FUJ00232619

Document Title:	Fujitsu Services RMGA 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 RMG Account
Document Status:	APPROVED
Author & Dept:	CS Security
External Distribution:	Sue Lowther

Approval Authorities:

Name	Role	Signature	Date
Tom Lillywhite	CISO	*T Lillywhite*	21 July 2010

Note: See Royal Mail Group Account HNG-X Reviewers/Approvers Role Matrix (PGM/DCM/ION/0001) for guidance.

0 Document Control

0.1 Table of Contents

0 DOCUMENT CONTROL 2
0.1 Table of Contents 2
0.2 Document Control 4
0.3 Review Details 4
0.4 Associated Documents (Internal & External) 5
0.5 Abbreviations 6
0.6 Glossary 7
0.7 Changes Expected 7
0.8 Copyright 7

1 INTRODUCTION 8

2 INFORMATION SECURITY POLICY 8

3 ISMS DOCUMENT STRUCTURE 10

4 OBJECTIVES OF THE ISMS 11
4.1 Objective Measures & Effectiveness 11

5 ORGANISATION AND SCOPE 13
5.1 RMGA Organisation 13
5.2 Management Commitment 13
5.3 Statement of Scope 14
5.3.1 Excluded from Scope: 14
5.4 Boundaries and Interfaces 14
5.5 External Parties 15
5.6 Other Fujitsu Business Units. 15

6 INFORMATION SECURITY RISK ASSESSMENT 15
6.1 Risk Management Approach (Methodology & Tools) 15
6.2 Risk Treatment Plan 17
6.3 Risk Treatment Options 17
6.4 Statement of Applicability 18

7 ORGANISING INFORMATION SECURITY 18
7.1.1 Information Security Management Review 20
7.1.2 Information Security Service Review 20

8 DOCUMENT AND RECORD MANAGEMENT 20
8.1 Key ISMS Documents and Records 20

9 KEY PERSONNEL....................21
9.1.1 Fujitsu Services RMG Account Director 21
9.1.2 Fujitsu Services RMGA Operations Director 21
9.1.3 Fujitsu Services RMGA Programme Director 22
9.1.4 Quality Manager 22
9.1.5 Chief Information Security Officer (CISO) 22
9.1.6 Staff Responsibilities 23
9.1.7 Other Responsibilities 23

10 COMPLIANCE AND REPORTING....................24
10.1 ISO27001 Compliance Audits 24
10.2 Reporting 24
10.3 Supporting Post Office Ltd Compliance 24
10.4 Legal Compliance 25

11 COMMUNICATION AND AWARENESS....................25

12 OPERATIONAL SECURITY....................25
12.1 User Administration 25
12.2 Administration of Changes 25
12.3 Acceptance into Service 26
12.4 Analyse Security Logs 26
12.5 Anti-Virus and Malicious Software Management 26
12.6 Security Incident Management 26
12.7 Cryptographic Key Management 27
12.8 Information Retrieval and Prosecution Support 27
12.9 Physical Access Control 27

13 BUSINESS CONTINUITY MANAGEMENT....................28

14 ELECTRONIC MAIL....................28

15 APPENDIX A – SITE, FUNCTIONS, STAFF....................29

16 APPENDIX B – ASSETS....................32

0.2 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	

0.3 Review Details

Review Comments by :	
Review Comments to :	CISO & RMGADocumentManagemen GRO
Mandatory Review	
Account Director	Gavin Bounds
Operations Director	James Davidson
Chief Information Security Officer (CISO)	Tom Lillywhite
Service Director	Gaeten van Achte
Programme Director	Alan D'Alvarez
Optional Review	
Commercial Director	Guy Wilkerson
Security Services Manager	Donna Munro
Quality Manager	David Parker
Issued for Information – Please restrict this distribution list to a minimum	
Head of Information Security, POL	Sue Lowther

(*) = Reviewers that returned comments

0.4 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)	2.0	16-Apr-07	RMGA HNG-X Generic Master Document Template	Dimensions
SVM/SEC/PRO/0033			Risk Management Procedures	Dimensions
SVM/SEC/MAN/0001	8.0		RMGA Statement of Applicability	Dimensions
SVM/SEC/POL/0003	5.0		RMGA Information Security Policy	Dimensions

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

0.5 Abbreviations

Abbreviation	Definition
IG	Information Governance
ISMR	Information Security Management Review
ISMS	Information Security Management System
NCN	Non-Conformity Notice
RMGA	Royal Mail Group Account
ToR	Terms of Reference
Fujitsu	Fujitsu Services RMG Account,
CISO	Chief Information Security Officer
RTP	Risk Treatment Plan
ISP	Information Security Policy
SOA	Statement of Applicability
ARQ	Audit Request Query
SLA	Service Level Agreement
OLA	Operational Level Agreement

0.6 Glossary

Term	Definition

0.7 Changes Expected

Changes

0.8 Copyright

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 RMG Account to ensure that:
   a. The requirements of ISO27001:2005 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.
4. This policy is set within the context of the ISMS and interfaces the following Fujitsu Services Master Policies:

Property and Physical Security [CPM3]

Legal Compliance [CPM6]

Security [CPM20]

