FUJ00232654

Post Office HNG-X Account ISMS Manual

FUJITSU RESTRICTED
COMMERCIAL IN CONFIDENCE

Document Title: Post Office HNG-X Account ISMS Manual

Document Reference: SVM/SEC/MAN/0003

Document Type: Manual

Release: N/A

Abstract: An approach and framework to implementing, maintaining, monitoring and improving Information Security on the Post Office HNG-X Account.

Document Status: APPROVED

Author & Dept: Chris Cole – Post Office Account Security Management Team

Approval Authorities:

Name	Role	Signature	Date
Tom Lillywhite	Post Office Account CISO		

FUJ00232654

0 Document Control

Table of Contents

0 DOCUMENT CONTROL 2
Table of Contents 2
0.1 Document History 7
Review Details 8
Associated Documents (Internal & External) 10
Abbreviations 13
Glossary 16
Changes Expected 16

1 INTRODUCTION AND SCOPE 17
1.1 ISMS Manual Overview 17
1.2 Scope 17
1.2.1 Statement of Scope 17
1.2.2 Exclusions 17
1.2.3 Statement of Applicability 17

2 INFORMATION SECURITY MANAGEMENT 18
2.1 Information Security Definition 18
2.2 ISMS Operating Procedures 18
2.2.1 Introduction 18
2.2.2 PCDA Model 18
2.2.3 Management Review of ISMS 20
2.3 Identifying Non-Conformities to the ISMS 20
2.3.1 Corrective Action Plan 20
2.3.2 Preventative Action Plan 21
2.4 Corrective and Preventative Action Plans 21
2.4.1 Determining the Causes of Non-Conformities 21
2.4.2 Evaluating Actions Required 21
2.4.3 Implementing Mitigating Measures 22

3 DOCUMENT AND RECORDS MANAGEMENT 23
3.1 Introduction 23
3.1 ISMS Document Structure 23
3.2 Key Documents and Records 24

4 INFORMATION SECURITY RISK MANAGEMENT 25
4.1 Information Security Risk Management Objectives 25
4.2 Information Security Risk Management Approach 25
4.3 Measuring Information Security Risks 25
4.4 Risk Treatment Options 26
4.5 Monitoring POA Information Security Risks 26

5 INFORMATION SECURITY POLICY 27
5.1 Fujitsu Corporate Information Security Requirement 27

FUJ00232654

5.1.1 POA Information Security Policy 27
5.1.2 POA Information Security Policy Review 27

6 ORGANISING INFORMATION SECURITY 30

6.1 POA Information Security Organisation 30
6.1.1 Management Commitment to Information Security 30
6.1.2 Information Security Co-ordination 31
6.1.3 Allocation of Information Security Responsibilities 32
6.1.4 Authorisation Process for Information Processing Facilities 34
6.1.5 Confidentiality Agreements 36
6.1.6 Contact with Authorities 36
6.1.7 Contact with Special Interest Groups 36
6.1.8 Independent Review of Information Security 36
6.2 External Parties 37
6.2.1 Identification of Risks Relating to External Parties 37
6.2.2 Addressing Security when Dealing with Customers 37
6.2.3 Addressing Security in Third Party Agreements 37

7 ASSET MANAGEMENT 38

7.1 Responsibility for Assets 38
7.1.1 Inventory of Assets 38
7.1.2 Ownership of Assets 38
7.1.3 Acceptable Use Policy 38
7.2 Information Classification 39
7.2.1 Fujitsu / POL Classification Guidelines 39
7.2.2 Information Labelling and Handling 41

8 HUMAN RESOURCES 43

8.1 Prior to Employment 43
8.1.1 Roles and Responsibilities 43
8.1.2 Screening 43
8.1.3 Terms and Conditions of Employment 44
8.2 During Employment 45
8.2.1 Management Responsibilities 45
8.2.2 Information Security Education and Training 45
8.2.3 Disciplinary Process 45
8.3 Termination Responsibilities 46
8.3.1 Termination Responsibilities 46
8.3.2 Return of Assets 46
8.3.3 Removal of Access Rights 46

9 PHYSICAL AND ENVIRONMENTAL SECURITY 47

9.1 Secure Areas 47
9.1.1 Physical Security Perimeter 47
9.1.2 Physical Entry Controls 47
9.1.3 Securing Offices, Rooms and Facilities 47
9.1.4 Protecting Against External and Environmental Threats 48
9.1.5 Working in Secure Areas 48
9.1.6 Public Access, Delivery and Loading Areas 49
9.2 Equipment Security 50
9.2.1 Equipment Location and Protection 50
9.2.2 Supporting Utilities 50

FUJ00232654

9.2.3 Cabling Security....51
9.2.4 Equipment Maintenance....51
9.2.5 Security of Equipment Off-Premises....51
9.2.6 Secure Disposal or Re-use....52
9.2.7 Removal of Property....53

10 COMMUNICATIONS AND OPERATIONS MANAGEMENT....54

10.1 Operational Procedures and Responsibilities....54
10.1.1 Documented Operating Procedures....54
10.1.2 Change Management....54
10.1.3 Segregation of Duties....56
10.1.4 Separation of Development, Test and Operational Facilities....56
10.2 Third Party Service Delivery Management....56
10.2.1 Service Delivery....56
10.2.2 Monitoring and Review of Third Party Services....57
10.2.3 Managing Changes to Third Party Services....57
10.3 System Planning and Acceptance....58
10.3.1 Capacity Planning....58
10.3.2 System Acceptance....58
10.4 Protection against Malicious and Mobile Code....60
10.4.1 Controls against Malicious Software....60
10.4.2 Controls against Mobile Code....60
10.5 Backup....61
10.5.1 Information Backup....61
10.6 Network Security Management....62
10.6.1 Network Controls....62
10.6.2 Security of Network Services....62
10.7 Media Handling....62
10.7.1 Management of Removable Media....63
10.7.2 Disposal of Media....63
10.7.3 Information Handling Procedures....63
10.7.4 Security of System Documentation....63
10.8 Exchange of Information....65
10.8.1 Information Exchange Policies and Procedures....65
10.8.2 Exchange Agreements....65
10.8.3 Physical Media in Transit....65
10.8.4 Electronic Messaging....66
10.8.5 Business Information Systems....66
10.9 Electronic Commerce Services....67
10.9.1 Electronic Commerce Security....67
10.9.2 On-Line Transactions....67
10.9.3 Publicly Available Information....68
10.10 Monitoring....69
10.10.1 Audit Logging....69
10.10.2 Monitoring System Use....70
10.10.3 Protection of Log Information....71
10.10.4 Administrator and Operator Logs....71
10.10.5 Fault Logging....72
10.10.6 Clock Synchronisation....72

11 ACCESS CONTROL....73

11.1 Business Requirement for Access Control....73
11.1.1 Access Control Policy....73
11.2 User Access Management....75

FUJ00232654

11.2.1 User Registration....75
11.2.2 Privilege Management....75
11.2.3 User Password Management....76
11.2.4 Review of User Access Rights....76
11.3 User Responsibilities....77
11.3.1 Password Use....77
11.3.2 Unattended User Equipment....77
11.3.3 Clear Desk and Clear Screen Policy....77
11.4 Network Access Control....78
11.4.1 Policy on Use of Network Services....78
11.4.2 User Authentication for External Connections....78
11.4.3 Equipment Identification in Networks....79
11.4.4 Remote Diagnostic and Configuration Port Protection....79
11.4.5 Segregation in Networks....80
11.4.6 Network Connection Control....80
11.4.7 Network Routing Control....81
11.5 Operating System Access Control....82
11.5.1 Secure Log-on Procedures....82
11.5.2 User Identification and Authentication....82
11.5.3 Password Management System....82
11.5.4 Use of System Utilities....83
11.5.5 Session Time-out....83
11.5.6 Limitation of Connection Time....83
11.6 Application and Information Access Control....84
11.6.1 Information Access Restriction....84
11.6.2 Sensitive System Isolation....84
11.7 Mobile Computing and Teleworking....85
11.7.1 Mobile Computing and Communications....85
11.7.2 Teleworking....85

12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE....87

12.1 Security Requirements of Information Systems....87
12.1.1 Security Requirements Analysis and Specification....87
12.2 Correct Processing in Applications....89
12.2.1 Input Data Validation....89
12.2.2 Control of Internal Processing....89
12.2.3 Message Integrity....89
12.2.4 Output Data Validation....89
12.3 Cryptographic Controls....91
12.3.1 Policy on the Use of Cryptographic Controls....91
12.3.2 Key Management....91
12.4 Security of System Files....93
12.4.1 Control of Operational Software....93
12.4.2 Protection of System Test Data....93
12.4.3 Access Control to Program Source Code....93
12.5 Security in Development and Support Processes....94
12.5.1 Change Control Procedures....94
12.5.2 Technical Review of Applications after Operating System Changes....94
12.5.3 Restrictions on Changes to Software Packages....94
12.5.4 Information Leakage....95
12.5.5 Outsourced Software Development....96
12.6 Technical Vulnerability Management....97
12.6.1 Control of Technical Vulnerabilities....97

FUJ00232654

13 INFORMATION SECURITY INCIDENT MANAGEMENT 99

13.1 Reporting Information Security Events and Weaknesses 99
13.1.1 Reporting Information Security Incidents 99
13.1.2 Reporting Security Weaknesses 99
13.2 Management of Information Security Incidents and Improvements 100
13.2.1 Responsibilities and Procedures 100
13.2.2 Learning from Information Security Incidents 100
13.2.3 Collection of Evidence 100

14 BUSINESS CONTINUITY MANAGEMENT 102

14.1 Information Security aspects of Business Continuity 102
14.1.1 Including Information Security in the Business Continuity Management Process 102
14.1.2 Business Continuity and Information Security Risk Assessment 102
14.1.3 Developing and Implementing Continuity Plans including Information Security 102
14.1.4 Business Continuity Planning Framework 103
14.1.5 Testing, Maintaining and Re-assessing Business Continuity Plans 103

15 COMPLIANCE 105

15.1 Compliance with Legal Requirements 105
15.1.1 Identification of Applicable Legislation 105
15.1.2 Intellectual Property Rights (IPR) 106
15.1.3 Data Retention and Protection of Organisational Records 106
15.1.4 Data Protection and Privacy of Personal Data 106
15.1.5 Prevention of Misuse of Information Processing Facilities 106
15.1.6 Regulation of Cryptographic Controls 107
15.2 Compliance with Security Policies and Standards and Technical Compliance 108
15.2.1 Compliance with Security Policies and Standards 108
15.2.2 Technical Compliance Checking 108
15.3 Information Systems Audit Considerations 109
15.3.1 Information System Audit Controls 109
15.3.2 Protection of Information System Audit Tools 109

FUJ00232654

0.1 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - 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	21/12/2012	Approval version	
3.1	13/09/2013	Major Revision. This ISMS Manual is a change of approach and addresses the requirements of ISO/IEC 27001:2005 and is intended to capture how the POA is compliant.	
3.2	24/10/2013	Revised following review.	
4.0	29-Jan-2014	Approval version	

FUJ00232654

Review Details

Review Comments by :	
Review Comments to :	CISO, Information Security Risk and Assurance Manager
Mandatory Review	

