUJ00232652

9.4 Legal Compliance

The Fujitsu Services Corporate Legal Department monitors legislation which is applicable to the Fujitsu UK & I business. They will provide information, advice and guidance to the UK & I Divisions to ensure corporate compliance is maintained with statutory requirements.

Within Core Division, the Information Assurance Group publish and maintain the Fujitsu UK&I [corporate] Security Policy Manual and all the related sub-policies specific to the use of corporate assets and corporate network activity.

CMP06 provides a specific policy statement on the review of processes against current legislation and standards and CMP05 details applicable Policies and Standards relevant to IT processes.

10 Communication and Awareness

The POA Induction process for new joiners includes security induction and awareness material that is appropriate both as a reminder of Fujitsu Security Policy and responsibilities and those specific areas of information security especially relevant or specific to the account.

The induction material will be reviewed and updated by the Security Operations team within the security function. In addition the CISO, Delivery Executive or Security Operations Manager will issue security notices and reminders on a needs basis.

11 Security Operations

11.1 User Administration

The Security Operations Team will be responsible for:

- The administration, issuing and audit of Two Factor authentication used by system administrators and support staff accessing the Live Service;
- Ensuring that Fujitsu users of POL Services are validated (BS + Experian checks) before being given access to the live Service.

The Security Operations Manager is responsible for ensuring that these tasks are carried out in accordance with the Security Policy and for authorising physical access rights requiring strong authentication for secure access.

11.2 Administration of Changes

Operational Change Management is the responsibility of the Change Management Team within Service Management.

The Security Operations Team is responsible for reviewing change requests and assessing the impact of changes for compliance with Security Policy and Controls and for any impact on the Confidentiality, Integrity and Availability of Services. They are supported in the technical aspects of these assessments by the Technical Security Architect.

11.3 Acceptance into Service

FUJ00232652

Responsibility for accepting new Services rests with the Service Introduction Manager who is responsible for ensuring that new services that have identified security requirements have been addressed and any assurance undertaken to the satisfaction of the CISO as delegated to the appropriate authority for the applicable governance mechanism. The process shall ensure that the security elements of Acceptance into Service have been met and this will be approved via the Security Operations Team.

11.4 Analyse Security Logs

The Security Operations Team is responsible for providing a number of security event management and firewall event analysis activities:

- Managing and operating the audit mechanisms and security event management system (including firewall events) to monitor, detect, track, record and report events that might threaten the security of the Service Infrastructure (security weaknesses). This includes the review of security event filter to optimise performance;
- Regularly analysing audit trails to identify trends and to assist the investigation of security incidents/breaches;
- Establishing and monitoring adequate firewall policies / rule bases based on the output of risk assessments as appropriate;
- Where potential attacks, or areas of vulnerability, are identified ensuring prompt investigation and providing advice for any remedial action (as part of security incident management) to minimise the impact of any security breach.

Any successful attacks will be subject to the POA Customer Service Incident Management Process.

11.5 Anti-Virus and Malicious Software Management

The Operational Security team provides a number of anti-virus and malicious software management activities. For HNG-X, Sophos/ESET AV offers a level of protection against known malware.

Managing the distribution of updated anti-virus software across the live estate to protect the Services from malicious software, including regular 'Signature' updates to identify and cleanse new and emerging virus strains;

Configuring, and maintaining, alerting mechanisms and event filters to provide automatic notification and prompt virus incident response (in accordance with security incident response procedures);

Regular checking of emerging viruses and other malicious software to determine any required defensive measures;

11.6 Security Incident Management

The Operational Security Team participate in the POA Customer Service Incident Management Process (SVM/SDM/PRO/0018) and POA Customer Service Problem Management Process (SVM/SDM/PRO/0025) with regard to Security related Incidents and Problems.

The Operational Security Manager is the prime point of contact for information security related events, incidents and breaches and is responsible for communicating relevant security incident

©Copyright Fujitsu Services Ltd 2012

FUJ00232652

details to POL, as well as attending the monthly ISMF meeting to review information security incidents.

11.7 Cryptographic Key Management

The Operational Security Team provide a key management service to control the certification and distribution of cryptographic key material used to protect the confidentiality and integrity of Post Office business data. This consists of three primary activities:

Managing cryptographic key suppliers;

Manual cryptographic key management – creating, distributing, auditing and replenishment of manual cryptographic keys;

Managing an automated Key Management System (KMS) - creating, distributing and replenishment of cryptographic material as well as assisting support teams with error resolution and problem management related to the KMS.

The KMS is a critical business system and as such is subject to service optimisation and the provision of business continuity arrangements.

An actual, or suspected, compromise of any keys (including PIN Pads) will be treated as a security incident and managed accordingly. In particular, key change mechanisms will be invoked. If a key is identified compromised a corrective action plan will be carried out in accordance to the agreed correct action response for that key.

An actual, or suspected, compromise of any keys (including PIN Pads) will be treated as a security incident and managed accordingly. In particular, key change mechanisms will be invoked.

11.8 Information Retrieval and Prosecution Support

The Security Operations Team is responsible for the management of the day-to-day extraction of transaction and event data from the audit system, the analysis of supporting information and the provision of associated investigation / prosecution support. This requires close co-operation with Audit and Investigation staff in Post Office Ltd, the provision of witness statements and reports, and possible attendance at Court to give evidence.

Data extracted can be in response to either Transaction Record Queries, or Audit Record Queries, including APOP Voucher Queries (Reference document SVM/SDM/SD/0017). Activities under this section constitute a Service to Post Office Ltd in support of their investigation and prosecution activities. It is not intended to represent an audit activity of user activity for security risk purposes.

11.9 Physical Access Control

The Security Operations Team is responsible for the administration, issue and control of the Fujitsu Services (Post Office Account) Ltd Horizon Security Passes. All staff that require access to a Post Office branch to provide support and maintenance will need to be issued with a Horizon Security Pass. The Horizon Security Pass allows employees of the Post Office Account (POA) to be identified as those who have been successfully vetted by Post Office Limited (POL).

In addition access to Fujitsu sites, offices and rooms used in the execution of business in the POA are requested and managed through Site Facilities and Fujitsu Group Security processes.

©Copyright Fujitsu Services Ltd 2012

FUJ00232652

12 Business Continuity Management

Comprehensive Business Continuity Management is in place within POA and associated documentation can be found in Dimensions.

13 Electronic Mail

Information is transmitted in accordance with Fujitsu Services (and where appropriate POL) policies and procedures for the use and management of email systems.

©Copyright Fujitsu Services Ltd 2012

FUJ00232652

14 Appendix A – Asset Types

The Asset, together with owners, are documented within the Acuity Stream Database. All assets are grouped by Asset Class. The table below contains the Asset Classes currently configured in Stream. Details of full assets and their ownership can be output from Acuity Stream.

AssetClassName	Description
3rd Party	3rd Party organisation
3rd Party Service	Services provided by 3rd Parties
Internal 3rd Party	Other Fujitsu Business Units
Application	Business & Support Applications
Customer	Customer
Counter	Post Office Counters
FS Corporate Systems	
External Connection	External Connections to 3rd Parties and Clients
Ops Function / Team	Operational Functions / Teams
Non Ops Function/Team	Staff with non operational roles
ISMS	POA ISMS Scope
Location / Room	Locations - includes Rooms and facilities
Media	Mobile Storage Devices of any kind
Network	Communications Infrastructure
Organisation	Organisational Unit
Platform	Information System (Hardware and Operating System)
PCI DSS	PCI DSS Scope
Peripherals	Other Peripherals Devices attached to platforms or end user devices
PinPad	Counter Pin Pad for card payment
Site	Buildings

©Copyright Fujitsu Services Ltd 2012