Intellectual Property [CPM21]

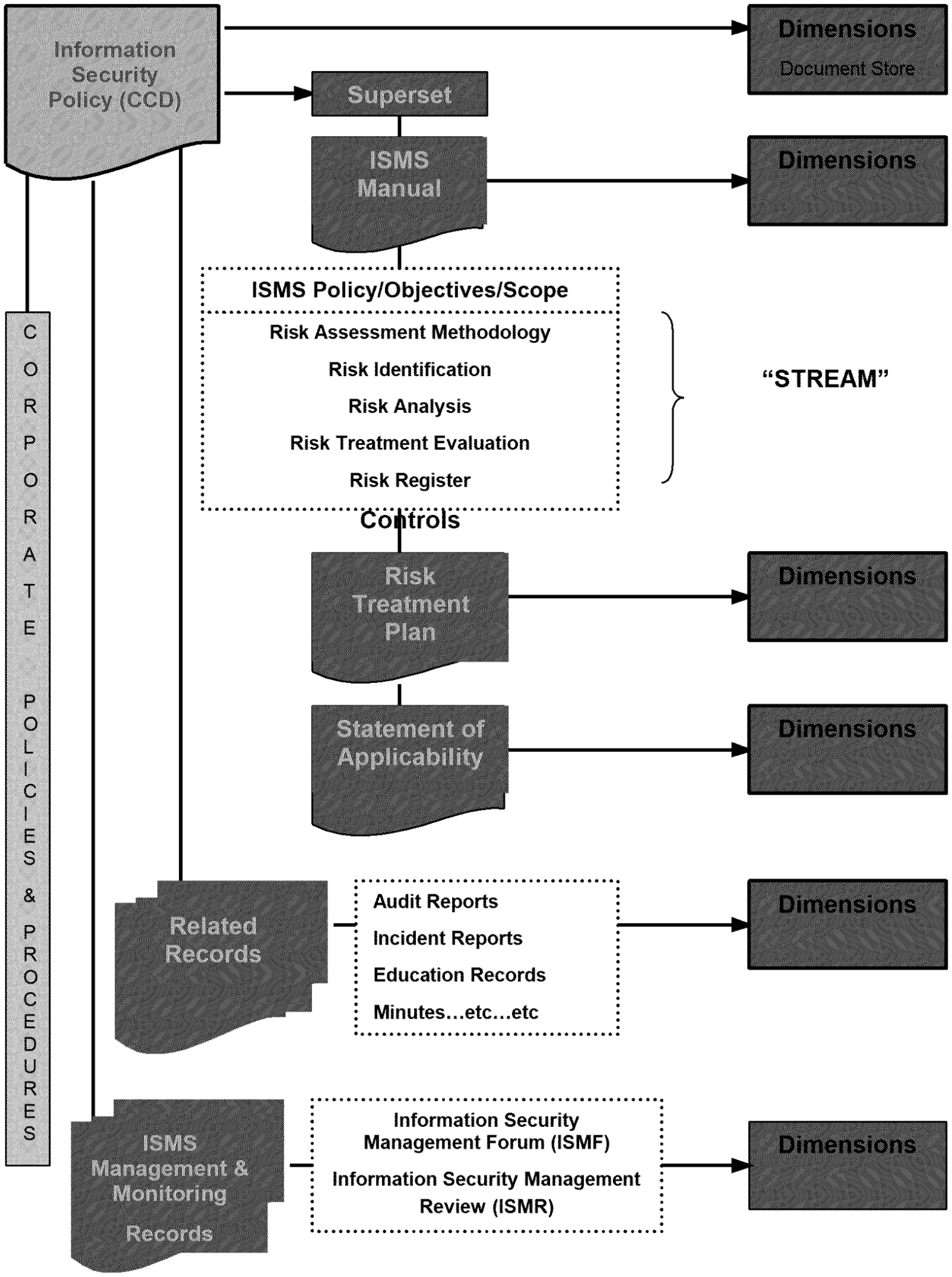
Risk Policy [CPM27]

Business Continuity [CPM31]

Fujitsu Services (UK & I) Security 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

3 ISMS Document Structure


Information Security Policy (CCD)
Dimensions
Document Store
Superset
ISMS Manual
Dimensions
ISMS Policy/Objectives/Scope
Risk Assessment Methodology
Risk Identification
Risk Analysis
Risk Treatment Evaluation
Risk Register
"STREAM"
Controls
Risk Treatment Plan
Dimensions
Statement of Applicability
Dimensions
CORPORATE POLICIES & PROCEDURES
Related Records
Audit Reports
Incident Reports
Education Records
Minutes…etc…etc
Dimensions
ISMS Management & Monitoring Records
Information Security Management Forum (ISMF)
Information Security Management Review (ISMR)
Dimensions

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

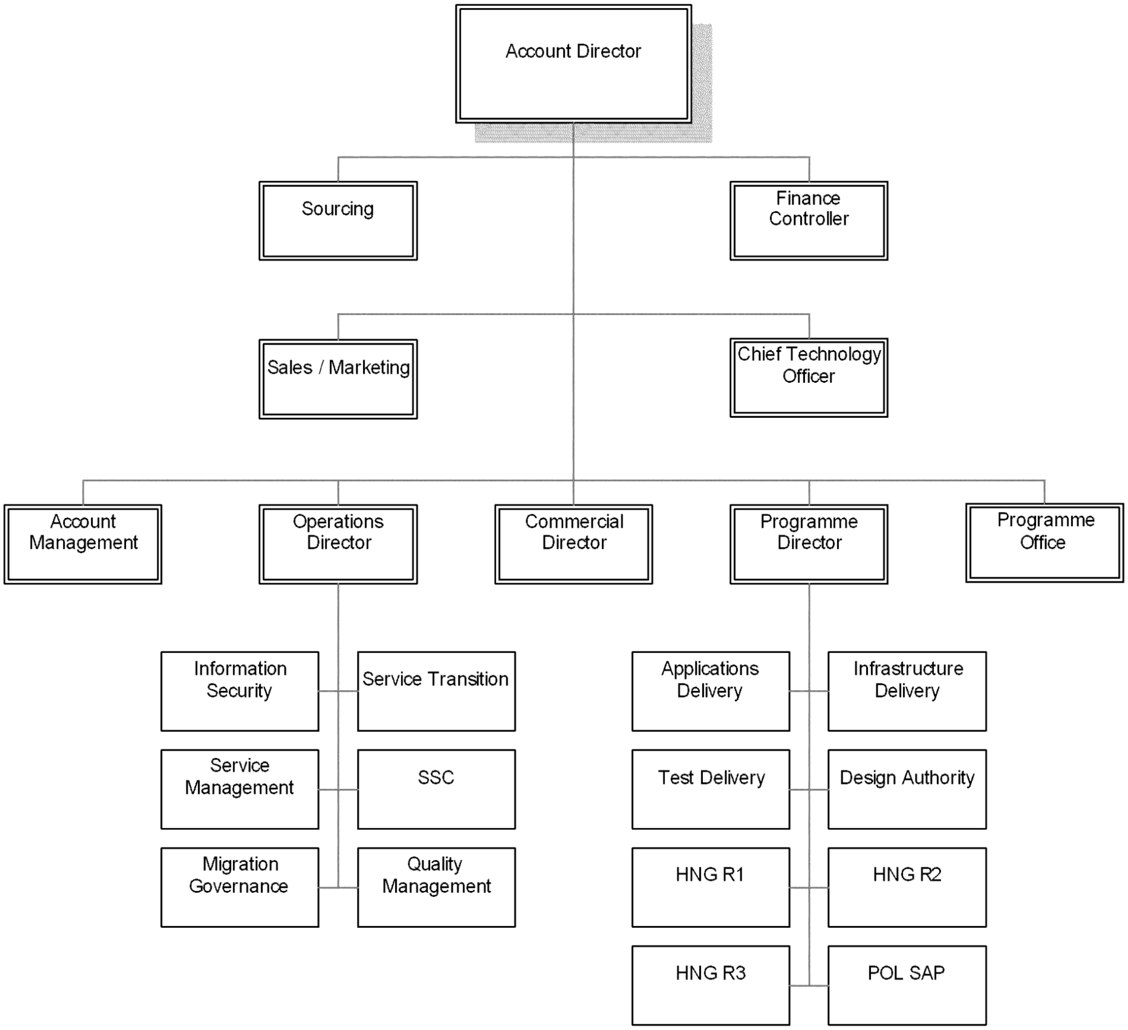
No	Objective	Measures	Measurement
1	A management system, based on an information security risk approach, exists to establish, implement, operate, monitor, review, maintain and improve information security.	Demonstrated through the ongoing maintenance of the ISMS per registration to ISO27001:2005, under 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 RMGA, 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 Weekly) and ISMF (Monthly) Minutes (8 senior managers invited) • PMO Records – 315 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 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 risk assessment tool and associated records. • STREAM Dashboard • Last risk assessment update May 2010. • Monthly risk assessment meeting

		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 RMG Account 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 RMGA training	• RMG Account Security Communications Plan (last review May 2010) • May/June 2010 Corporate Security CBT Course – RMG Account recorded 94% attendance • RMG Account Induction Course (all joiners) approved and established by ISMR – commences July 2010. • Audit results of personnel security and awareness highlighted incomplete documentation only; no security reports (2009/2010) indicate personnel security failings leading to data loss/compromise
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); appraissal system

5 Organisation and Scope

5.1 RMGA Organisation

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



5.2 Management Commitment

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

- approval of this ISMS Manual which describes the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS;
- approval of the RMGA Information Security Policy
- the provision of resources and approval of roles and responsibilities for information security, including ensuring adequate skills and competencies;
- an ongoing communications and awareness strategy; and
- Participation in the Information Security Management Review (ISMR) for the oversight of information security, including risk management escalation and approval, internal audits and the sponsorship of management reviews.

5.3 Statement of Scope

The operation and maintenance of the Royal Mail Group Account (RMGA) 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 sites, functions, staff and assets are recorded in Appendix A (15) and Appendix B (16) respectively)

5.3.1 Excluded from Scope:

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

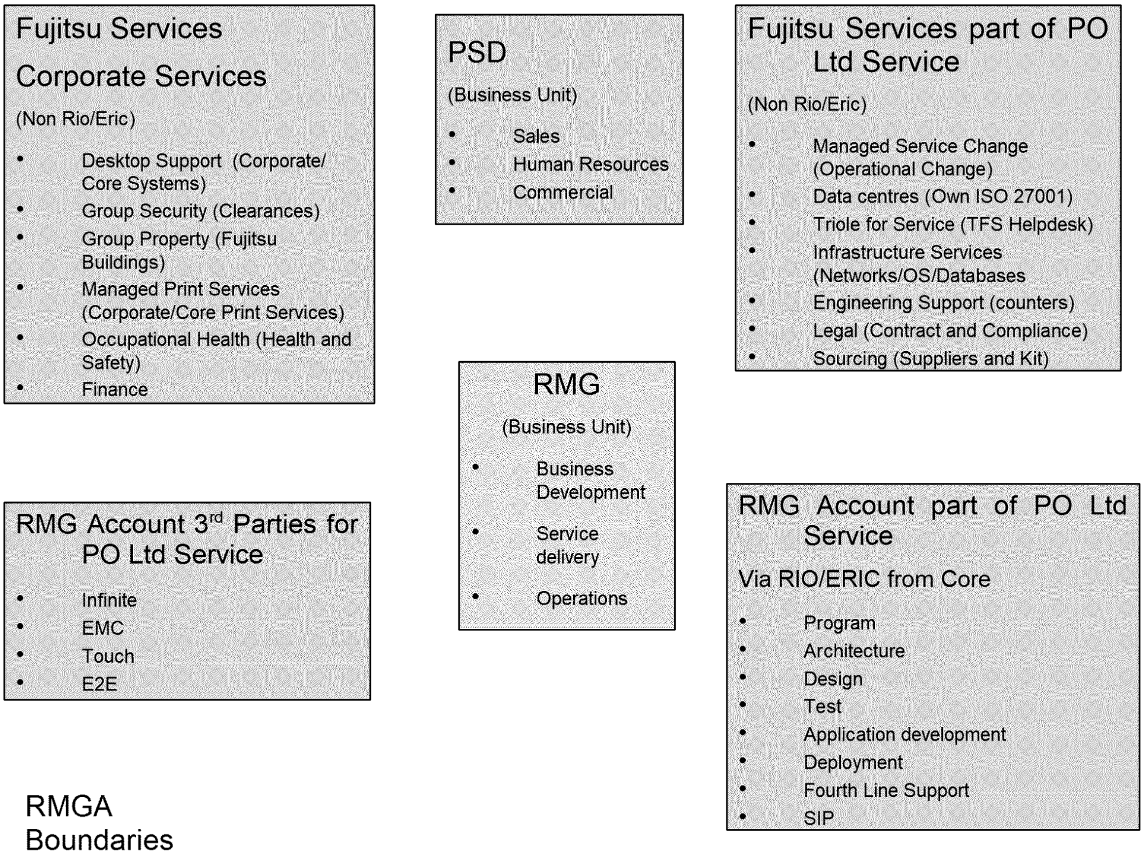
PO Ltd. has a contract with Prism (a joint venture of CSC and BT). PO Ltd. also have a contract with Fujitsu Services who's suppliers include BT. There is no overlap between the services BT sell through Prism and those that they sell to Fujitsu Services.

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

RMGA Services provided to RMG (Group rather than PO Ltd),

The Horizon service (predecessor to Horizon on Line) and the Wigan and Bootle Datacentres since this service and locations are due to be decommissioned within the 1st half of 2010

5.4 Boundaries and Interfaces



Fujitsu Services

Corporate Services

(Non Rio/Eric)

- Desktop Support (Corporate/ Core Systems)
- Group Security (Clearances)
- Group Property (Fujitsu Buildings)
- Managed Print Services (Corporate/Core Print Services)
- Occupational Health (Health and Safety)
- Finance

PSD

(Business Unit)

- Sales
- Human Resources
- Commercial

Fujitsu Services part of PO Ltd Service

(Non Rio/Eric)

- Managed Service Change (Operational Change)
- Data centres (Own ISO 27001)
- Triole for Service (TFS Helpdesk)
- Infrastructure Services (Networks/OS/Databases
- Engineering Support (counters)
- Legal (Contract and Compliance)
- Sourcing (Suppliers and Kit)

RMG

(Business Unit)

- Business Development
- Service delivery
- Operations

RMG Account 3rd Parties for PO Ltd Service

- Infinite
- EMC
- Touch
- E2E

RMG Account part of PO Ltd Service

Via RIO/ERIC from Core

- Program
- Architecture
- Design
- Test
- Application development
- Deployment
- Fourth Line Support
- SIP

RMGA Boundaries

Data Centre and Networks hosts, 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.

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

RMGA 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 RMGA Information Security Policy security requirements must be agreed, documented and defined in agreements with any external parties, who require access to RMGA 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 RMGA to confirm that compliance to RMGA security requirements. RMGA may accept SAS70 type II or BSI ISO27001 registration as evidence of compliance all or part of the RMGA security requirements where the scope of the external audit includes all aspects of services provided to RMGA.

In addition Section 10.8 of the RMGA 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.

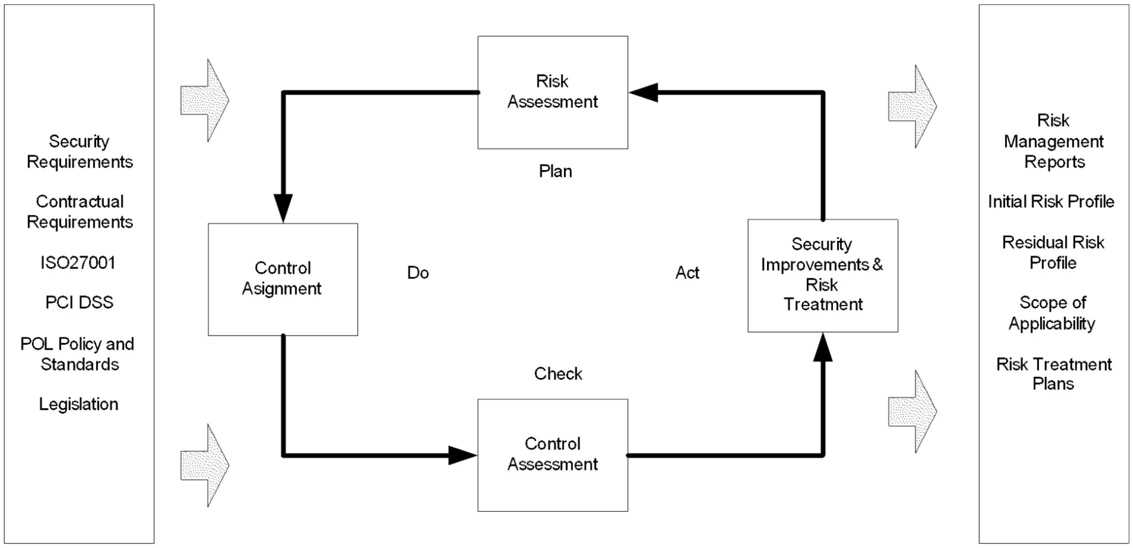
For the purpose of the RMGA ISMS other Fujitsu business units will be treated as external parties as per section 4.5 above.

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) Manage Risk Process.

6.5 Risk Management Approach (Methodology & Tools)

Risk management is a continuous and iterative process which underpins the ISO27001

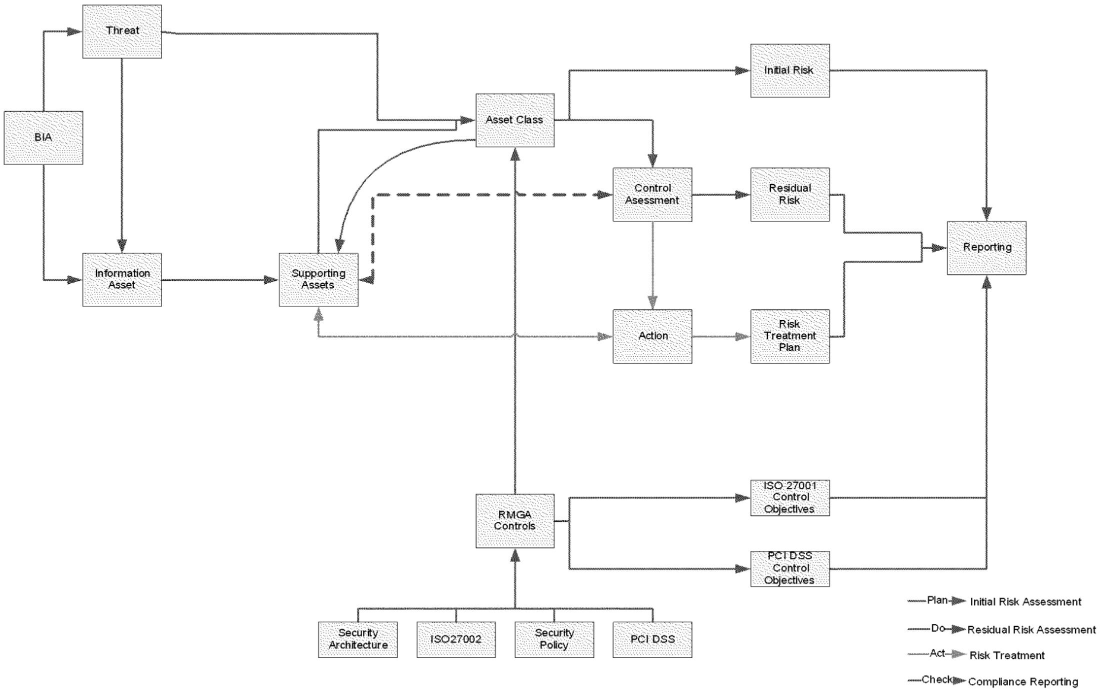


RMGA has selected the Acuity Stream risk management tool to manage:

- 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



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.

6.6 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 RMGA CISO/ISMF, in conjunction with the risk owners.

6.7 Risk Treatment Options

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.

6.8 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.

7 Organising Information Security

The information security organisation within RMGA is, under the leadership of the Account Director, through his role as chair of the RMGA Information Security Management Review (ISMR). The ISMR is made up of a core membership representing key areas of the RMGA account business..

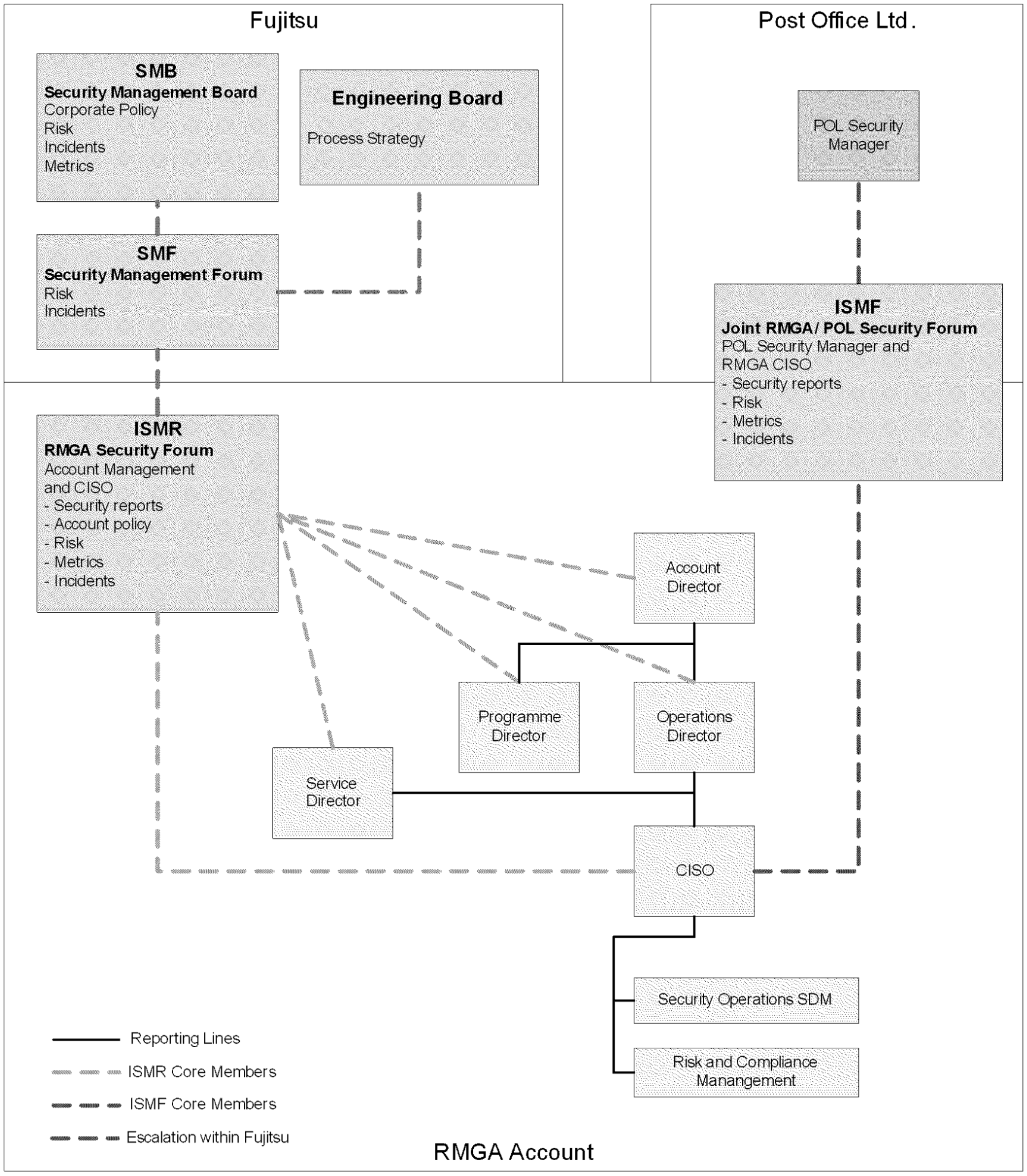
Information security liaison between Post Office Ltd and RMGA is conducted through the Information Security Forum (ISMF). Whose core membership comprises the RMGA CISO and Post Office Ltd. Security Manager.

The CISO is responsible to the Account Director for management of all information security matters within the scope of the registration; He is also a member of both the ISMR and ISMF and maintains contact with the Fujitsu Security Management Forum (SMF)

At Both the ISMR and ISMF information security reports, risks, metrics and incidents are considered. The ISMR in addition is considered the acceptance body for RMGA account security policies. Minutes are taken of actions and decision for both these forums and are stored in Dimensions.

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

In terms of precedent the ISMR is considered as the authoritative body for the RMGA account..



7.5.1 Information Security Management Review

To ensure that areas of security risk or concern are assessed, appropriate controls are defined and effectively implemented and to manage levels of security risk to an appropriate level there is a Management forum, the RMGA Information Security Management Review meeting. Objectives and responsibilities of the meeting are documented in “Fujitsu Services RMGA ISMR Terms of Reference (SVM/SEC/STD/0027)”. Also included in the document is a membership list, mode of operation and deliverables

The RMGA ISMR is responsible for:

- Approval for strategies and master policies supporting the Objectives.
- Identifying and reviewing metrics measuring the effectiveness of Security activities across the RMG Account
- Ownership of ISMS Management Review Change Control processes

7.5.2 Information Security Service Review

Regular reviews of the RMGA Information Security Service are conducted through the ISMF which is attended both by the RMGA CISO and the PO Ltd. Security Manager

8 Document and Record Management

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

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

8.5 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
RMGA Information Security Management Forum TOR's	Dimensions	Life of the ISMS
Risk Registers	Dimensions	Life of the ISMS
Risk Treatment Plans	Dimensions	Life of the ISMS
Integrated Audit Plan	Dimensions	Current year +1
Audit Reports	Dimensions	7 years
Reports of Security Incidents	Dimensions	7 years
ISMF Minutes	Dimensions	Life of the ISMS
Information Security Monthly Report	Dimensions	Life of the ISMS

9 Key Personnel

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

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

9.5.1 Fujitsu Services RMG Account Director

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

- Overall control and management of information security throughout the Fujitsu Services RMG Account;
- Chairmanship of the ISMR
- Provision of adequate resources for information security;
- Appointing an experienced security professional responsible for managing and coordinating security across the complete RMGA domain.
- Approval authority for the Fujitsu Services RMGA Information Security Policy;
- Establishing the information security interface with the customer; and
- Establishing the information security interface with all Fujitsu Services subcontractors

Senior management is supported by the Information Governance staff which consists of experienced specialists with specific expertise in the areas of IT security and risk management.

9.5.2 Fujitsu Services RMGA Operations Director

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

- Line management for the Chief Information Security Officer; (CISO);
- Ownership and overall control and management of operational security throughout RMGA;
- Day to day management of security related risks;
- Chairing the RMGA Information Security Management Review Board;
- Acting as the approval authority for Royal Mail Group Account's Security Procedures; and
- Overall control of risk management and audit functions, including deciding the criteria for accepting risks and the acceptable levels of risk.

9.5.3 Fujitsu Services RMGA Programme Director

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

- Ensuring that responsibilities and procedures for the management and operation of all information processing facilities are established, documented and maintained; and
- Ensuring that changes to information processing facilities and systems are controlled.

9.5.4 Quality Manager

The information security-related responsibilities of the Fujitsu Services RMGA Programme Assurance Manager include:

- Overall control of risk management and audit functions;
- Co-ordinating all audit related activities;
- Providing a point of contact for external audit personnel;
- Planning and carrying out audits of RMGA's business functions; and
- Maintaining an integrated audit plan.

9.5.5 Chief Information Security Officer (CISO)

The CISO is responsible for the overall design of RMGA's security control framework. The CISO will lead the engagement with customer stakeholders with an interest in governance, control and security matters. The CISO will ensure the responsibilities of the Information Governance and Operational Security Teams are met. Full details are contained within the "RMGA CISO Terms of Reference" (Ref SVM/SEC/STD/0026) and include:

Developing and publishing all security-related policies and guidelines applicable at RMGA level;

- Reviewing and approving information security policies and procedures owned and implemented at business level;
- Providing a point of contact for POL Head of Information Security

Ensuring that security incidents are recorded and investigated;

Monitoring for compliance with the RMGA Information Security Policy;

Ensuring all RMGA Staff are screened in line with contractual requirements, FS Group Policy and this policy;

Ensuring that security relevant events are recorded

Ensuring that system audit trails are analysed on a regular basis;

Defining the information security risk assessment approach of RMGA:

Analysis and evaluation of information security risks and evaluating options for the treatment of risks; and

Co-ordinating the implementation and operation of the Information Security Management System.

9.5.6 Staff Responsibilities

All RMGA 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 RMGA 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

9.5.7 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	ISRB	General ISMS Awareness + BMS.

10 Compliance and Reporting

10.5 ISO27001 Compliance Audits

In support of the ISO27001 compliance requirements, and to provide ongoing assurance of compliance, regular compliance audits 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 ISO27001 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. BS7799/ISO27001 Lead Auditor/ Auditor.

Audits are carried out as part of the RMGA Internal Audit Plan (PGM/PAS/PLA/0005). 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 ISO27001 registration, independent external audits will be conducted as determined by the audit body.

10.6 Reporting

Information Governance staff provide a monthly Information Security Reporting Pack which informs the Management Team, as an input to the Fujitsu Services RMGA ISMR, of RMGA ISO27001 compliance status, results of audits and current risk status. It is intended that the details contained in this report will expand over time. This includes reports from the Operational Security Team such as a summary of the types and numbers of incidents that may impact on the confidentiality, integrity or availability of RMGA systems.

A subset of this monthly report is included in the Service Review Book which is provided monthly to the customer.

10.7 Supporting Post Office Ltd Compliance

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

- Achieving ISO27001 compliance and registration
- Ensuring agreed information security controls are managed and effective
- Completing security questionnaires from POL and any of its clients.
- 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.

10.8 Legal Compliance

The Fujitsu Servcies 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 Information Services Security Policy (ITS/M1) and all of the related sub-policies specific to the use of corporate assets and corporate network activity.

ITS/17 provides a specific policy statement on the review of processes against current legislation and standards and contains a link to a sub-document of the legislation and standards relevant to IT processes.

IRRELEVANT

11 Communication and Awareness

A programme of security awareness training, including Information Security overviews, is provided to all new Fujitsu arrivals, as part of induction training. The service covers the provision of periodic awareness activities as defined in the RMGA communications plan..

.

12 Operational Security

12.5 User Administration

The Operational Security 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 before being given access to the live Service.

The Operational Security Service Delivery 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.

12.6 Administration of Changes

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

The Operational Security 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.

12.7 Acceptance into Service

Responsibility for accepting new Services rests with the Service Transition Management Team. who are responsible for ensuring that new services identify their security requirements and that the security elements of Acceptance into Service have been met.

12.8 Analyse Security Logs

The Operational Security 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 RMGA Customer Service Incident Management Process.

12.9 Anti-Virus and Malicious Software Management

The Operational Security team provides a number of anti-virus and malicious software management activities. For HNG-X, the updated version of Sophos cover malware as well as anti-virus.

Managing the distribution of updated anti-virus software across the live estate to protect the Services from malicious software, including regular DAT 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;

12.10 Security Incident Management

The Operational Security Team participate in the RMGA Customer Service Incident Management Process (SVM/SDM/PRO/0018)and RMGA 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 details to POL, as well as attending the monthly ISMF meeting to review information security incidents.

12.11 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.

12.12 Information Retrieval and Prosecution Support

The operational security 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).

12.13 Physical Access Control

The Operational Security Team is responsible for the administration, issue and control of the Fujitsu Services (Royal Mail Group Account) Ltd Horizon Security Passes. All staff who 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 Royal Mail Group Account (RMGA) to be identified as those who have been successfully vetted by Post Office Limited (POL).

13 Business Continuity Management

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

14 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.

FUJ00232619

15 Appendix A – SITE, FUNCTIONS, STAFF

Site	Function	Operational Unit	No. of Staff
BRA01	3rd Line Support - ISP&DSL	Network Operations	1
	3rd Line Support - Voice	Network Operations	1
	NOSS	Network Operations	1
BRA01			9

FUJ00232619

Total			
	Business Operations	Datacentres	1
HOM99	Business Operations	Datacentres	2
	Capacity, GE and Assss	Datacentres	6
	Data Centres HQ	Datacentres	4
	Regional DC North	Datacentres	1
	Sales Engagement	Datacentres	1
	Strategy and Development	Datacentres	1
	Data Centres & Networks HQ	Datacentres & Networks - HQ	2
	3rd Line Support - FSBN, MWS & Shared La	Network Operations	2
	3rd Line Support - Voice	Network Operations	2
	3rd Party Management - Direct Costs	Network Operations	3
	Network Operations HQ	Network Operations	1
	Network Security Support	Network Operations	12
HOM99 Total			37
IRE11	Business Operations	Datacentres	3
	Regional DC North	Datacentres	40
	3rd Line Support - Northern Ireland	Network Operations	7
	Network Operations Centre - NI	Network Operations	1
IRE11 Total			51
IRE19	Network Operations Centre - NI	Network Operations	31
Location X	3rd Line Support - Northern Ireland	Network Operations	2
	Network Operations Centre - NI	Network Operations	1
Location X total			3
Location Y	Business Operations	Datacentres	1
	Capacity, GE and Assss	Datacentres	1
Location Y Total			2
Grand Total			X
BRA01	Service Delivery	Service Delivery	5

		Management	
BRA01	Service Support	Service Delivery Management	9
BRA01	Operations Support	Service Delivery Management	4
BRA01	Release Management	Service Delivery Management	5
STE04	Service Delivery	Service Delivery Management	2
MAN34	Service Support	Service Delivery Management	1
BRA01	Reference Data	Service Delivery Management	7
HOM99	Service Delivery	Service Delivery Management	2
BRA01	Service Transition	Service Delivery Management	4
CRE02	Operation Business Change	Service Delivery Management	6
BRA01	Commercial	Commercial Management	2
LON22	Commercial	Commercial Management	1
BRA01	Finance	Finance Management	4
HOM99	Sales	Business Development	1
BRA01	Account Management	Business Development	2
HOM99	Architect	Business Development	4
BRA01	Programme Management	Business Development	1
BRA01	SSC/ Application Support	SSC/ Application Support	25
HOM99	Security	Security & Risk Management	1
WAR13	Security	Security & Risk Management	1
LON22	Security	Security & Risk Management	1
BRA01	Security	Security & Risk	1

		Management	
LON22	Project Management Office (PMO)	Project Management	1
BRA01	Project Management Office (PMO)	Project Management	4
BRA01	Deployment	Project Management	7
BRA01	Delivery	Project Management	8
HOM99	Delivery	Project Management	1
BRA01	Account Leadership	CS Operations	5
		TOTAL STAFF	345[1]

16 Appendix B – Assets

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

[1] This figures fluctuates on a regular basis; staff are brought in for a specific item of work, quite short term sometimes, and then leave the Account

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	RMGA 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