Role	Name	Paragraphs
CISO	Brad Warren	All
Acting CISO	Tom Lillywhite	All
Delivery Executive	James Davidson	6.1.1, 6.1.3,
Security Operations Manager	Kumudu Amaratunga	4, 6.1.3, 8.1.3, 9.1.3, 9.1.5, 10.4.1, 10.6.2, 10.7.1, 10.10.1, 10.10.3, 10.10.4, 10.10.5, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.3.1, 11.3.2, 11.3.3, 11.4.1, 12.3.1, 12.3.2, 12.6.1, 13.1.1, 13.1.2, 13.2.1, 13.2.3, 15.1.6, 15.3.1, 15.3.2,
Quality and Compliance Manager	Bill Membery	3, 6.1.3, 6.1.8,
Security Architect	Dave Haywood	6.1.4, 10.6.1, 10.9.1, 10.9.2, 10.10.6, 11.4.2, 11.4.3, 11.4.3, 11.4.4, 11.4.5, 11.4.6, 11.4.7, 11.5.1, 11.5.2, 11.5.3, 11.5.4, 11.5.5, 11.5.6, 11.6.1, 11.6.2, 12.4.1, 12.4.2, 12.4.3, 12.5.2, 12.5.3, 12.5.4,
Commercial Manager	Sarah Guest	7.1.1, 7.1.2, 10.8.2, 15.1.1, 15.1.2, 15.1.3, 15.1.4
Service Implementation Manager	Ian Sinclair	9.2.6, 9.2.7, 10.7.2, 10.8.3
Document Manager	Matthew Lenton	10.1.1, 10.7.4,
Commercial Change Manager	Ken Westfield	10.1.2, 10.2.3, 12.5.1
HNG-X Test LST Test Manager	Mark Ascott	10.1.4, 12.4.2
Lead SDM - End User Services	Leighton Machin	10.2.1, 10.2.2
Network Infrastructure Manager	Andy Hemingway	10.2.1, 10.2.2
Systems Management & Global Cloud Manager	Catherine Obeng	10.2.1, 10.2.2
Service Manager	Gaby Reynolds	10.2.1, 10.2.2
Software Support Centre Manager	Steve Parker	10.3.1,
Service Governance Manager	Adam Bowe	10.3.2,
Software Development Manager	Nick Lawman	10.4.2, 12.2.1, 12.2.2, 12.2.3, 12.2.4, 12.5.5
Principal Technical Services Specialist	Edward Ashford	10.5.1
Tech Support Specialist	Niall Vincent	10.10.2

FUJ00232654

Business Continuity Manager	Sathish Ramalingam	14.1.1, 14.1.2, 14.1.3, 14.1.4, 14.1.5
Optional Reviewer		
Role	**Name**	**Paragraphs**
Security Operations Manager	Kumudu Amaratunga	All (other than those stated above)
Quality and Compliance Manager	Bill Membery	4, 7.1.1, 7.1.2, 7.1.3
Issued for Information – Please restrict this distribution list to a minimum		
Position/Role	Name	
POL	Via the ISMF.	

FUJ00232654

Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
ISO/IEC 27001:2005.	1.0	October 2005	Information Technology Techniques – Security Techniques – Information Security Management Systems – Requirements	BSI ISO/IEC
SVM/SEC/POL/0003			HNG-X Account Information Security Policy	Dimensions
NSN	2.0	8 May 2013	Fujitsu UK&I BMS Security Policy Manual.	Café Vik
CPM20	8.1	11 Apr 2011	Fujitsu Security Master Policy	Café Vik
CPM3	6.1	19 Jul 2011	Property and Physical Security	Café Vik
CPM6	7.4	21 Nov 2011	Legal Compliance	Café Vik
CPM21	3.4	21 Nov 2011	Intellectual Property	Café Vik
CPM27	2.11	17 Aug 2011	Risk Policy	Café Vik
CPM31	6.1	11 Apr 2011	Business Continuity	Café VIK
CPM36	2.2	8 Apr 2011	Data Protection	Café Vik
C-MP1.2	4.03	8 Aug 2011	Manage Risk Process (Fujitsu Eyes Only)	Café Vik
N/A	1.0	11 May 2011	Fujitsu Way Code of Conduct Global Business Standards	Café Vik
Group/Q&BE/08	4.2	24 Jul 2012	Control of Documents Policy	Café Vik
N/A	1.0	17 Jul 2009	(Fujitsu) Security Governance	Café Vik
SVM/SEC/PRO/0033			HNG-X Information Security Risk Management Procedure	
SVM/SEC/STD/0027			QMSR Terms of Reference	Dimensions
SVM/SEC/STD/0031	2.0	18 Feb 2009	Information Security Management Forum Terms of Reference	Dimensions
N/A	2.4	19 Jun 2013	Professionals Communities Policy	Café Vik
SVM/SEC/MAN/2220	0.4	13 Jun 2013	POA Security Roles and Responsibilities	Dimensions
SVM/SEC/STD/0026			POA CISO Terms of Reference	Dimensions
C-IDBM1.3	3.4	22 Oct 2012	Infrastructure Design and Build Methodology	Café Vik
NSN	1.0	1 Jun 2011	Fujitsu Conduct Policy	Café Vik
NSN	1.0	1 Mar 2011	Fujitsu Conduct Guidelines.	Café Vik
NSN	2.1	1 Aug 2012	Bullying, Harassment and Victimisation Policy	Café Vik

FUJ00232654

COM/MGT/REP/0001	6.3	20 Mar 2013	Transfer Asset Register	Dimensions
ITG-PO1	3.1	12 Jul 2013	Fujitsu UK & Ireland Business Operations, Information and Technology Group Internal IT Policy	Café Vik
SVM/SEC/STG/0739	1.0	31 May 2010	Security Communications Strategy	Dimensions
NSN	1.2	11 Feb 2013	Quick Reference Guide - Fujitsu UK & I – Information Classification Matrix.	Café Vik
FPVS v 3-1	3.1	12 Sep 2012	Explanatory Notes and Application Form: Fujitsu Personnel Vetting	Café Vik
NSN	2.2	1 Oct 2012	Fujitsu Welcome on Board (WoB) Process	Café Vik
GB/BSA/0002	2.0	16 May 2013	Group Security Site Audits Process	Café Vik
ISN001021	3.2	9 Jul 2009	Data Centres Site Access System: User Guide	Café Vik
ISN/001377			Physical and Environmental security of Data Centre environments	Café Vik
ITGSM-POL-0017	N/A	24 Jun 2013	Information and Technology Group Care of IT Equipment Policy	Café Vik
PGM/CM/PLA/0001			Configuration Plan for HNG-X	Dimension
PA/PER/033	8.3	7 May 2013	HNG-X Capacity Management and Business Volumes	Dimensions
SVM/SDM/PRO/0039	2.0	13 Jul 2012	Removal and or Destruction of Electronic Media	Dimensions
DES/SYM/HLD/0015	0.6	26 Nov 2010	HNG-X Backup and Recovery HLD	Dimension
SC002	7	17 Nov 2010	Manage Recycle Service	Café Vik
DEV/INF/LLD/0112	4.1	10 Mar 2011	HNG-X Test Services – LST Rig Low Level Design	Dimensions
DEV/INF/LLD/0032	4.14	28 May 2013	SV&I HNG-X Test Services Low Level Design	Dimensions
DEV/GEN/SPE/0007			HNG-X Platform Hardware Instance List	Dimensions
ARC/NET/ARC/0001			HNG-X Network Architecture	Dimensions
ARC/SEC/ARC/0003	3.0	12 May 2012	HNG-X Architecture – Security Architecture	Dimensions
ARC/SVS/ARC/0001	3.1	5 Apr 2012	Horizon (On-Line) Architecture – Support Service	Dimensions
ISN006654	1.0	19 Dec 2012	User Registration Management Procedure	Café Vik
NSN	0.2	6 Dec 2012	Account User Access Procedure	Café Vik

FUJ00232654

ITGSM-05	-	22 Feb 2013	Information and Technology Group Fujitsu Managed Mobile Service Security Policy	Café Vik
N/A			A Managers Guide to Home Based Working	Café Vik
CADBM1.2	4.0	26 Sep 2008	Fujitsu UK&I BMS ADBM Build and Unit Test	Café Vik
PGM/PAS/PRO/0002	6.0	1 May 2013	HNG-X Design & Build Methodology Requirements and Design Process	Dimensions
PGM/PAS/PRO/0003	5.0	1 May 2013	HNG-X Design & Build Methodology Code, Build and Component Test Process	Dimensions
DEV/GEN/TEM/0003	2.0	25 Jan 2013	HNG-X Generic Code Review Template	Dimensions
DEV/GEN/SPG/0023	4.6	17 May 2013	HNG-X Tool for Obfuscation of Counter/BAL-OSR Data: Support Guide	Dimensions
PO SMC 4LS GDC SoW	6.0	7 Sep 2012	Statement of Work Post Office Account Fourth Line Support & System Management Centre From the India GDC	Dimensions
I-IS1.1	2.1	25 Jan 2011	Fujitsu UK&I BMS Security Incident Process	Café Vik
DES/APP/HLD/0029			Audit Data Retrieval High Level Design	Dimensions
CPM31	8.0	12 July 2013	Fujitsu UK&I BMS Business Continuity Master Policy	Cafe Vik
I-AB 1.9	1.1	14 Jan 2011	Manage Continuity of Fujitsu UK & Ireland Business Process	Café Vik
SVM/SDM/PLA/0003	1.0	4 Mar 2009	HNG-X Business Continuity Test Plan	Dimensions
NSN			Business Continuity Test Schedule Planner	
PGM/PAS/MAN/0004	4.0	20 Jun 2012	Quality and Compliance Framework	Dimensions
Group/Q&BE/03	7.0	21 Feb 2013	Documentation and Record Standards	Café Vik

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

FUJ00232654

Abbreviations

Abbreviation	Definition
AD	Active Directory
ALM	Application Lifecycle Management
ARQ	Audit Record Queries
API	Application Programming Interface
BAL	Branch Access Layer
BAU	Business as Usual
BMS	Business Management System
DPA	Data Protection Act
CBT	Computer Based Training
CCB	Change Control Board
CCD	Contract Controlled Document
CISO	Chief Information Security Officer
COTS	Commercial Off the Shelf
CP	Change Proposal
CR	Change Request
CSLC	Customer Solution Lifecycle
CT	Commercial Terms
DAB	Design Approval Board
GDC	Global Delivery Centre
GRN	Goods Return Note
HLD	High Level Design
HNGxDBM	HNG-X Design & Build Methodology
HR	Human Resources
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IDBM	Infrastructure Design and Build Methodology
IDS	Intrusion Detection Systems
IPR	Intellectual Property Rights
ISAE	International Standard of Assurance Engagements
ISBR	Information Security Review Board
ISMS	Information Security Management System

FUJ00232654

ISMF	Information Security Management Forum
KSS	Key Services
KSC	Key Service Client
LAN	Local Area Network
LST	Live System Test (LST)
LLD	Low Level Design
MSC	Managed Service Change
NPS	Network Persistence Store.
NTP	Network Time Protocol
OLA	Operational Level Agreement
OSM	Operations Security Manager
OSR	Online Service Router
PAM	Pluggable Authentication Module
PAN	Primary Account Number
PCCB	Programme Change Control Board
PCDA	Plan, Do, Check, Act
PCI-DSS	Payment Card Industry – Data Security Standards
PDC	Primary Domain Controller
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POA	Post Office Account
POL	Post Office Limited
POLMI	Post Office Limited Management Information System
POMS	Post Office Managed Switch
QMSR	Quality Management and Security Review Board
RDP	Remote Desktop Protocol
RWP	Request for Work Package
RPO	Recovery Point Objective
RTO	Return to Operation
SoA	Statement of Applicability
SLA	Service Level Agreement
SLS	Supply and Lifecycle Services
SMC	Systems Management & Global Cloud
SOP	Standard Operating Procedure
SoW	Statement of Work

FUJ00232654

SPG	Support Guide
SSIP	Security Services Improvement Programme
SSL	Secure Sockets Layer
SV&I	Systems Validation and Integrity
TEM	Tivoli Event Management
TNT	Thomas Nationwide Transport
TK	Traffic Keys
UPS	Uninterruptible Power Supplies
WAN	Wide Area Network
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
4LS	4th Line Support

FUJ00232654

Glossary

Term	Definition
Cardholder Data	PCI-DSS Term defined as the PAN or the PAN plus any of the following: • Cardholder Name • Expiration Date • Service Code • Start Date • Issue Number;
PCI-DSS	A set of security controls defined by the Payment Card Industry organisation.

Changes Expected

Changes
This is a major revision and changes are expected following peer review.

FUJ00232654

1 Introduction and Scope

1.1 ISMS Manual Overview

This Information Security Management System (ISMS) Manual supports the Fujitsu Post Office Account Information Security Policy in describing the overall strategy for providing Information Security and is based upon security practice as defined by ISO/IEC 27001:2005.

It should be noted that achieving ISO/IEC 27001:2005 certification or indeed Compliance is not a contractual deliverable but as both Post Office Limited (POL) and Fujitsu recognise the benefits that adherence to the Standard brings the overarching principles will underpin the Fujitsu Post Office Account Information Security approach.

Section 5 of this document sets out the Executive Information Security Policy Statement for the Post Office Account which, together with the Framework of Controls in sections 6 to 15 satisfy the Contractual requirements.

1.2 Scope

1.2.1 Statement of Scope

This ISMS covers activities undertaken by the Account in the provision of contracted services to POL including design, development, deployment, operation and support of services, as well as the programme management, stakeholder management, governance and administrative procedures applied by executive management to oversee those services.

This ISMS Manual document describes the overall strategy for providing Information Security and is based upon best practice as defined by ISO/IEC27001:2005.

The actual scope of the Services provided to POL, and which is addressed in complying with ISO27001:2005, covers the operation and maintenance of the Post Office Account (POA) on-shore and off-shore services.

The scope also incorporates the assets of the service provided by Fujitsu; especially in regards to the secure acquisition, handling, processing, storage, transmission and communication of POL Transaction and Client Data, Personal Identifiable Information, POL Financial Information, POA and POL Management Information, Audit Data and Operational Data.

1.2.2 Exclusions

Information security risks within POL and their agents' sites that are outside of the scope of the Services provided by the Account are excluded from the scope of the POA ISMS.

Services provided by Fujitsu's Global Delivery Centre (GDC) are mentioned within this ISMS Manual but it should be recognised that GDC hold independent ISO/IEC 27001:2005 Certification. This is accepted by the POA and their local implementation is not further expanded upon.

1.2.3 Statement of Applicability

The POA shall implement and maintain a Statement of Applicability which will capture the Controls in place to support the ISMS. It shall also specifically state what ISO/IEC 27001:2005 Controls are out of scope and include a justification for their exclusion.

FUJ00232654

2 Information Security Management

2.1 Information Security Definition

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, an associated document suite - the Information Security Management System (ISMS) has been created to provide for a systematic approach to managing sensitive company information so that it remains secure. It also encompasses people, processes and IT systems.

2.2 ISMS Operating Procedures

2.2.1 Introduction

ISMS Operating Procedures are written descriptions of the management processes and activities necessary to plan operate and control the ISMS.

2.2.2 PCDA Model

The POA HNG-X Account adopts the Plan, Do, Check, Act (PDCA) process approach for Information Security management as presented in ISO/IEC 27001:2005 which promotes:

- Understanding an organization's Information Security requirements and the need to establish policy and objectives for Information Security.
- Implementing and operating controls to manage an organization's Information Security risks in the context of the organization's overall business risks.
- Monitoring and reviewing the performance and effectiveness of the ISMS.
- Continual improvement based on objective measurement.

2.2.2.1 Plan

FUJ00232654

The cyclic Information Security lifecycle offers reoccurring opportunities for continuous improvements to the ISMS. New opportunities for improvement to reduce a new or previously identified risk can come from a variety of sources including, but not limited to,

- Audit findings
- Information Security reviews
- Information Security incidents
- Change in industry best practise advice
- Technology change
- Environment change

When the requirement for a new or a significant change to existing, policy / process / procedure etc is identified an Information Security Risk may be added to the Information Security Risk Register to identify the level of risk that the POA and / or POL is exposed to.

The QMSR and / or the ISMF shall be the forums for any proposed changes:

- To the Information Security Management System that may have an impact on the Confidentiality, Integrity or Availability of the Services or POL data.
- To the documentation within the ISMS Framework.

2.2.2.2 Do

On appropriate approval the CISO is to instigate the implementation of the Controls as identified in the Risk Treatment Plan.

The CISO is to determine the most appropriate mechanism to communicate the Control change to all members of staff. Options to be considered include, but are not limited to,

- Email bulletin
- Sharepoint
- Notice Boards
- Workshops
- Internal training sessions
- Other (as identified)

2.2.2.3 Check

Whilst it is expected that all Information Security Controls will be monitored and reviewed, particular attention should be given to newly introduced Controls to assess whether they are performing as intended in reducing Information Security risk levels.

The POA is also subject to a variety of external and internal Fujitsu Audits and therefore a specific Account internal Information Security audit programme is considered to be superfluous as it is anticipated that all requirements will be met in customer / internal Fujitsu driven activities.

2.2.2.4 Act

The Statement of Applicability is to be adjusted accordingly and the document management control updated.

FUJ00232654

The ISMS change is to be formally communicated to all staff and all interested parties with an appropriate level detail according to each circumstance.

All lessons learnt shall be captured and any improvement principles that can be applied to any other preventative or corrective actions should be extended across the ISMS.

2.2.3 Management Review of ISMS

The CISO shall ensure that the ISMS is reviewed at planned intervals (at least annually to ensure its continuing suitability, adequacy and effectiveness.

This review shall include assessing opportunities for improvement and the need for changes to the ISMS, including the Information Security policy and Information Security objectives.

2.2.3.1 Review Inputs

The review shall consider

- Results of ISMS Audits (External and Internal)
- Major Information Security Incidents
- Status of Information Security Risk Register
- Feedback (both Internal and External)
- Changes that could impact the ISMS

2.2.3.2 Review Outputs

The review shall produce

- ISMS Improvement Recommendations (SSIP opportunities)
- Updates to the Risk Assessment and Risk Treatment Plans
- Modifications of Processes and Procedures
- Endorsement of current Resource Needs
- Improvements to ISMS Effectiveness Measuring

2.3 Identifying Non-Conformities to the ISMS

Whilst desirable, it is unreasonable to assume that the ISMS will function completely smoothly without any need to adjust any of the controls implemented.

How non-conformities to the ISMS are discovered will determine whether the Corrective or Preventative Action Plan is followed.

However, in practice once the non-conformity has been identified the same model is used for both Corrective and Preventative Plans thereafter

2.3.1 Corrective Action Plan

The Corrective Action Plan should be initiated when non-conformity is identified as the result of an activity that has occurred.

Nonconformities can be identified through a number of avenues including

FUJ00232654

- Information Security Incidents
- Monitoring and Alerting
- Internal and Independent Audit Reports

2.3.2 Preventative Action Plan

The Preventative Action Plan should be initiated when non-conformity is identified as the result of an activity that has either not occurred or has not been previously reported as an Information Security Incident.

Potential nonconformities can be identified through a number of avenues including

- Management Reviews of the ISMS
- Internal and Independent Audit Reports
- Monitoring and Alerting
- Reporting of Information Security Weaknesses

2.4 Corrective and Preventative Action Plans

2.4.1 Determining the Causes of Non-Conformities

2.4.1.1 Technical Non-Conformities

The CISO shall liaise with appropriate technical specialists to identify the root cause of any technical non-conformity.

2.4.1.2 Non-Technical Non-Conformities

The CISO shall engage will appropriate business representatives to identify the root cause of any non-technical non-conformity.

2.4.2 Evaluating Actions Required

The CISO shall instigate a risk assessment to determine likelihood and impact and resulting severity and priority of the non-conformance(s).

The results of the risk assessment shall be presented to the Quarterly Quality Management and Security Review Board (QMSR).

Potentially the results may also be shared with POL at the Information Security Management Forum (ISMF).

2.4.2.1 Immediate Actions

The CISO is to liaise with the Account Commercial Manager to determine whether the identified non-conformity constitutes a breach of Contract.

Any non-conformity that constitutes a breach of Contract is to be addressed with the highest priority and captured in the Information Security Risk Register.

FUJ00232654

Should any additional resource be required the CISO is to consider presenting mitigating proposals at an appropriate POA Change Board.

2.4.2.2 Longer Term Remediation

An entry shall be made in the Information Security Risk Register and managed according the combined likelihood and impact scores as defined by the Information Security Risk Management Methodology. Additionally, ISMS non-conformities may be considered as a candidate for remediation through the SSIP.

Where remediation of the non-conformity falls outside the Contractual boundaries then the CISO shall present any recommendations for POL to consider as a Project.

2.4.3 Implementing Mitigating Measures

Any adjustment to mitigating security controls must be approved at an appropriate managerial level proportional to the level of change required.

FUJ00232654

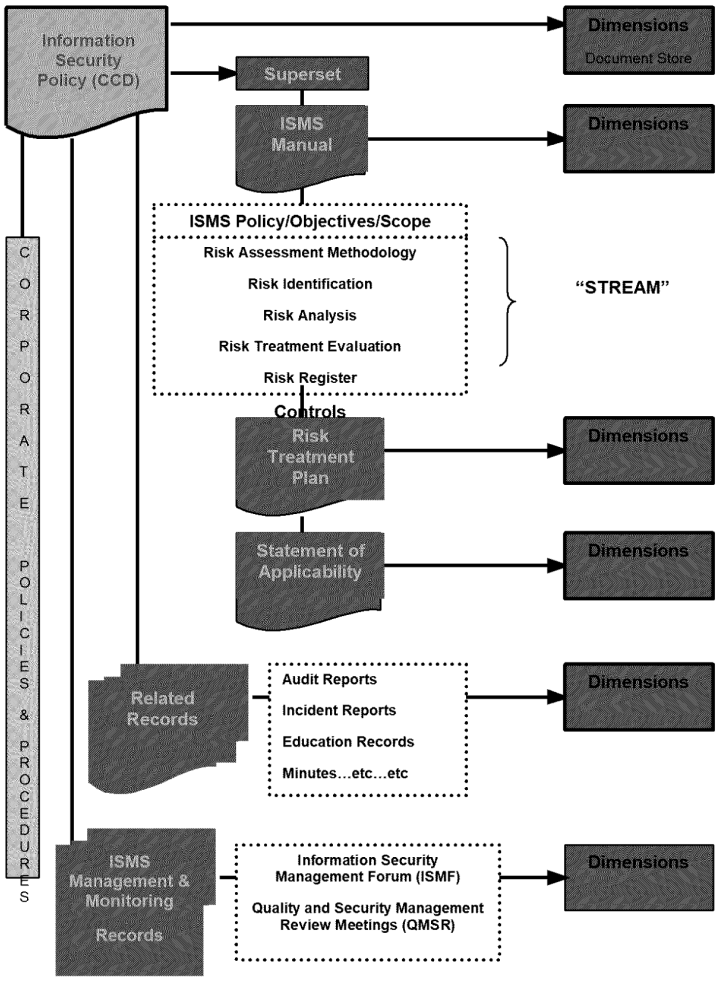
3 Document and Records Management

3.1 Introduction

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.

3.1 ISMS Document Structure



FUJ00232654

3.2 Key Documents and Records

The following key documents support the ISMS:

Document Description	Location	Retention
POA Information Security Policy	Dimensions	Life of the ISMS
ISMS Manual (this document)	Dimensions	Life of the ISMS
Statement of Applicability	Dimensions	Life of the ISMS
Information Security Management Forum/Board TOR's	Dimensions	Life of the ISMS
QMSR/ISMF Minutes	Share	Life of the ISMS
Information Security Risk Registers	Standalone	Life of the ISMS
Risk Treatment Plans	Share	Life of the ISMS
Integrated Audit Plan	Dimensions	Current year +1
Audit Reports	Dimensions	7 years
Reports of Security Incidents	Share	7 years
Information Security Monthly Report	Share	Life of the ISMS

FUJ00232654

4 Information Security Risk Management

4.1 Information Security Risk Management Objectives

The objectives of effective Information Security Risk Management are:

- Identify, implement and manage security related controls for the Service provided to the Fujitsu Services Post Office Account (POA) and POL.
- To facilitate the overall management of Information Security risk relating to Information, People, including Property, Documentation, Technology and Infrastructure within the Service provided by POA.
- To provide appropriate management information in relation to Information Security Risk and ensure that this is co-ordinated with the POA Business Risk management process and POL.

4.2 Information Security Risk Management Approach

Information Security Risks must be managed in accordance with the ISO/IEC 27001:2005, LINK ASSIS, PCI DSS Standards, as per contractually agreed version, and the Fujitsu Services Corporate Manage Risk Process as documented in the HNG-X Information Security Risk Management Procedure (Ref:- SVM/SEC/PRO/0033).

The POA Information Security Risk Management approach is not a blanket risk assessment activity but a more responsive, planned or reactive technique for making business decisions around risk and business or technical controls, on an as-needs and timely basis.

The POA will assess these risks to identify whether there are potential threats which could be exposed by a vulnerability that, if exploited, could have an adverse impact on the POA or POL.

An entry into the Information Security Risk Register shall be seen as evidence that the Information Security Risk Assessment process has been applied.

The Fujitsu Services Post Office Account will implement and maintain Information Security Risk Registers which shall be the repository for Information Security Risks.

4.3 Measuring Information Security Risks

The measuring of Information Security Risk can be subjective and may therefore require some collaboration to determine the Impact any risk may have on POL and the Likelihood of the risk happening.

Although measured separately it the combination of Likelihood and Impact that determines the level of risk posed.

Measuring Information Security Risk is an ongoing activity and should be re-assessed after mitigating Controls have been implemented and periodically to validate the Information Security Risk exposure.

FUJ00232654

4.4 Risk Treatment Options

There are several options available when considering identified Information Security Risks. The chosen option (or mix of management techniques) will depend on the nature and level of the risk.

The key options are:

Risk Tolerance	For low-frequency, low-impact risks, where the cost of control is greater than the potential risk, the ISMF may choose to accept such risks.
Risk Termination	Where an activity generates an Information Security Risk, and there is the option to cease the particular activity or to conduct the process in a different way, then the QMSR / ISMF may choose to do so in order to avoid the risk concerned.
Risk Treatment	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.

4.5 Monitoring POA Information Security Risks

Fujitsu shall appoint an Information Security Risk Manager who shall report directly to the CISO and shall be Fujitsu's representative at the ISMF.

The Information Security Risk Manager shall maintain the Information Security Risk Register and liaise with Risk Owners on the progress of Risk entries and provide summary updates to the ISMF as required.

FUJ00232654

5 Information Security Policy

5.1 Fujitsu Corporate Information Security Requirement

The Post Office Account is to be compliant to the Fujitsu UK&I BMS Security Master Policy (Ref:- CPM20) as the policy is applicable to all Employees, Contractors and businesses carried on by Fujitsu Services Limited and its subsidiaries and any other company or organisation (including working partners operating or carrying out work on Fujitsu UK & Ireland sites or elsewhere on behalf of Fujitsu UK & Ireland) that is managed by the Chief Executive Officer, Fujitsu United Kingdom and Ireland.

Failure to comply with this Policy, the Fujitsu UK&I BMS Security Policy Manual, or any subsidiary policies and procedures or to neglect personal security responsibilities as laid down in the Global Business Group Global Business Standards may lead to disciplinary action.

Further guidance to managing Information Security is provided in the Fujitsu Manage Information Security Policy (Ref:- C-MSv1.10).

5.1.1 POA Information Security Policy

The Post Office HNG-X Account Information Security Policy (Ref:- SVM/SEC/POL/0003) captures the Executive Information Security Policy Statement, management direction and support for Information Security, along with the minimum standards to be met by the Post Office Account.

It is consistent with Contractual and Regulatory commitments and relevant POL Information Security Requirements as expressed in their Information Security policies and overarching applicable principles of ISO/IEC27001:2005.

5.1.1.1 Communication

The Information Security Policy Owner shall ensure that all changes to the Post Office HNG-X Account Information Security Policy, POA ISMS Manual and supporting documentation is communicated across the entire Fujitsu Post Office Account and that the reviewed document replaces the previous one so that there is only one document in circulation.

5.1.2 POA Information Security Policy Review

The Post Office HNG-X Account Information Security Policy is owned by the Fujitsu Post Office Account Chief Information Security Officer (CISO) who is responsible for its maintenance and review.

The Post Office HNG-X Account Information Security Policy will be formally reviewed at least annually, after major changes to the scope of services and after any significant security incident or occurrence.

The policy will be also be updated whenever necessary to reflect the needs and obligations of the Fujitsu Post Office Account and developments in relevant best practice.

The annual review will include a review of effectiveness, impact of the policy on the business and the effect of technology changes on the policy.

5.1.2.1 Review Timings - Scheduled Annual Review

FUJ00232654

At a period no later than eleven calendar months from the previous approval date the CISO is to initiate a review of the Post Office HNG-X Account Information Security.

It should be noted that some Policy and Procedural documents referenced from the Post Office HNG-X Account Information Security Policy are owned and maintained at a corporate level and their maintenance is outside the influence of the Account Security Management Team.

The Account Security Management Team will request that these be updated but no guarantees can be given.

5.1.2.2 Review Timings - Unscheduled Annual Review

On notification of a major Information Security incident or significant change affecting the ISMS the CISO is to initiate a targeted review of the relevant Information Security Documentation as soon as reasonably practical, typically within 20 working days.

Note:- An unscheduled review of individual Information Security Documentation does not replace the annual review cycle requirement as not all areas of the Information Security Documentation will be reviewed.

5.1.2.3 Review Scope - Scheduled Annual Review

The annual Information Security Policy review shall encompass the Post Office HNG-X Account Information Security Policy and POA ISMS Manual.

Consideration must be given to any Account specific documentation referenced from either the Post Office HNG-X Account Information Security Policy or POA ISMS Manual

5.1.2.4 Review Scope - Unscheduled Annual Review

Any ad-hoc Information Security Documentation review initiated by a major Information Security Incident or significant change shall only address those segments of the Information Security Policy, ISMS Manual or supporting procedures and / or work instructions that the major Information Security incident or significant change affects.

5.1.2.5 Conducting the Review - Scheduled Annual Review

The CISO shall engage the services of all relevant business areas in reviewing the continuing suitability, adequacy, and effectiveness of the Information Security Policy, the ISMS Manual and all supporting procedures and work instructions and capture any changes within 15 working days.

5.1.2.6 Conducting the Review - Unscheduled Annual Review

The CISO shall engage the services of business areas impacted by the major Information Security incident or significant change in reviewing the continuing suitability, adequacy, and effectiveness of the Information Security Policy, ISMS Manual or supporting procedures and capture any changes within 20 working days.

5.1.2.7 Documentation

All alterations to the Information Security Policy, ISMS Manual or supporting procedures and / or work instructions shall be captured by version control within the document history.

FUJ00232654

The CISO is responsible for presenting the reviewed Information Security Policy, ISMS Manual or supporting procedures and / or work instructions to the Delivery Executive, or a nominated representative, for management approval.

5.1.2.8 Senior Management Approval

The Delivery Executive or a nominated representative shall approve the Post Office HNG-X Account Information Security Policy prior to the annual renewal date.

5.1.2.9 Senior Management Non-Approval

The Delivery Executive or a nominated representative shall identify and communicate to document owners any non-approval issues prior to the annual renewal date.

5.1.2.10 Senior Management Non-Approval – CISO's Action

Document owners should agree a corrective course of action, with agreeable timescales, with the Delivery Executive or a nominated representative.

FUJ00232654

6 Organising Information Security

6.1 POA Information Security Organisation

6.1.1 Management Commitment to Information Security

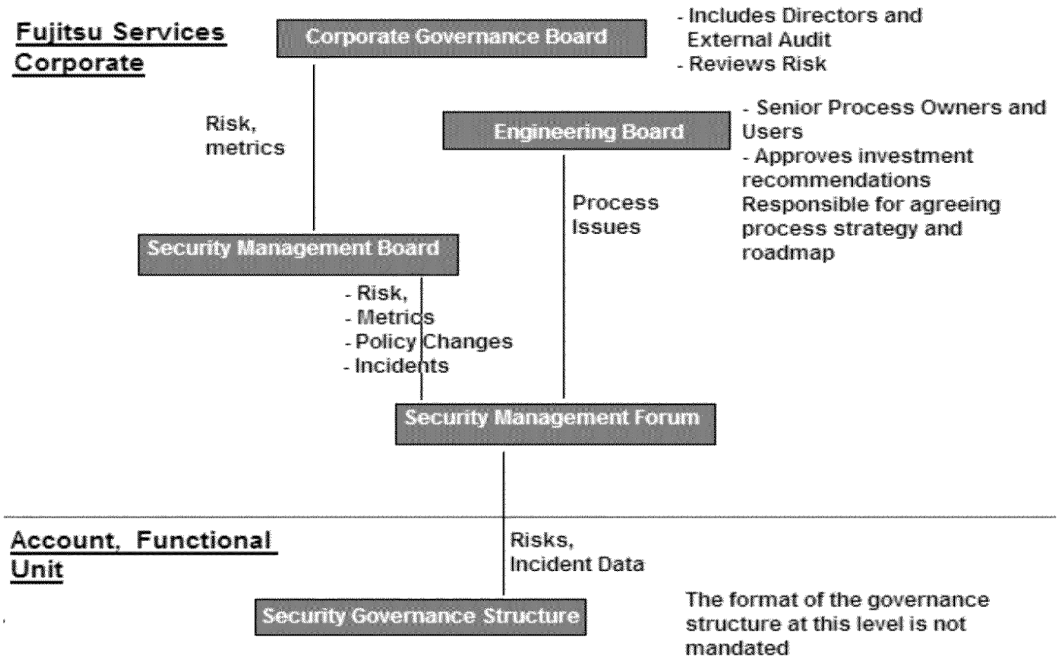
Senior Management commitment to Information Security is demonstrated on Fujitsu's Post Office Account by the Delivery Executive having approved the Information Security Policy and by giving delegated authority of Information Security implementation to the CISO.

6.1.1.1 Fujitsu's Corporate Security Governance Framework

Ensuring effective management of business risk is the responsibility of the Corporate Governance Board, made up of directors and external audit.

The Security Management Board is responsible for overseeing the strategy for mitigating security risk and reporting that this is being carried out to the Corporate Governance Board. It approves Security Policy and mandates this to all areas of the business. It receives details of risks and incidents from the Security Management Forum as well as reports from external sources.

The Security Management Forum is responsible for recommending changes to security policy and process, based on changes to business circumstances and a review of incidents and risks submitted by businesses. Process changes are communicated to the Engineering Board to ensure they are compatible with other processes.



FUJ00232654

6.1.1.2 Fujitsu Post Office Account Security Governance

Information Security is an inherent part of, and is seen as a core responsibility of, the Fujitsu Post Office Account. Executive sponsorship ensures that the Account:

- Allocates sufficient expert resource to address its Information Security obligations;
- Participates fully in customer meetings and workshops responsible for information exchange, the advancement of best practice definition and communication;
- Takes steps to ensure that all of its services are delivered from a standpoint of compliance with this Policy, through endorsement by executive management and a culture of intolerance of non-adherence.
- Will communicate this commitment throughout the Account and to any sub-contractors. This will be reinforced through a training and awareness process for all Post Office Account staff.

6.1.1.3 Post Office Account Organisation Chart

The Post Office Account Management and Security Organisation charts are found at:

Post Office Account Organisation Chart

6.1.1.4 Post Office Account Security Team Organisation Chart

The POA Security Team Organisation Chart can be found on Page 7 at

http://sites.cafevik.fs.fujitsu.com/sites/00672/RMGA%20Org%20Charts/Post%20Office%20Account%20Organisation.pdf

6.1.2 Information Security Co-ordination

6.1.2.1 Quarterly Quality Management and Security Review Board (QMSR)

There is a POA Quality Management and Security Review Board (QMSR) which meets quarterly and is chaired by the Delivery Executive. Membership and governance of the QMSR is detailed in the QMSR Terms of Reference (Ref:- SVM/SEC/STD/0027).

6.1.2.2 Information Security Management Forum (ISMF)

The Post Office Account and POL sends appropriate representation to the monthly Information Security Management Forum (ISMF) which operates in accordance with terms of reference (Ref:- SVM/SEC/STD/0031) agreed between both parties

FUJ00232654

6.1.3 Allocation of Information Security Responsibilities

The POA Security Roles and Responsibilities (Ref:-SVM/SEC/MAN/2220) fully defines security roles and responsibilities and is summarised below.

6.1.3.1 Fujitsu Service Post Office Account Delivery Executive

The POA Delivery Executive has ultimate responsibility for security, with the responsibility for policy and the general direction of Information Security delegated to the CISO.

The Information Security related responsibilities of the POA Delivery Executive include:

- Overall control and management of Information Security throughout the POA.
- Provision of adequate resources for Information Security and appointing an experienced security professional responsible for managing and coordinating Information Security across the complete POA domain.
- Approval authority for the POA Information Security Policy.
- Ownership and overall control and management of Operational Security throughout POA.
- Overall control of Information Security Risk Management and Audit functions.
- Chairing the POA Quarterly Quality Management and Security Review Board;

Senior management is supported by the POA Security Team which consists of experienced specialists with specific expertise in the areas of IT security and Information Security Risk Management.

6.1.3.2 POA Chief Information Security Officer (CISO)

The CISO is responsible for the overall design of POA's Information Security control framework and the responsibilities of the POA CISO are documented in Terms of Reference (Ref:-SVM/SEC/STD/0026) and summarised as:-

- Leads the engagement with customer stakeholders with an interest in governance, control and Information Security matters.
- Providing a point of contact for POL Head of Information Security.
- Developing and publishing all Information Security related policies and procedures applicable at POA level.
- Co-ordinating the implementation and operation of the ISMS.
- Reviewing the Post Office HNG-X Account Information Security Policy and approving supporting Information Security procedures owned and implemented at business level.
- Monitoring for compliance with the POA HNG-X Account Information Security Policy.
- Ensuring that Information Security incidents and events are recorded and investigated.
- Ensuring that system audit trails are analysed on a regular basis.
- Defining the Information Security Risk Management methodology of POA.
- Analysis and evaluation of Information Security risks and evaluating options for the treatment of risks.

FUJ00232654

- Ensuring all POA Staff are screened in line with Contractual requirements and Fujitsu Services Group Policy.

6.1.3.3 POA Operations Security Manager (OSM)

The Responsibilities of the Operations Security Manager include:

- The management of Information Security incidents
- The provision and oversight of event auditing services
- Management of the Patching and Associated Anti-Virus Service (including chairing the Patch Approval Board
- Impact assessment, authorisation and approval for all operational and system design changes to ensure the implementation of security controls in technology and processes.
- Co-ordinating the evaluation of all new security products proposed.
- Providing regular Information Security operational reporting on activities and status.

6.1.3.4 POA Information Security Risk and Compliance Manager

The Information Security Risk and Compliance Manager is responsible for the day-to-day Information Security Risk Management and documentation of the ISMS. The responsibilities of the POA Information Security Risk and Compliance include:

- Maintaining the Information Security Risk Register
- Production and maintenance of the HNG-X Information Security Policy
- Production and maintenance of the HNG-X ISMS Manual
- Co-ordination of ISMS supporting documentation.
- Maintenance of the Statement of Applicability.

6.1.3.5 POA Quality and Compliance Manager

The Information Security related responsibilities of the POA Quality Manager include:

- Ensuring Compliance to all POL and Fujitsu Compliance requirements.
- Co-ordinating all audit related activities.
- Providing a point of contact for external audit personnel.
- Planning and carrying out audits of POA's business functions.
- Maintaining an integrated audit plan.

6.1.3.6 Physical Security

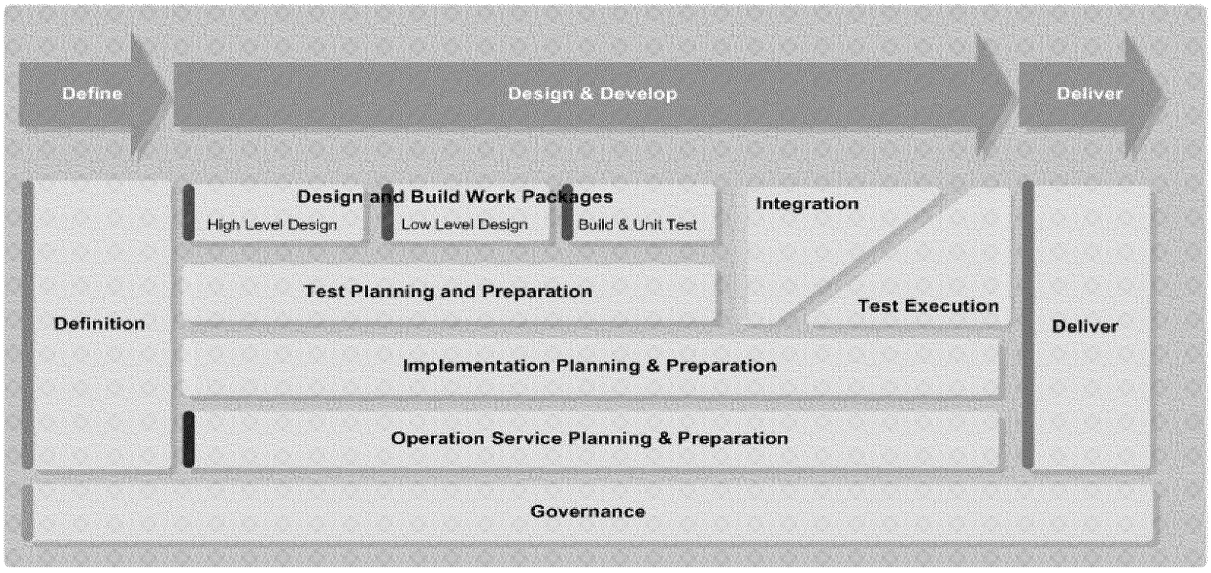
Group Property and Group Security have responsibility for physical security at all sites used by the Post Office Account.

FUJ00232654

6.1.4 Authorisation Process for Information Processing Facilities

The Infrastructure Design and Build Methodology (Ref: C-IDBM1.3) is the standard lifecycle model used within Fujitsu Services for all Infrastructure Design and Build projects.

It is made up of the following core processes, summarised and portrayed in the diagram below.



6.1.4.1 Definition

This process deals with the gathering of requirements from all stakeholders, identification of the existing environment into which the new infrastructure must integrate, and identification of the new technical solution. This will normally be part of a general requirements gathering activity, and the infrastructure requirements may only be a subset of the overall requirements.

During this stage, the designer will normally need to provide technical information to the project team to allow them to produce overview project plans and allocate resources.

Key output from this process is the Requirements Traceability Matrix (RTM) which provides information on where requirements are being covered, information on the requirements, and the overall design. Initial information on the risks, issues, assumptions and dependencies is also passed to the project managers at this stage, including technical information on the logical order of tasks, what might make suitable work packages etc.

6.1.4.2 Design and Build Work Packages

This process takes the requirements, and turns them into a high level design, then a low level design, and eventually into build instructions and the initial component builds. The list of items needed is also generated during this process.

This is often considered the main part of the design process, but it cannot be successful in isolation. Key outputs from this process are the High Level Design, Low Level Design, Bill of Materials, build instructions, and associated automation for the builds.

FUJ00232654

6.1.4.3 Implementation Planning and Preparation

This process runs in parallel with the Design & Build process. During this phase, the designer helps the project manager identify the work required to implement the infrastructure, and realisable proportions for work package planning.

These steps, from planning the strategy down to more detailed planning, inform project management planning.

6.1.4.4 Test Planning and Preparation

This process defines the activities required to plan and prepare for the verification and validation of a deliverable.

6.1.4.5 Integration

This process takes individual components and assembles them together to form increasingly larger components.

This process works closely with the Test Execution process, as each completed set of components is built, they should be tested, until the solution can be tested as a whole.

6.1.4.6 Test Execution

This process defines the testing activities used to verify and validate a deliverable to ensure that customer requirements are satisfied.

The main testing activities occur within the Integrate & Test phase; however, an important test activity – build/unit testing is carried out as work-packages or modules are developed and built

6.1.4.7 Operational Service Planning and Preparation

This process ensures that the infrastructure solution can be supported once it is operational. This will include planning for resources, skills and training, and ensuring that support staff have the tools, information and access to provide effective support.

6.1.4.8 Delivery

This process is concerned with the final stages of the project, such as final builds, and deployment into the live environment, followed by the handover to operational support.

6.1.4.9 Governance

This process is concerned with ensuring that the other IDBM processes work. This includes the IDBM gateways, which check that the IDBM processes are being run correctly.

It also describes how designs should be peer reviewed and approved, and how change should be handled.

Further information is contained at http://portals.cafevik.fs.fujitsu.com/00135/Pages/Home.aspx

FUJ00232654

6.1.5 Confidentiality Agreements

All employment contracts (permanent and temporary) as well as consultant, contractor and supplier contracts (Generic Supplier Contract Template) include clauses governing the treatment of Customer (in this case POL) information gained as a result of their employment.

Fujitsu staff on the Post Office Account must be aware of their obligations set out in Paragraph 2.6.3 of Schedule A4, Legislation, Policies and Standards. For clarity Paragraph 2.6.3 is reproduced below:-

"Fujitsu Services shall not disclose any Personal Data to any person except to such of its employees, agents, sub-contractors, third parties performing software maintenance or support and consultants in each case who require that information in order for Fujitsu Services to perform its obligations under this Agreement.

Prior to disclosing Personal Data or any portion thereof to such employees, agents, sub-contractors, third parties or consultants, Fujitsu Services shall ensure the relevant employee, agent, sub-contractor, third party or consultant is subject to a written contract with Fujitsu Services requiring them to comply with Fujitsu Services' obligations herein regarding the security and confidentiality of the Personal Data and to comply with Fujitsu Services' instructions in processing it.

Fujitsu Services shall not knowingly cause or allow an employee, agent, sub-contractor, third party performing software maintenance or support or consultant to process Personal Data in a way that Fujitsu Services would not itself be entitled to process it under this Agreement."

6.1.6 Contact with Authorities

Co-operation with external organisations is through established Fujitsu Corporate channels.

- Contact with law enforcement authorities, government vetting agencies and Centre for the Protection of National Infrastructure will be maintained by Fujitsu Group Security.
- Contact with regulatory bodies and the Information Commissioner will be maintained by Fujitsu Group Legal.

6.1.7 Contact with Special Interest Groups

General contact with special interest security groups and best practice security organisations will be maintained by the Post Office Account Security Team but only via voluntary, individual membership of such groups and any value added provided by Fujitsu individual membership shall be viewed as a benefit to POL.

6.1.8 Independent Review of Information Security

All areas of Information Security are subject to regular independent reviews. As documented in the POA Audit High Level Plan these include:

- ISAE3402 – Annual external audit conducted by Ernst & Young to support POL Financial Reporting.
- PCI –DSS – Annual requirement from POL who own and manage the audit.
- ISO/IEC 27001:2005 - Annual POA Accreditation which is part of Fujitsu Certification and own by the CISO.
- LINK Audit – Annual audit conducted by POL external auditor.

FUJ00232654

6.2 External Parties

6.2.1 Identification of Risks Relating to External Parties

The risks associated with access to POA information and information processing facilities by third parties will be assessed and appropriate security controls implemented in line with HNG-X Information Security Risk Management Procedure (Ref:- SVM/SEC/PRO/0033).

These controls must be agreed, documented and defined in agreements with any external parties.

Physical access to any POA processing facilities provided by Fujitsu shall not be provided to third parties until all security requirements have been satisfied and evidence recorded.

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

6.2.1.1 3rd Party Connectivity

As described in the HNG-X Network Architecture (Ref:- ARC/NET/ARC/0001) Third parties will connect to a Transit LAN. The Transit LAN is considered to be the boundary between the HNG-X network and any externally administered organisation that HNG-X connects to.

The transit LAN exists both for security and to provide an unambiguous demarcation between HNG-X and that organisation

6.2.1.2 Off-Shoring

Prior to any off shoring work undertaken, staff must refer to the CESG Good Practice Guide No 6 to Off Shoring Managing Security Risks.

Note:- POL have a requirement to advise Government clients of any off-shoring of any service/support service which may impact upon Government information/data.

6.2.2 Addressing Security when Dealing with Customers

Any customer access to POL Account information will be subject to the requirements of the HNG-X Account Information Security Policy (Ref:- SVM/SEC/POL/0003) and applicable components of this ISMS Manual.

6.2.3 Addressing Security in Third Party Agreements

Suppliers of goods and services to Fujitsu that support the Services provided to POL must be subject to formal agreements, using the (Fujitsu) Generic Supplier Contract Template (or equivalent) document as a baseline standard.

The Ariba system is Fujitsu's standard toolset for the Managed Procurement Cycle and Contracting with Suppliers processes and captures all evidence of compliance with and approval of the project steps belonging to these processes. It also captures Third Party Governance. (http://www.cafevik.fs.fujitsu.com/00110/manageprocurement/Pages/home.aspx)

Individual agreements with suppliers of standard COTS components are not required provided that there is clear evidence the components meet all security, regulatory and contractual requirements.

FUJ00232654

7 Asset Management

7.1 Responsibility for Assets

7.1.1 Inventory of Assets

Asset identification and recording is a key aspect of Information Security management and is the maintenance of correct and up-to-date asset information is key to a number of business objectives as described in the Information and Technology Group Hardware Asset Management Policy (Ref:- ITGSM-POL-003).

The POA maintains a Transfer Asset Management Database which is owned by the Commercial Manager. This database contains the data maintained on all major asset hardware, software, development, and data holdings held in an Access database, which is further documented in the Transfer Asset Register (Ref:- COM/MGT/REP/0001).

The Asset Register covers:

- All assets employed by Fujitsu specifically for the delivery of the Services.
- This asset register is a snapshot in time and details assets as at a set moment in time and the impact of any changes due to the development of POL projects that are in progress at this time are not included.

The register is structured according to the main categories of asset, namely:

- Software
- Hardware
- Documentation
- Data

The assets identified within the database are shown where appropriate by their functionality ie:- Production, Test and Development, Counter Estate, Supplier/Third Party.

7.1.2 Ownership of Assets

All assets issued as part of the POA HNG-X Service will be assigned an owner, who will be responsible for the asset as per the Fujitsu UK & Ireland Business Management System Security Policy Manual.

The owner may be a team, rather than an individual. Details of ownership must be documented in the inventory of assets which will be reviewed regular (at least yearly) to ensure its accuracy.

7.1.3 Acceptable Use Policy

All personnel using Fujitsu Post Office Account and Corporate systems will be subject to Fujitsu corporate acceptable use policies as captured in the Fujitsu UK & Ireland Business Management System Security Policy Manual, the Acceptable Use of IT Within Fujitsu Services and the Fujitsu UK & Ireland Business Operations, Information and Technology Group Internal IT Policy (Ref:ITG-PO1).

FUJ00232654

7.2 Information Classification

7.2.1 Fujitsu / POL Classification Guidelines

All information concerning POL and its contracted services, that are not in the public domain, shall be considered potentially sensitive and by default treated as private to POL and its contractors.

Fujitsu has a formal approach to information classification documented in the Fujitsu UK & Ireland Business Management System Security Policy Manual.

The POL Limited Community Information Security Policy for Horizon & Horizon Online (Ref:- External Document - POL/HNG/CIS/001) documents the Information Security Classifications used within POL.

All Users who have access to multiple sources of sensitive, personal, contractual or financial data and whereby this information is then acquired or stored by them run the risk that the classification level (through aggregation) may increase /decrease and this must be reviewed and assessed.

The current Fujitsu and POL approved markings consist of a classification level and Fujitsu also has an optional qualifier.

7.2.1.1 Fujitsu Unclassified

Information marked as Unclassified can be freely shared inside and outside of the company. This marking is optional where its use is unnecessary, however it must be used where there may be some uncertainty about the classification to remove any ambiguity. By definition, Unclassified would never be associated with a qualifier.

7.2.1.2 Fujitsu Restricted

This marking is used for information where there is no reason for disclosure outside of Fujitsu (or the 'qualifier' group if present) and where disclosure to unauthorized persons might cause minor damage.

Examples are company announcements on business plans and internal telephone directories.

7.2.1.3 Fujitsu Confidential

This is used for information where unauthorised disclosure (even within Fujitsu) would cause significant harm to our interests. This would normally inflict harm by virtue of financial loss; loss of profitability or opportunity; embarrassment or loss of reputation.

Examples are sensitive customer information, negotiating positions, market assessments, or competitive information, and technical information that could impact the security of IT systems.

7.2.1.4 Fujitsu Secret

This is used for information and material of an extremely confidential and sensitive nature, or of strategic importance, the disclosure of which could cause grave damage to the interests of the Company.

FUJ00232654

Examples are high-level business and competition strategy and plans, very sensitive competitor, partner or contractor assessments, patent secrecy information, and information, including passwords, vital to the security of IT systems.

7.2.1.5 Fujitsu Optional Qualifiers – Eyes Only

This indicates the scope of data disclosure (e.g. Fujitsu UK&I Eyes Only or Applications Services Eyes Only).

7.2.1.6 Fujitsu Optional Qualifiers – Commercially Sensitive

This applies to information and material which is intended to be shared with a limited number of third parties for business purposes and where disclosure would not result in any significant impact to either Fujitsu or the recipient. It would be used in conjunction with Fujitsu Restricted.

7.2.1.7 Fujitsu Optional Qualifiers – Commercial in Confidence

This applies to information and material, the unauthorized disclosure of which could cause embarrassment or might be detrimental to the interests of the Company, but which nevertheless can be shared with third parties if necessary for business purposes. It would usually be used with Fujitsu Confidential but could be used with Fujitsu Restricted (ie this document).

7.2.1.8 Fujitsu Optional Qualifiers – Personal Addressee Only

This is used where a confidential document is sent to a person where access should be limited to the owner, their delegated representatives, and the intended recipient of the document. An example would be a letter re pay increases. Where the document contains personal information, it would have a handling marking of Fujitsu Confidential.

7.2.1.9 Fujitsu Optional Qualifiers – Staff Restricted

This is used for matters relating to staff and their services, where the subject matter under discussion could apply to a group of staff, and where disclosure or unauthorized access could lead to commercial embarrassment or staff discontent. Examples are bonus scheme details and warnings over disciplinary matters not attributable to an individual.

7.2.1.10 Fujitsu Optional Qualifiers – Personal Information

This marking should also be used for Personal Information requiring special handling. This comprises sensitive personal information as described in the UK Data Protection Act along with other personal information that Fujitsu believes should be subject to similar protection.

Any document containing such personal information should have a handling marking of Fujitsu Confidential or Fujitsu Secret.

7.2.1.11 POL Confidential

“Information that has been assessed to be of a sensitive nature and likely to cause damage following unauthorised disclosure. Personal data (as defined by the Data Protection Act) is classified as confidential. Personal data includes customer account numbers and any transaction data associated with them. FAD codes are sometimes used for authentication purposes and must therefore be treated as CONFIDENTIAL. Transaction records that do not identify a person are confidential on bulk data/reports only. Transaction receipts for individual transactions do not

FUJ00232654

need to be labelled as CONFIDENTIAL, since they are intended as a receipt for a transaction by an individual".

7.2.1.12 POL Strictly Confidential

"Information meeting the classification standards of government departments, the security services, clients, or assessed to be so sensitive that unauthorised disclosure would cause acute organisational damage.

Information identifying cash handling staff, routes and/or timings is STRICTLY CONFIDENTIAL. PIN data and all encryption keys are also interpreted as STRICTLY CONFIDENTIAL".

7.2.1.13 POL Internal

All other information must be classified as INTERNAL unless specifically authorised for release.

7.2.2 Information Labelling and Handling

Data handling guidance is a corporate responsibility and is captured in Fujitsu UK & Ireland Business Management System Security Policy Manual and the Quick Reference Guide - Fujitsu UK & I – Information Classification Matrix.

All documentation and displayed output from POL systems containing information classified as Confidential or Strictly Confidential must carry an appropriate classification label. Fujitsu Restricted documents containing sensitive information shall be stored within the secure library in Dimensions according to the labelling and handling requirements.

POA information, which supports delivery of the Service, that requires protection from unauthorised access (whilst not exhaustive) includes for example:

- The business data exchanged with POL. and its clients (e.g. reference data to support EPOSS and transaction data resulting from Post Office counter activities.)
  Business data is transferred between POL., POL. Clients and the POA Data Centres and between the Data Centres and the Post Office branches. It is stored at the main operation systems and also in archives. Some data is also available for management services via the SMDB.
  POA Classification: Fujitsu Restricted.
  POL Classification: Confidential

- POA business management data - financials, service level agreements etc.
  Confidentiality and integrity requirements exist for much of this data. The Management Information System collects this data from the operational systems. This is then forwarded as appropriate to POA sites, POL. and their Clients.
  POA Classification: Fujitsu Restricted
  POL Classification: Internal - the inclusion of any personal data (as defined by the DPA) in this category, escalates the POL classification to Confidential

- Information contained in documents exchanged between POA and POL in the course of normal business communications.
  POA Classification: Fujitsu Restricted
  POL Classification: Internal - detailing security breaches or potential security breaches, escalates the POL classification to confidential.

- Other supporting the business processes such as training data (special, non-sensitive, business style data used in training sessions) and on-line documentation
  POA Classification: Fujitsu Restricted

FUJ00232654

POL Classification: Internal

- Operational systems data such as the software, configuration information, Tivoli scripts, system management event logs etc. This information must be held in Dimensions Document Management and associated configuration management servers and is subject to change management access controls.
  POA Classification: Fujitsu Restricted.
  POL Classification: Confidential

- Security information about users, Sensitive personal data, details of security investigations, keys, security audit logs etc.
  POA Classification: Fujitsu Secret.
  POL Classification: Strictly Confidential

In addition, POL has specific requirements for the handling of Cardholder Data and Sensitive Authentication Data (see Glossary for definition):

- Sensitive Authentication Data shall not be stored in any file or database including log, audit or diagnostic files after a transaction has been authorised even if the data is encrypted. Such data shall also be deleted after use.

- Cardholder Data shall be rendered unreadable anywhere it is stored (including data on portable media, backup media, and in logs) by using any of the following approaches: One-way hashes (hashed indexes) such as SHA-1, Truncation, Index tokens and PADs with the PADs being securely stored; Strong cryptography such as Triple-DES 128-bit or AES 256-bit with associated key management processes and procedures.

- All Sensitive Authentication Data and Cardholder Data shall be encrypted using approved algorithms and encryption protocols whilst in transit over any public network. It is prohibited to send unencrypted PANs by e-mail. Approved algorithms are 128-bit 3DES (as per ANSI X9.52) and 256-bit AES (FIPS 197). Approved encryption protocols are SSL v3 / TLS, SSH, IPSec, and PPTP. In all other respects Sensitive Authentication data and cardholder data must be treated as POL Confidential: POA Fujitsu Restricted

Any exceptions to these policy requirements will be specifically agreed in writing in the document entitled "Security Constraints" (ARC/SEC/ARC/0001).

FUJ00232654

8 Human Resources

8.1 Prior to Employment

8.1.1 Roles and Responsibilities

8.1.1.1 Professional Communities

Fujitsu has a Professionals Communities Policy which stipulates that the development of its employees is best served by defining and maintaining a set of Professional Communities. These Professional Communities define and support capability development of employees.

The Professional Community structure provides a framework for each employee to connect with groups of people with similar skills and objectives.

These groups are aligned to an organisational structure that supports the specific business needs of our customers.

All employees within Fujitsu are members of a Professional Community which is consistent with their role.

8.1.1.2 Job Descriptions

All personnel engaged on the Fujitsu POA will have Job Descriptions and / or Terms of Reference for their position.

Where POA Staff have specific Information Security responsibilities these will be defined in documented job descriptions and is further documented in POA Security Roles and Responsibilities (Ref~:- SVM/SEC/MAN/2220)

Generic security responsibilities for all staff will be included in all role descriptions or objectives for the appropriate professional community

8.1.2 Screening

8.1.2.1 Employee Background Checks

UK. Fujitsu carries out Personnel Vetting in order to confirm identity, honesty, integrity and right to work in the UK. To achieve this Fujitsu uses the Fujitsu Personnel Vetting Standard as captured in the Explanatory Notes and Application Form: Fujitsu Personnel Vetting (Ref:- FPVS v 3-1)

Some of Fujitsu's Commercial clients, however, from both Commercial and Government sectors, require additional checks to the FPVS to be made before individuals are permitted to work on their accounts.

Completion of the Pre-Employment Screening process is a mandatory condition of employment and **must** be completed within two months of an employee's start date or referral will be made to HR which may affect the continuation of employment.

8.1.2.2 Additional Checks / Security Clearances

FUJ00232654

Requirements for further pre-employment checks for POA Staff are outlined below. It is the responsibility of the hiring manager to ensure that employees have the appropriate level of security for their role.

- Additional security checks, in accordance with POL vetting procedures, must be performed for all POA engineer staff that requires access to Post Office branches in order to undertake development, support or maintenance activities.
- Satisfactory Credit Reference Bureau checks will be required for all POA Staff who have access to financial information contained within Post Office systems.
- Criminal Record Checks will be carried out on POA Staff. This will be done as part of a UK Government specified Baseline Standard check.
- Higher level UK Security Clearance may be required for individuals who have access to POL information classified as Strictly Confidential. Advice should be sought from the Chief Information Security Officer who will confirm the requirement with POL on a case by case basis.

When an existing Fujitsu employee transfers to work on the POA then the hiring manager must ensure the employee has either satisfied the checks above or that the checks are performed if the employee has not already been fully checked.

8.1.3 Terms and Conditions of Employment

8.1.3.1 Employee Contracts

All personnel engaged on the Fujitsu Services Post Office Account will have a signed contract of employment.

The employment contract stipulates that it is mandatory to follow all Fujitsu HR and Information Security Policies.

The Fujitsu Welcome on Board Process aims to integrate the employee into their new/changed environment and provide them with appropriate tools and information to enable them to become effective in their new role quickly and introduce employees to key policies and procedures governing their work

8.1.3.2 Third Party Agreements

As previously captured in Paragraph 6.2.3 suppliers of goods and services to Fujitsu that support the Services provided to POL must be subject to formal agreements, using the (Fujitsu) Generic Supplier Contract Template (or equivalent) document as a baseline standard.

Individual agreements with suppliers of standard COTS components are not required provided that there is clear evidence the components meet all security, regulatory and contractual requirements.

FUJ00232654

8.2 During Employment

8.2.1 Management Responsibilities

All Line Managers are to ensure that POA staff and contractors apply security in accordance with agreed Fujitsu and the POL Information Security Policy (Ref:- SVM/SEC/POL/0003 and supporting procedures.

8.2.1.1 Intimidation

There is always a risk that employees with access to sensitive material could come under forms of intimidation. Employees who have been, or are subject to intimidation should attempt to contact their Line Manager or whoever they report to on the POA either directly or indirectly as soon as it is safe to do so.

Intimidation is considered a form of Bullying or Harassment and any escalations should be in accordance with the Bullying, Harassment and Victimisation Policy.

Employees should not knowingly endanger themselves or others in order to protect company or client assets from theft or damage by criminal entities.

8.2.2 Information Security Education and Training

8.2.2.1 Fujitsu Post Office Account Information Security Awareness

The CISO and the POA Information Security Management Team will promote Information Security awareness and explain the importance and use of Information Security controls.

The Security Communications Strategy (Ref:- SVM/SEC/STG/0739) will promote Information Security awareness and explain the importance and use of Information Security controls. This includes Information Security training as part of Fujitsu POA induction courses for new joiners to the Account. All employees and, where relevant, third party users, will receive appropriate training and regular updates in organisational policies and procedures.

8.2.2.2 Mandatory Fujitsu Internal Information Security Awareness

All Fujitsu Services employees are mandated to complete Information Security Awareness CBT annually.

Additionally, there are other Information Security related CBT's that become available from Fujitsu Corporate including, but not limited to:-

- Data Handling
- Date Protection Act

8.2.3 Disciplinary Process

Any member of POA Staff failing to adhere to the HNG-X Information Security Policy, associated Information Security procedures and instructions may render themselves liable to disciplinary action in accordance with the Corporate Fujitsu Conduct Policy and Fujitsu Conduct Guidelines.

FUJ00232654

8.3 Termination Responsibilities

8.3.1 Termination Responsibilities

When a member of the POA staff exits or transfers from the Account it is the Line Manager's responsibility to ensure that all assets; including information, software and hardware assets are reviewed and returned and that access rights are reviewed and where applicable revoked or adjusted upon change.

Any specific security responsibilities of the departing individual must also be reviewed and reallocated, as necessary.

8.3.2 Return of Assets

All POA Staff must return all of POA Assets in their possession upon termination of their employment, contract or agreement.

When a POA Staff member leaves or is reassigned Line Managers must follow formal HR procedures to ensure the return of all POA property where applicable. This will include return of all POA equipment and software licences. The line manager must ensure that any POA data which is held on personally allocated computers is removed

In accordance with the Corporate Leaving Employment Policy and Internal IT Policy (Ref: ITG-01) all IT assets must be returned to the central equipment management service. Equipment should not be redeployed locally.

8.3.3 Removal of Access Rights

The access rights of all POA staff to information and information processing facilities must be removed upon termination of their employment contract or agreement or adjusted upon change of company assignment or role, including revoking their rights to the system and escorting them from POA premises as documented in the Post Office Account User Access Procedure (Ref:-SVM/SEC/PRO/0012).

When staff members move within the Account, computer access must be modified or terminated as appropriate to their change of role.

Line Managers must ensure that individual access, roles, permissions and capabilities to both physical and information systems are revoked on termination of employment.

Group, system utility or generic administrator accesses using shared, default, or known-sequence passwords, safe combination numbers, etc, must be changed on the departure of a member of the team; this too is a Line Management responsibility.

FUJ00232654

9 Physical and Environmental Security

9.1 Secure Areas

9.1.1 Physical Security Perimeter

Group Property and Group Security have ultimate responsibility for physical security at all sites used by the Post Office Account.

The POA CISO is responsible for working with Group Property and Group Security to ensure that the appropriate physical and environmental controls are in place, based on risk assessment, to protect assets from unauthorised access, damage and interference in line with POA requirements.

All physical perimeters of Fujitsu POL Account sites are clearly defined and site security personnel at Fujitsu POL Account sites maintain an appropriate level of control over the physical security perimeter of each site deploying security barriers, entry controls, CCTV, security fences, special lighting etc. as necessary.

Within all POA sites consideration is also given to any security threats presented by neighbouring premises.

Intrusion detection alarm systems must be used for installations which are left unattended and Alarm Systems must be tested regularly and maintained to manufacturers' requirements.

There are regular visits by Fujitsu Corporate to Fujitsu POA sites to maintain the appropriate levels of physical security ensuring no gaps or weaknesses are introduced.

Data Centres providing processing facilities for Post Office data will have much higher levels of physical security than general offices even though their outward appearance may portray a lower Fujitsu Corporate profile.

All Fujitsu Data Centres are audited frequently in accordance with the Group Security Site Audits Process (Ref:- GB/BSA/0002) for Physical Security and the POA will work closely with the Data Centre Managers to ensure that any observations are acted upon. (It should be noted that this is not just limited to the activities conducted by POA sponsored external auditors).

In short, any POA / POL sensitive information, wherever it is stored, must be physically protected in line with the Information Security Policy and Contractual obligations.

9.1.2 Physical Entry Controls

Generic physical access is the responsibility of Group Property and Group Security has ultimate responsibility for physical security at all sites used by the Post Office Account.

Data centres providing processing facilities for POL data have very high levels of physical security and access is in accordance with Data Centres Site Access System: User Guide (Ref: ISN001021).

POA visitors to POL sites will be subject to any POL screening/vetting procedures and must abide by processes and procedures for such visits provided to the by POL.

9.1.3 Securing Offices, Rooms and Facilities

FUJ00232654

The Fujitsu's POA employs a best practice approach to securing offices, rooms and facilities across all sites, including a Clear Desk Policy.

In practice this means

- Access to all secure areas is strictly controlled.
- All papers, discs and portable media that contain Fujitsu's POA Information are to be stored in an appropriately secured place when not in use.
- PCs and workstations are to be protected by passwords and, either locked or a password-protected screen-saver invoked when not in use.
- Support functions and equipment e.g. photocopiers, fax machines must be sited appropriately within the secure area to avoid demands for access which could compromise information.
- Doors and windows must be locked when unattended and external protection must be considered for windows particularly at ground level.
- Directories and internal telephone books identifying locations of sensitive processing facilities must not be readily accessible by the public.
- The use of portable wireless devices, including items such as 3G phones, is forbidden in areas where sensitive data is stored, processed or transmitted. Cameras, and mobile phones with built in cameras are similarly prohibited.

9.1.4 Protecting Against External and Environmental Threats

Detailed policy for Physical and Environmental security of Data Centre environments (ISN/001377) is included in Fujitsu Data Centre Security Policies.

The selection and design of a secure area must take account of the possibility of damage from fire, flood, explosion, civil unrest and other forms of natural or manmade disasters.

Account should also be taken of relevant health and safety standards and consideration must be given also to any security threats presented by neighbouring premises.

Hazardous or combustible materials must be stored securely at a safe distance from a secure area and bulk supply such as stationery must not be stored within a secure area until required.

There is a Live and Test/DR Data Centre. In the event that there is a disaster at the live site, a decision is required to invoke manual fail-over to the Test/DR Data Centre with RTOs of 2, 5 and 48 hours depending upon the service.

Data is replicated between the Live and Test/DR Data Centre in real time, over the inter-site link in order to avoid the delays, costs and security risks inherent in moving data physically and to meet agreed RPOs.

There is sufficient resilience built into the Live Data-centre to minimise the risk of equipment or service failures invoking the HNG-X Data Centre disaster recovery plan.

9.1.5 Working in Secure Areas

FUJ00232654

Information processing facilities for POL data must be housed in secure areas in accordance with the Fujitsu UK&I BMS Security Policy Manual.

Managers responsible for secure areas must ensure that access rights to secure areas are regularly reviewed and updated at least monthly.

Information processing facilities managed by POA must be physically separated from those managed by third parties.

Physical and logical segregation of POA Assets from other Fujitsu contracts must be maintained, however shared use of data centres, server rooms and environmental facilities is permitted.

Security measures associated with installed equipment must take these factors into consideration to reduce POA's risks to an acceptable level.

Similar considerations apply to POA Assets at other non-POA sites (e.g. AP Client sites).

Unoccupied secure areas must be physically locked and subject to at least daily periodic checks, and there must be physical protection and guidelines for those staff working in secure areas.

Access to sensitive information and information processing facilities must be controlled and restricted to authorised persons only. Authentication controls (e.g. swipe card plus PIN) must be used to authorise and validate all access. An audit trail of all access must be maintained securely.

9.1.6 Public Access, Delivery and Loading Areas

The Fujitsu UK&I BMS Security Policy Manual specifically states that Public access to Fujitsu's POA sites will be through main entrances.

Additionally there is clear direction that where POA sites have isolated delivery and loading areas then these will be monitored when in use by the site security staff either directly or via the site CCTV.

Direct access to the site will not normally be granted to staff via the loading bay or delivery area. The loading bay and delivery area doors are to be kept locked when not in use.

FUJ00232654

9.2 Equipment Security

9.2.1 Equipment Location and Protection

9.2.1.1 Location

In accordance with the Fujitsu UK&I BMS Security Policy Manual all equipment should be located so that it avoids unnecessary access into work areas. Sensitive network devices including servers, routers, firewall etc will be located in secure areas which with some exceptions to meet business requirements shall be in Fujitsu Data Centres.

All printers located in secure areas should be used only used by those processing information in secure areas. General printing shall be conducted outside secure areas. Support functions and equipment ie photocopiers, fax machines must be sited appropriately to avoid demands for access which could compromise information.

9.2.1.2 Positioning

All equipment in secure areas should be positioned so that monitors cannot be viewed by personnel outside secure areas.

All desktop monitors should be positioned so that they cannot be viewed by personnel external to the building or from general public areas

9.2.1.3 Environmental Conditions

Excessive heat and humidity can have an adverse affect on the performance of technology. All equipment placed in racking shall have sufficient gaps to allow air flow and when necessary fans shall be used to cool the room.

Secure areas should be as dust free as possible and consideration should be given to using keyboard membranes should the dust levels warrant them.

9.2.1.4 Prevention of Accidental Damage

There shall be no eating or drinking in secure areas although eating and drinking is permitted at normal desktops.

9.2.2 Supporting Utilities

9.2.2.1 Inspections

The inspection and maintenance of supporting utilities of Fujitsu locations providing Services to the POA is the responsibility of Group Property and is in line with the Fujitsu UK&I BMS Security Policy Manual.

Fujitsu Data Centres are audited frequently in accordance with the Group Security Site Audits Process (Ref:- GB/BSA/0002).and they hold current ISO/IEC 27001:2005 Certification.

9.2.2.2 Uninterruptible Power Supplies (UPS)

FUJ00232654

All critical system components should have a UPS attached so that an orderly shutdown of equipment can be carried out in the event of a power outage.

Plug sockets or multiple adapters shall not be overloaded and surge protection devices should be applied to critical system components.

9.2.2.3 Emergency Contingencies

All key staff members maintaining critical system components should know the location of emergency power off switches in case the need arises for a rapid power down in case of an emergency. The building emergency lighting should activate in case of main power failure.

9.2.3 Cabling Security

As described in HNS Data Centres Blueprint for Availability Management (Ref:- ISN001376) Data Centre Managers are ultimately responsible for all IT and infrastructure and the availability thereof of all equipment within the Data Centre(s).

9.2.4 Equipment Maintenance

Owners of equipment must ensure that it is correctly maintained to enable its continued availability and integrity.

HNS Data Centres Blueprint for Availability Management (Ref:- ISN001376) Data Centre Managers are responsible for planning all maintenance and testing activities related to ensuring continuous availability is achieved.

9.2.4.1 Faults

All faults with Fujitsu assets are to be reported to the Fujitsu Services 7799 Helpdesk in line with the requirements set out in the Fujitsu UK&I BMS Manage Incidents Policy (Ref:- SM-5).

Hardware or Software errors within the HNG-X environment are reported to the Service Desk and managed to closure in accordance with the POA Operations Incident Management Procedure (Ref:- SVM/SDM/PRO/0018).

Within Data Centres the Break-Fix Data Handling SOP (Ref:- ISN07358) covers the end to end process for dealing with the handling and processing of faulty parts within the Data Centres

9.2.4.2 Maintenance Scheduling

All equipment shall be maintained in accordance with the manufacturers' instructions by qualified and authorised maintenance personnel. A record is to be kept by owners of all maintenance work carried out.

9.2.5 Security of Equipment Off-Premises

Off site equipment must be stored securely and adequately protected. Additionally equipment movement must be controlled and subject to appropriate authorization.

FUJ00232654

Regardless of ownership, any use of POA IT equipment by Fujitsu POA personnel outside of all POA premises must be authorised by Line Management who is responsible for ensuring that the user is aware of the security requirements and the access controls requirements.

The Information and Technology Group Care of IT Equipment Policy (Ref:- ITGSM-POL-0017) requires that all permanent, temporary employees, agency staff and contractors are required to take all reasonable precautions to ensure the safety and security of IT equipment in their care.

9.2.5.1 Security Advice – Top 10 Tips to Protecting Laptops and Portable Media

There is guidance on the Fujitsu UK& I Security Portal for Fujitsu staff in protecting laptops and portable media:-

- Only devices registered with and provided and built by Fujitsu may be connected to the Fujitsu network. Item such as Modems, PDAs, Mobile Telephones and other such peripherals must not be connected to a PC or laptop which is or can be also connected to any network that is supporting the Fujitsu business. Such action may inadvertently enable unauthorised users to access Fujitsu systems.
- Never leave equipment unattended in a public place. Most hotels provide safes, either in rooms or at reception: use these to store valuable equipment and information when not in use.
- Avoid displaying any sensitive information on your laptop screen in a public place – you never know who may be looking over your shoulder.
- Make sure that your password is a mix of at least eight alphabetic and numeric characters. A password can be made stronger if desired or if required to meet a specific standard by increasing the number of characters and using upper and lower case and punctuation symbols.
- Before you take your laptop out of the office make sure the hard disk is encrypted.
- When travelling by car: laptops must be stored out of sight in the boot of the car and must not be left in unattended vehicles. Always put your laptop and valuables out of site prior to starting your journey as it is known that thieves can wait at traffic lights watching for cars to stop and then stealing items by simply opening the car door.
- You must not take your laptop or mobile anywhere outside the UK without written approval from your line manager.
- Non-Fujitsu laptops must not be connected to the Fujitsu networks in any way or used to store any company information.
- If you have an RSA Token, do not store it with your laptop, keep them separately.
- The use of non-encrypted USB devices is prohibited.

9.2.6 Secure Disposal or Re-use

The reuse, resale and safe disposal of redundant IT equipment within the POA is provided by Fujitsu's Supply and Lifecycle Services based in Warrington under the Manage Recycle Service (Ref:- SC002).

FUJ00232654

The Service cover all aspects associated with the recycling and refurbishment of IT equipment; from cleaning, auditing, data purging, testing and disposal and in addition Supply and Lifecycle Services provides a guarantee of compliance with all environmental legislation.

Removal and or Destruction of Electronic Media (Ref:- SVM/SDM/PRO/0039) defines the procedures for handling the removal and or destruction of electronic media that is faulty, or requires replacement that holds (or may have held) Sensitive information.

9.2.7 Removal of Property

The removal from site of any equipment (not personally issued laptops etc) which may have been used for storage of sensitive POA or POA data and information must be authorised in advance by appropriate Line Management avoiding any conflict of interests.

9.2.7.1 General

The Fujitsu UK&I BMS Security Policy Manual requires that all equipment moves (with the exception of the personal allocation of Laptop PCs, PDAs, mobile phones or other equipment specifically allocated for personal use) are to be registered on the relevant equipment asset register in accordance with the relevant Asset Management process.

9.2.7.2 Data Centre Procedures

The Data Centres Data Handling Policy (Ref:- ISN006632) is compliant with Fujitsu corporate policies on handling and transporting data and media (as captured in the Fujitsu UK&I BMS Security Policy Manual) and explicitly states that with the exception of Break / Fix requirements (Break-Fix Data Handling SOP (Ref:- ISN07358))an MSC must be raised by the account for all transportation of Data and Equipment irrespective of Protective Marking. This MSC must detail the name of the courier or Trusted Person as well as the Protective Marking or labelling of any data.

9.2.7.3 Security Staff – Random Checks

The Fujitsu UK&I BMS Security Policy Manual also states that Security employees may undertake random checks to ensure that property being removed from Fujitsu UK&I premises (with the exceptions stated above) has the correct authorised documentation.

9.2.7.4 Decommissioning of Equipment

All decommissioning must take account of the removal of any sensitive or confidential information stored on any hardware or electronic media including backups and must ensure that any equipment that is not required is securely stored and documented or disposed of in a secure manner (including network equipment). This includes all equipment used to provide the POA service.

FUJ00232654

10 Communications and Operations Management

10.1 Operational Procedures and Responsibilities

10.1.1 Documented Operating Procedures

The Configuration Plan for HNG-X (Ref:- PGM/CM/PLA/0001) provides an overview used to provide version control and Configuration Management of all Software, Document Management and Change Management configuration items used within the POA solution.

Documents are considered by the POA HNG-X Programme as configurable items and managed as such, with unique identification and strict version control. Documents are defined as outputs from each of the programme lifecycle stages which describe and support the delivery of applications and environments for the HNG-x solution. These are controlled documents and will reside in the HNG-X Dimensions configuration management database.

This is also the case for documents originating from sources external to Fujitsu.

Operating procedures must be treated as formal documents. They must have a named Owner and a Security Classification applied and any Changes must only be made after approval by authorised management.

10.1.1.1 Support Guides

The HNG-X Design & Build Methodology Implementation & Support Documentation Process (Ref:- PGM/PAS/PRO/0007) states the requirement for a Support Guide (SPG), which will provide technical support staff with information to enable them to support that system once it has gone live.

Support guides are also required by the End to End Application Support Strategy (Ref:- SVM/SDM/PRO/0875) and generally written by a combination of the architect / designer for the product and the developers of that product and are based on the DEV/GEN/TEM/0009 document management template.

10.1.2 Change Management

Changes to the provision of services, must be formally managed, taking account of the criticality of business, systems and processes involved and the re-assessment of risks.

The Fujitsu POA has a dedicated Change Management function governed by the Fujitsu Manage Change Policy (Ref: SM-3) and Manage Change Process (Ref: C-MSv1.5).

Information Security is an integral component of the POA Change Management function and is evidenced by the Account Security Management participation in the Change Boards (PCCB & CCB) and the Managed Service Change (MSC) process.

The Change Boards have the total authority and responsibility to accept, reject or defer a Change Proposal (CP) irrespective of its origination (Customer or Internal) and as such acts on behalf of the POA Management Team.

10.1.2.1 Change Owner

This is the individual who owns the change and will progress it through from inception through impacting to Board Presentation, agreement to implementation, support and finally to closure.

FUJ00232654

The Change Owner has the following responsibilities:-

- Understand and own the business need identified within the CP on behalf of the POA.
- Ensure the requirement is clearly identified on the CP and ensure that it is understood and supported.
- Be familiar with and agree all documentation prepared for the Change Boards.
- Where the change is a Change Request (CR) or Request for Work Package (RWP) related construct and complete Commercial Terms (CT) and/or Change Control Note (CCN) for presentation to CCB prior to submission.
- Review impacts, comments, assumptions entered against the Change before attending the CCB, resolving and mitigating all issues.
- Ensure that all aspects of the change have been considered and any associated costs are included in the impacts to be presented.
- Attend the CCB to represent the Business Case for the CP.
- Ensure that any impact on the HNG-X Release Plan is included in the change and the submission to the CCB (having been discussed with the relevant HNG-X Release Manager).
- Ensure that all changes presented to CCB are targeted at an agreed specific Maintenance Release Slot or Major Release where software delivery is required.
- Ensure that all changes presented to CCB include full life-cycle costs i.e. on-going and support costs, not just one-off project costs, which should have been communicated to and agreed with Finance before presentation.

10.1.2.2 Change Originator

This is the individual who owns completes the CP (and other forms) and supplies them to Change Management – normally at the request or direction of the Change Owner.

The Change Originator has the following responsibilities:-

- