POL00401509

Security Management Service: Service Description
FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)

Document Title:	Security Management Service: Service Description
Document Reference:	SVM/SDM/SD/0017
Document Type:	Service Description – Contract Controlled Document
Release:	HNG-X and HNG-X Application Roll Out Transitional Period
Abstract:	Service Description for the Security Management Service as provided under contract to Post Office
Document Status:	APPROVED
Author & Dept:	Kumudu Amaratunga , POA Security Operations Manager
External Distribution:	Julie George Post Office: Head of Information Security
Security Risk Assessment Confirmed	YES. See section 0.9.

Approval Authorities:

Name	Role	Record in Dimensions	
Steve Beddoe	Post Office: Senior Service Delivery Manager		
Keith Smith	Fujitsu Services: POA CISO		
Peter Thompson	Fujitsu Services, POA Service Director		
Julie George	Post Office: Head of Information Security		

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

POL00401509

0 Document Control

0.1 Table of Contents

POL00401509

POL00401509

0.2 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
1.0	24/08/06	Agreed	
1.1	28/08/08	Amendments after Aug 08 review with POL	
2.0	31/12/2008	Agreed	
2.1	09/08/2010	Amendments after review of service . Change for CT0724	
2.2	13-Oct-2010	Updated in response to review co mments	
3.0	15-Oct-2010	Approval version	
3.1	28 –Oct 2013	Amendments for CCNs listed	CCN1305a, CCN 1306a, CCN1309a, CCN 1332a
3.2	30-Oct-2013	Revised following CISO review.	As above
3.3	12-Nov-2013	Minor corrections for review version.	As above
3.4	22-Nov-2013	Definition of abbreviations from 2.1.7 (G) added to section 0.5.	
3.5	25-Nov-2013	Corrections to document references in 0.3; 2.1.6; 2.1.9.1,	
4.0	04-Dec-2013	Approval version	
4.1	20 –Mar-2014	Amendment for CCN listed ; deleted section 3 HNG-X Applications Roll Out – Transitional Period ; corrected section numbering.	CCN1400
5.0	04-Apr-2014	Approval version	CCN1400
5.1	03-Mar-2015	Draft incorporating BPO426	

0.3 Review Details

Review Comments by :	
Review Comments to :	Kumudu Amaratunga & Post Office Account Document Managementmailto:

Mandatory Review	
Role	Name
Post Office: Head of Information Security	Julie George
Post Office: Senior Commercial Manager	Liz Tuddenham
Fujitsu Services: Senior Commercial Manager	Sarah Guest
Fujitsu Services: CISO	Keith Smith
Post Office: Senior Service Delivery Manager	Steve Beddoe
Optional Review	
Role	Name
Fujitsu Services: Commercial Manager	Adrian McMahon Stone
Post Office: Commercial Manager	Sue Stewart
Fujitsu Services: SSC (for Configuration Management)	Steve Parker; sscdm GRO
Fujitsu Services: Security Architect	Dave Haywood
Fujitsu Services: Senior Operations Manager	
Issued for Information – Please restrict this	

POL00401509

distribution list to a minimum	
Position/Role	Name
Post Office: Head of Systems Operations	Dave Hulbert

(*) = Reviewers that returned comments

0.4 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)			Security Management Service: Service Description	Dimensions
SVM/SDM/PRO/0018			CS Incident Management Process	Dimensions
SVM/SEC/POL/0003			Post Office Account HNG-X Information Security Policy	Dimensions
SVM/SEC/STD/0006			Information Risk Management Approach	Dimensions
SVM/SEC/STD/0027			Information Security Management Review	Dimensions
SVM/SDM/SD/0015			Reconciliation Service, Service Description	Dimensions
(POL: POL/HNG/CIS/001)SVM/SEC/POL/0005			POL Community Information Security Policy for Horizon	Dimensions
SVM/SEC/PRO/0018			Audit Retrieval Process	Dimensions
SVM/SEC/PRO/0017			Management of the Prosecution Support Service	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
APOP	Automated Payment
ARQ	Audit Retrieval Query
CAN	Certification Authority Server
CCD	Contract Controlled Document
CISP	Community Information Security Policy
EPOSS	Electronic Point of Sale
FIM	File Integrity Monitoring
ID	Identification Number
IDS	Intrusion Detection System
IPS	Intrusion Prevention System

POL00401509

Abbreviation	Definition
ISO	International Standard
KMNG	Key Management
MIS	Management Information System
NPS	Network Persistent Store
PAN	Personnel Authentication Number
PCI DSS	Payment card Industry Data security Standard
PIN	Personnel Identifier Number
POL	Post Office Ltd
POA	Post Office Account
TES QA	Transaction Enquiry Service
TOR	Terms of Reference
VPX	HNG-X VPN (Virtual Private Network) Server
VSD	Virtual Server Host Discrete

0.6 Glossary

Term	Definition

0.7 Changes Expected

Changes
A revised version of this document will be produced incorporating the requirement of PCIv3 (subject to a Change Request)

0.8 Security Risk Assessment

Security risks have been assessed and it is considered that there are no security risks relating specifically to this document.

POL00401509

1 SERVICE SUMMARY

1.1 Introduction

The Security Management Service provides a range of security-related activities that support the establishment and maintenance of an ISO 27001 compliant infrastructure. The Security Management Service monitors operations and introduces specific protective security controls to maintain the integrity, availability and confidentiality of information used and produced by the various Services, other than the Service Integration Service.

For the avoidance of doubt from 01 April 2014 this Security Management Service excludes any activity related to Credence or POLSAP systems. Such activity is included in the scope of the Credence/MDM Service, POLSAP Hosting Service or POLSAP Application Support Service. This service has never included any activity relating to the Salesforce Support Service.

1.2 Deliveries

Fujitsu Services' contractual obligations for delivering and maintaining provision of a secure system is set out in Clause 16 (Security) of the Agreement. The Security Management Service consists of the following elements:

(a) Implementation and maintenance of Post Office security policy and procedures

(b) Compliance monitoring and audit

(c) Cryptographic key management

(d) Security event management and firewall event analysis

(e) System and physical access control

(f) Anti-virus and malicious software management

(g) Monitoring of any IDS or IPS in place

(h) Security incident reporting and problem management

(i) System security change management

(j) Security awareness and training

(k) Information Retrieval and Audit

(l) Subject Information Requests management

(m) Prevailing threats and vulnerability management

(n) Litigation support

(o) Commission external SOC1 report against ISAE3402 standard (as detailed in Section 2.1.17)

(p) Management of Risk

(q) Monthly Reporting

(r) File Integrity Monitoring

(s) PCI DSS support

(t) PCI DSS internal penetration testing

POL00401509

1.3 Training

The Security Management Service staff will be appropriately trained to carry out the Service and training requirements reviewed on a yearly basis.

1.4 Responsibilities

In performing the Security Management Service, Fujitsu Services shall be responsible for:

A. Delivery of the security policy as specified in paragraph 4.1.3 of Schedule A4 of the Agreement;

B. Maintaining with Post Office the identity of the persons from both Parties authorised to receive sensitive security-related material (including cryptographic key components); and

C. Liaising with Post Office in the manner described in the CCD entitled: "Post Office HNG-X Account Information Security Policy" (SVM/SEC/POL/0003).

D. Running monthly internal Information Security Management Review (ISMR) providing agreed monthly reports; and

E. Attending monthly customer Information Security Management Forum (ISMF) providing agreed monthly reports.

POL00401509

2 HNG-X

2.1 SERVICE DEFINITION

2.1.1 SECURITY ORGANISATION AND MANAGEMENT

Security organisation and management within the Security Management Service provides a number of organisational and management activities required for compliance with ISO 27001 and to support PCI DSS standard. These are:

A. The setting up and operating of the ISMS compliant with ISO27001

B. the co-ordination of security activities and prioritising of activities according to risk within the appropriate Fujitsu Services Security risk register;

C. the creation and maintenance of security-related procedural and process documentation to assist compliance and help maintain correct operation by Fujitsu Services and Post Office staff;

D. the regular reviews of Fujitsu Services Security Management Service documentation to provide appropriate security input and compliance to the requirements of ISO 9001;

E. the management of ISO 27001 gap analysis, preparation of a plan for implementation in accordance with agreed terms of reference (TOR) and monitoring of corrective actions; and

F. informing Post Office of any changes to the HNG-X Infrastructure and Applications that are likely to have an impact upon security.

G. Support POL with PCI DSS framework to achieve their compliance

2.1.2 COMPLIANCE MONITORING AND AUDIT

Compliance monitoring and audit within the Security Management Service provides a number of compliance monitoring and audit activities required for compliance with ISO 27001. These are:

A. the undertaking of periodic physical security and system security audits of the Data Centre and other locations used to provide the Services, other than the Service Integration Service, on a risk management basis to provide ongoing assurance of compliance to security policies and procedures. Activities will include reviews of operational processes, provision of reports covering IT, environmental, physical, personnel security etc. and the monitoring of identified corrective actions;

and

B. the provision of advice and guidance on issues affecting personnel security within Fujitsu Services including the investigation of personnel security issues and staff vetting queries.

C. Produce a monthly plan to address the various Audit and ISO/IEC 27001 compliance issues, and shared with the customer in the monthly review

2.1.3 CRYPTOGRAPHIC KEY MANAGEMENT

The cryptographic key management element of the Security Management Service provides a number of cryptographic key management activities. These are:

POL00401509

A. management of the KMNG Workstation and the Active Directory SubCA for the creation, distribution and installation of required cryptographic material to the live estate and the maintenance of periodic key replacement for all Branches in addition to the safeguarding of live and reserve keys;

B. operation of Key management functionality and configuration changes to the HNG-X Application in order to optimise service;

C. management of KMNG and Active Directory (SubCA) event logging and incident handling to assist the Systems Management Service, the Third Line Support Service and the Application Support Service (Fourth Line) in error resolution and problem management;

D. Management of the manual cryptographic estate by maintaining the creation, distribution, auditing and periodic replacement of cryptographic keys within agreed timescales; and

E. Supervision and management of the Root CA (CAN) as the trust anchor of the HNGx system.

2.1.4 PIN PADS

2.1.4.1 The Security Management Service shall ensure PIN Pads comply with the requirements of ISO 9564. Fujitsu Services' key management service for any key directly or indirectly protecting the secrecy of PIN values (together, "PIN Encryption Keys") shall comply with ISO 11568 Parts 1 to 3.

2.1.4.2 The key management service used between each PIN Pad and the rest of the HNG-X Services shall be the DUKPT scheme as described in paragraph 6.2 of Schedule A4 of the Agreement.

2.1.4.3 In the event of an actual or suspected key compromise in respect of a PIN encryption key used within the HNG-X Services, Fujitsu Services shall implement key change mechanisms in accordance with the principles stated in ISO 11568 Parts 1 to 3.

2.1.5 SECURITY EVENT MANAGEMENT AND FIREWALL EVENT ANALYSIS

The security event management and firewall event analysis element of the Security Management Service provides a number of security event management and firewall event analysis activities. These include:

A. management of audit mechanisms to monitor detect and record events that might threaten the security of the HNG-X Service Infrastructure;

B. operation of the security event management system utilising the Systems Management Service system to track and report events of security significance and daily monitoring of the security event management system to identify relevant events and logging of details;

C. regular analysis of audit trails to identify new features and vulnerabilities introduced by new systems to facilitate trend analysis and to assist the investigation of security breaches;

D. reviewing security configurations of event filters to optimise efficiency and minimise security weaknesses;

E. undertaking risk assessments to establish adequate firewall policies / rule bases and the subsequent monitoring of events generated by the HNG-X Service Infrastructure;

F. analysis of firewall event logs using trend analysis software to identify the presence of any potential attacks or of areas of vulnerability and the provision of advice for any remedial action; and

POL00401509

G. prompt investigation and remedial action in order to minimise the impact of any security breach.

2.1.6 SYSTEM AND PHYSICAL ACCESS CONTROL

The system and physical access control element of the Security Management Service provides a number of system and physical access controls which are defined within the document entitled "Access Control Policy" (RS/POL/003), these are:

2.1.6.1 SYSTEM ACCESS CONTROL

A. Management of the process for validating those Users are authorised before being permitted access to the HNG-X Service Infrastructure.

B. Management of the allocation and auditing of authentications tokens are used to validate that Fujitsu Services users who access the HNG-X Central Infrastructure from locations remote from the Data Centres do so via secondary token authentication.

C. Management of system controls in the environment, Data Centre or location where the HNG-X Services are performed.

D. All TES QA users will be approved and a list of users restricted to a maximum of 20 customer users will be maintained by both POL operations and Fujitsu Services. This list will include asset records and user login details.

E. Fujitsu will put controls in place to record all branch global users including Audit and Engineer requesting access, all forms will be submitted to POL as per the agreed process.

2.1.6.2 PHYSICAL ACCESS CONTROL

F. Access to the live or test Data Centre is requested by a Fujitsu Services user via Fujitsu Services' online system in the following manner:

- the Fujitsu Services user will receive an e-mail to acknowledge submission;
- the Data Centre Operations Service will check throughout the day/night for any requests not yet actioned;
- the Data Centre Operations Service will action request with approval or rejection; and
- the Fujitsu Services user will receive notification to sanction request or refuse request with the reason for non-approval.

G. All Fujitsu Services users shall register and sign-in at reception when visiting the various premises occupied by the Systems Management Service and Third Line Support Service respectively.

2.1.7 ANTI-VIRUS AND MALICIOUS SOFTWARE MANAGEMENT

The anti-virus and malicious Software management element of the Security Management Service provides a number of anti-virus and malicious software management activities These are:

A. management of the distribution of updated anti-virus software and appropriate signatures across the HNG-X Service Infrastructure to maintain protection of the HNG-X Services from viruses and malicious software;

B. initial configuration of alerting mechanisms and event filters to provide automatic notification and prompt virus incident response;

C. provision of regular updates to identify and cleanse new and emerging virus strains;

POL00401509

D. ensure that the anti-virus products on PCI platform types are configured to automatically download and apply vendor signature updates (this activity may be limited to the last available updates available for the product version that is deployed); and

E. provision of event monitoring and incident response via normal incident handling procedures. Analysis of details to understand the threat and inform corrective actions.

F. monthly reporting in consideration of any of the above.

G. conducting of scheduled scan on PCI platforms and save Log files for further analysis for a period of 18 months. (MIS ,NPS, VSD, VPX Platforms).

2.1.8 PREVAILING THREATS AND VULNERABILITY MANAGEMENT

2.1.8.1 The Security Management Service shall ensure that any prevailing threats and vulnerabilities arising from hackers and / or crackers are managed in accordance with ISO 27001. Such prevailing threats and vulnerabilities may be exploited despite the presence of anti-virus monitoring, firewalls and intrusion detection software which Fujitsu Services has in place throughout the HNG-X Service Infrastructure and may be as a result of:

A. software defects requiring vendor issued patches

B. insecure accounts with weak or non-existent passwords;

C. unnecessary services, for example, Telnet or remote access;

D. built in weaknesses, for example, backdoor accounts; and

E. system mis-configuration.

F. trend analysis and forecasting of potential issues.

2.1.8.2 In managing such prevailing threats and vulnerabilities, the Security Management Service will:

A. assess the existing vulnerabilities on each element of the HNG-X Service Infrastructure;

B. determine the degree of risk for each vulnerability identified;

C. jointly review options to contain or resolve technical system vulnerabilities and take decisions in a monthly customer specific Patch Assessment Board (PAB);

D. Containment or resolve the vulnerability by the updating of Hardware and / or Software versions or by applying vendor issued service packs, hot fixes or Software patches; and

E. perform software patching scans of PCI platform types to determine if actions agreed to contain or resolve technical system vulnerabilities have been implemented and provide reporting into subsequent monthly Patch Assessment Board meetings (this activity may be limited to the vulnerability toolset capabilities and last available updates available for the version that is deployed);

F. in any investigation carried out by Post Office and/or by Fujitsu Services of any potential or actual security breach or threat, Post Office and Fujitsu Services shall report to each other (or Fujitsu Services shall report to Post Office Limited, if required by Post Office) any actual or potential security breach or threat identified in the course of such investigation that may have a material adverse effect upon the security of the Infrastructure. The procedures by which such threats shall be reported and the methodology for investigating and resolving business incidents (disputed Banking & Related Services Transactions are defined within the CCD entitled "Reconciliation Service, Service Description" (SVM/SDM/SD/0015)) shall be as set out in the

POL00401509

Working Document entitled "Security Incident Management, Joint Working Document" (SVM/SDM/PRO/0018).

2.1.9 SECURITY INCIDENT REPORTING AND PROBLEM MANAGEMENT

2.1.9.1 The security incident reporting and problem management element of the Security Management Service provides a number of security Incident reporting and problem management activities defined in detail in the Working Document entitled: "Security Incident Management, Joint Working Document" (SVM/SDM/PRO/0018). These are:

A. provision of a central point of contact for all security related issues;

B. investigation and reporting to Post Office of any actual or potential threats or breaches that may have a material effect on the HNG-X Services in accordance with agreed procedures; and

C. provision of ongoing liaison with Post Office and support to the Fujitsu Services' Security Board as defined in the CCD entitled "Post Office HNG-X Account Information Security Policy" (SVM/SEC/POL/0003).

2.1.10 SYSTEM SECURITY CHANGE MANAGEMENT

The system security change management element of the Security Management Service provides a number of system security change management activities. These are:

A. management of security compliance with agreed change processes and the assessment of the business and security impact of incident and problem management systems including the provision of options for resolution and containment of security and business risk; and

B. assessment of the business and security impact of Change Requests and the assessment and approval/rejection of security related operational Change Requests.

C. monthly reporting on existing service changes

2.1.11 PCI PENETRATION TESTING SERVICE

A penetration testing service will be provided as a call-off service to POL. This service will be provided to POL annually or when required following significant changes to the infrastructure / applications within the PCI cardholder environment.

Fujitsu will organise an internal tester to conduct an infrastructure penetration test of service accessible in the PCI cardholder environment from three external interfaces (Branch, Internet and Support). The testing will cover both Network and Application Layers.

The test will not cover plugging directly into the cardholder environment and a scan of the hosts; as such this test will concentrate on the compromise of services that the firewalls permit access to.

Exclusions:

- If an external test or support for an external test is required this will be subject to Change Control.
- Any remediation work identified as required as part of the penetration test..

2.1.12 FILE INTEGRITY MONITORING

POL00401509

The file integrity monitoring service protects the integrity of personal and sensitive data within the PCI DSS card holder data environment by checking whether the data and logs are not being altered as required by the requirements 10.5.5. of the PCI DSS standard and critical system files. Configuration and content files are monitored as required by requirement 11.5 of the standard.

File integrity monitoring solution (Trip wire) acts to alert personnel about unauthorised modification of critical system files, configuration files or content files and the software should be configured to perform critical file comparison at least on a weekly schedule and monitored by security operations under proactive monitoring.

File integrity monitoring activities will be provided Monday to Friday from 09:00 to 17:30 Hrs excluding public holidays.

2.1.12.1 Configuration Management / Baseline reviews:

- The Fujitsu system architect, platform owners and Security operations resources will identify and agree the initial scanning baseline, identifying files and folders to be scanned and the ones to be excluded.

- The baseline will require initial reviews to be carried out on a monthly basis until the baseline is stable and will then require quarterly reviews to be completed.

- Software, Hardware Maintenance and hosting capability in Fujitsu's Data Centre.

2.1.12.2 Weekly Scanning

Scans scheduled to run on a weekly basis on the applicable PCI platforms as detailed in DEV/GEN/SPE/0007 platform hardware instance list

2.1.12.3 Monitoring of Tripwire Service and Scans

A. Carryout checks to confirm that the Tripwire service is running on all the required PCI platforms, managing any issues/events raise as part of the daily checks

B. Provide product support to interfacing to the third party, to manage the file integrity monitoring product tool set.

C. POA security operation will check the output of scheduled scans – review reports produced and determine why changes occurred and raise an appropriate call for any exceptions that have been identified that are not covered by operational change activities

D. POA security will perform periodic reviews of the baseline on a quarterly basis, identifying any files/folders that should be excluded/added to the schedules and presented for discussion at the next review session whilst including the necessary amendments to the baseline for any changes to the PCI platforms

E. Scans to be retained for period of 12 months and will be available for review

2.1.12.4 Reporting

Report requirements to be agreed between POL and FJS these will be produced and made available to the Information Security Management Forum (ISMF) and Service Management Reviews (SMR)

2.1.12.5 Output from Fujitsu

POL00401509

Monthly reports

- Success/Failures status on reports run and remediation work
- Percentage of file folder exceptions
- Tripwire service availability

2.1.13 PCI SUPPORT FOR POST OFFICE

CCN1332a introduced additional obligations on Fujitsu Services in supporting POL's PCI DSS compliance, as follows:

A. Update of DES/SEC/ION/2006 PCI card holder environment on annual basis

B. Review of actual firewall configuration against SVM/SEC/STD/1985 Operational Firewall policy - on a bi-annual basis

C. Additional review steps to be added to SVM/SEC/PRO/0009 patch management process to include the ranking of vulnerabilities

D. Ongoing provision of the Fujitsu Services managed toolset for tracking Fujitsu Services domain PCI compliance. This includes maintaining relevant software licensing, infrastructure and configuration for Fujitsu Services user access

E. Management of the relevant Fujitsu Service toolset user accounts and ensuring updates are loaded in to the Fujitsu Services toolset for tracking Fujitsu Services domain PCI compliance activities

F. Fujitsu Services will provide resources to support POL in their controlled self-assessment annual audit against the PCI DSS Standard.

2.1.14 SECURITY AWARENESS AND TRAINING

A programme of security awareness training, including Information Security overviews, is provided to all new arrivals, as part of induction training. The service covers the provision of periodic awareness activities and training including induction training, presentations and briefing notes.

Provide monthly reporting on Fujitsu Post Office Account employee security awareness and induction training

The Fujitsu Services POA Security Communications Strategy details the various communication channels that are used and the different vehicles and methods available for ensuring that key messages regarding Information Security are effectively communicated to staff at all levels engaged in the Fujitsu Services POA.

2.1.15 INFORMATION RETRIEVAL AND AUDIT

2.1.15.1 DESCRIPTION OF TERMS

"Banking Transaction Record Query" means a record query in respect of a Banking & Related Services Transaction which the Data Reconciliation Service Host (DRSH) has reconciled or has reported as an exception, the result or records of which are subsequently queried or disputed by Post Office or a third party;

"Audit Record Query" means a record query that is not a Banking Transaction Record Query and which relates to Transactions.

POL00401509

"APOP Voucher Query" means a record query for APOP voucher archived records;

"Note: We are required to hold 7 years transaction records 'old data' is no longer available

"Period One" means, in respect of each Transaction the period of 90 days commencing on the date of that Transaction;

"Period Two" means, in respect of each Transaction the period commencing the day after expiry of Period One for that Transaction, expiring on the earlier of:

A. seven (7) years in the case of Transaction records and

B. the date of completion of transfer of Post Office Data (including the record of that Transaction) in accordance with Schedule E of the Agreement;

"Query Day" means each date against which an Audit Record Query is raised;

"New Data" means the extraction of records created on and following the 3rd January 2003 relating to Banking & Related Services Transactions (and, in the case of Audit Record Queries relating to all Transactions) meeting the Search Criteria, such extraction being limited to specific types of information/data fields as follows:

A. in the case of an Audit Record Query for Horizon transaction records - the ID for the User logged-on, Counter Position ID, stock unit reference, Transaction ID, Transaction start time and date, Customer Session ID, mode (e.g. serve customer), product number and quantity, and sales value, Entry Method, State, IOP Ident, Result, Foreign Indicator; and for HNG-X transaction records - the ID for the User logged-on, Counter Position ID, stock unit reference, Transaction ID, Transaction start time and date, Customer Session ID, mode (e.g. serve customer), product number and quantity, and sales value, Entry Method.

B. in the case of a Banking Transaction Record Query - Banking & Related Services Transaction ID, Banking & Related Services Transaction type, receipt date, receipt time, the reason code (in the case of a discrepancy) and DRSH sub-value(s) (e.g. C0 Confirmation, C1 Confirmation, NB Decline,

an 'Event Log' will also be produced and provided with the Audit Record Query, detailing; for Horizon transaction records - GroupID, ID, date, User, SU, EPOSSTransaction.T and EPOSSTransaction.Ti and for HNG-X transaction records - GroupID, ID, date, User, SU, ReportingEventID and EventDetailMsg.

"Search Criteria" means: To be specified for each individual Record Query. In the case of an Audit Record Query of either:

A. The date or dates (not exceeding 31 consecutive days), and PAN (or equivalent identifier); or

B. The date or dates (not exceeding 31 consecutive days), and Branch ; or in the absence of a Branch the full Branch postal address;

In the case of a Banking Transaction Record Query of either:

A. Date, Branch and PAN; or

B. Date and Branch ,

Fujitsu Services shall have access (such access being restricted to properly authorised Fujitsu Services staff) to records of each Banking & Related Services Transaction during Period One and Period Two.

2.1.15.1.1 Fujitsu Services shall carry out the data queries in accordance with the limits set out in section 2.4.1 of this Security Management Service, Service Description.

2.1.16 LITIGATION SUPPORT

POL00401509

2.1.16.1 Where Post Office submits an Audit Record Query in connection with litigation support, at Post Office's request Fujitsu Services shall, in addition to conducting that query:

A. present records of Transactions extracted by that query in , Excel or native flat file format, as agreed between the Parties; and

B. subject to the limits set out in section 2.4.1 analyse:

I. In order to check the integrity of records of Transactions extracted by that query;

II. request and allow the relevant employees of Fujitsu Services to prepare witness statements of fact in relation to that query, to the extent that such statements are reasonably required for the purpose of verifying the integrity of records provided by Audit Record Query and are based upon the analysis and documentation referred to in this section 2.1.13 of this Security Management Service, Service Description; and

III. request and allow the relevant employees to attend court to give evidence in respect of the witness statements referred to in the sub-section (c) (III) above;

C. provided that:

IV. Fujitsu Services' obligations set out in sub-sections (a) and (b) above shall be limited, in aggregate, to dealing with a maximum of 150 (in aggregate) Record Queries per year (on a rolling year basis);

V. Fujitsu Services' obligations in the case of provision of witnesses referred to in sub-section (c) above shall be to provide witnesses to attend court up to a maximum (for all such attendance) of 60 days per year (on a rolling year basis).

2.1.16.2 For the avoidance of doubt the target times set out in Table 1 for dealing with Audit Record Queries shall not apply in respect of Fujitsu Services' obligations under sub-section 2.1.13.1(c) above.

2.1.16.3 Any information requested beyond that available by Audit Record Query and/or any witness statements or witness attendance beyond that available in accordance with section 2.1.13.1 of this Security Management Service, Service Description shall be agreed on a case by case basis and shall be dealt with in accordance with the Change Control Procedure.

2.1.16.4 Sensitive card data included in records of Banking & Related Services Transactions extracted by record query and provided to Post Office (but, for the avoidance of doubt, not that included in records for Transactions extracted for Audit Record Queries in respect of any other Business Capability and Support Facility) shall be in the encrypted form in which they are held.

2.1.16.5 The Security Management Service shall ensure reasonable access to the audit trail of Banking & Related Services Transactions for Post Office auditors for audit purposes which access shall be by written request and reasonable notice to Fujitsu Services.

2.1.17 SOC1 ISAE3402 Support

Fujitsu Services shall support Post Office by commissioning an external auditor to perform a SOC1 report against the set of relevant controls from the ISAE3402 standard as agreed for the 2014 audit.

2.1.18 MANAGEMENT OF SECURITY RISKS

POL00401509

Fujitsu Services has an approved approach to the management of information security risk for POA which is documented in POA Information Risk Management Approach.

Fujitsu Services POA is required to conduct a robust programme of risk management (incorporating risk identification, assessment and containment) as a means of determining and confirming the appropriateness of information related security controls for Programme systems and services. The risk management programme is, on a day-to-day basis, undertaken by the Fujitsu Services POA IG staff. Although the options for risk management (i.e. acceptance, transfer, containment etc) are determined by the IG staff and the decision taken by the appropriate Programme or Operational management team, security risk oversight lies with the Information Security Management Review Body (ISMR), which is the highest authority within the Fujitsu Services POA for the management of information security risks.

2.1.19 MONTHLY REPORTING

Information Governance staff provide a monthly Information Security Reporting Pack which informs the Management Team, as an input to the Fujitsu Services POA ISMR, of progress towards ISO27001 compliance, 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 POA systems.

This report, together with report sub-sets contained in the service review book, is provided to the customer on a monthly basis.

2.2 SERVICE AVAILABILITY

The Security Management Service will be available between 09:00hrs to 17:30hrs Monday to Friday excluding all Bank Holidays. In exceptional circumstances such as Business Continuity or in responding to major security incidents the service will be extended as necessary to support these requirements.

2.3 SERVICE LEVELS AND REMEDIES

2.3.1 GENERAL PRINCIPLES

2.3.1.1 The performance of the Security Management Service against the Operational Level Target (OLT) applicable in respect of the relevant Security Management Service shall be measured and reported and success or failure against each shall be judged over the OLT calendar month.

2.3.1.2 The values applicable to each of the Security Management Service OLTs are identified within section 2.3.6 of this Security Management Service, Service Description.

2.3.2 SERVICE LEVEL RELIEF

This section is not applicable to the Security Management Service.

2.3.3 RECTIFICATION PLAN

See paragraph 7.1 of Schedule C1 of the Agreement

POL00401509

2.3.4 SERVICE LEVELS FOR WHICH LIQUIDATED DAMAGES APPLY

There are no specific SLTs applicable to the Security Management Service for which liquidated damages apply.

2.3.5 SERVICE LEVELS FOR WHICH NO LIQUIDATED DAMAGES APPLY

There are no specific SLTs applicable to the Security Management Service for which liquidated damages do not apply.

2.3.6 OPERATIONAL LEVEL AGREEMENT

Table 1 describes the OLTs applicable to the Security Management Service.

TABLE 1

	(1) **Banking Queries**	(2) **Limits on Audit Record Queries**
	7 Working Days	**Period One and Period Two**
Target Time		Subject to section 2.4.1, and applicable only in respect of Audit Record Queries, 7 Working Days (for queries of 14 or less days' duration) and 14 Working Days (for queries of greater than 14 days' duration).

2.3.7 PERFORMANCE METRICS

There are no contractual performance metrics applicable to the Security Management Service.

2.3.8 DESIGN TARGETS

There are no design targets applicable to the Security Management Service.

2.4 SERVICE LIMITS AND VOLUMETRIC'S

2.4.1 RECORD QUERIES

Table 2 defines the limits on Record Queries, including APOP Voucher Queries which Fujitsu Services shall be obliged to complete.

POL00401509

TABLE 2

	(1) Limits on Banking Transaction Record Queries		(2) Limits on Audit Record Queries
	Periods One and Two		**Period One and Period Two**
Limits	200 per year (on a rolling year basis) with no more than 24 in any calendar month		Subject to section 2.4.1, the limit per year (on a rolling year basis) shall be the first of the following to be reac hed; (i) 720 Audit Record Queries & APOP Voucher Queries or; (ii) 15,000 Query Days; APOP Voucher Queries being limited to 50 per year (on a rolling year basis) The limit per calendar month, allowing a 'burst rate' of 14% shall be the first of the following to be reached, of which not more than 10 shall be APOP Voucher Queries: (i) 100 Audit Record Queries, or (ii) 2100 Query Days subject to the constraints of the agreed annual limits above.

2.4.1.1 The limits set out in column 1 in Table 2 above and the provisions of this section 2.4.1 of this Security Management Service, Service Description shall apply in connection with the application of those limits.

2.4.1.2 The limits set out set out in the column 2 in Table 2 above and the provisions of this section 2.4.1 of this Security Management Service, Service Description shall apply in connection with the application of those limits with effect from the date of commencement of HNG-X Project Workstream X4 (HNG-X Application Roll Out).

2.4.1.3 For the purpose of applying the limits in column 2 in Table 2 above from the date of commencement of HNG-X Project Workstream X4 (HNG-X Application Roll Out) the number of queries equivalent to Audit Record Queries (and associated Query Days) that were carried out in the period up to 12 months prior to that date shall be included in calculating whether the annual limit has been reached (on a rolling year basis).

2.4.1.4 For the purpose of applying the limits in column 2 in Table 2 to the month in which the HNG-X Project Workstream X4 (HNG-X Application Roll Out) commences, the Audit Record Queries carried out since the commencement of that calendar month shall count towards the limits of Audit Record Queries for that month.

2.4.1.5 Where:

D. a new Audit Record Query which is received by Fujitsu Services or where Post Office requires analysis of an existing Audit Record Query; and

E. a member of Fujitsu Services' personnel is needed to deal with that new or existing Audit Record Query; but

F. that person is unavailable due to his or her attendance at court or other proceedings in connection with an Audit Record Query,

2.4.1.6 the target times specified in column 2 to Table 1 shall not apply to that new or existing Audit Record Query which the Security Management Service shall instead deal with as soon as reasonably practicable.

POL00401509

2.4.1.7 For the avoidance of doubt, the limits set out in column 1 to Table 2 in respect of Banking Transaction Record Queries shall not apply in respect of reconciliation incident management and settlement reporting carried out as a function of the DRSH.

2.4.1.8 Post Office may at any time on three (3) months' written notice vary the aggregate limits of Audit Record Queries which Fujitsu Services is required to carry out as specified in column 2 in Table 2, between:

A. the limits specified in Table 2; and

B. the following substitutes for those limits (applicable on the same basis): 1020 Audit Record Queries or 21250 Query Days per year on a rolling year basis, and a maximum, allowing a 'burst rate' of 14%, of 142 Audit Record Queries or 2975 Query Days per calendar month;

and between:

A. the substitute limits set out above;

and

B. the following substitutes for those limits (applicable on the same basis): 1500 Audit Record Queries or 31250 Query Days per year on a rolling year basis, and a maximum, allowing a 'burst rate' of 14%, of 210 Audit Record Queries or 4375 Query Days per calendar month.

2.4.1.9 Post Office shall submit Banking Transaction Record Queries to the Security Management Service.

2.5 ASSETS AND LICENCES

2.5.1 ASSETS

There are no assets associated with the Security Management Service.

2.5.2 LICENSES

There are no licences associated with the Security Management Service.

2.6 CHARGES

2.6.1 OPERATIONAL FIXED CHARGES

See Schedule D1 of the Agreement.

2.6.2 OPERATIONAL VARIABLE CHARGE

The Security Management Service operational variable charge is calculated against the number of Branches at a price per Branch as defined in Schedule D1 of the Agreement.

2.6.3 ADDITIONAL OPERATIONAL VARIABLE CHARGE

POL00401509

2.6.3.1 The additional operational variable charge applicable to the Security Management Service is applicable to the number of Audit Record Queries logged as defined in section 2.4.1 of this Security Management Service, Service Description.

2.6.3.2 Fujitsu Services' charges in respect of dealing with any Audit Record Queries up to the limits set out in section 2.4.1.2 shall be as specified in Schedule D1 of the Agreement.

2.7 DEPENDENCIES AND INTERFACES WITH OTHER OPERATIONAL SERVICES

Any changes agreed between Post Office and Fujitsu Services to the scope or availability of the Security Management Service and/or any of the other Operational Services will be agreed in accordance with the Change Control Procedure. As at the Amendment Date, this Security Management Service interfaces with all of the Operational Services.

2.8 POST OFFICE DEPENDENCIES AND RESPONSIBILITIES

In addition to the generic Post Office responsibilities set out in Schedule A5 of the Agreement, Post Office shall comply with section 2.4.1.8 of this Security Management Service, Service Description.

2.9 BUSINESS CONTINUITY

There are business continuity arrangements set up for the Security Management Service. The facilities are located at Sackville House in Lewes and provide a complete back up service to the Live Operation.

2.10 DOCUMENTATION SET SUPPORTING THE SERVICE

See the document set listed at section 0.4 of this Security Management Service, Service Description. Should any elements of the Security Management Service be changed following agreement with Post Office, Fujitsu Services will ensure these documents are also reviewed and amended where necessary in line with changes agreed.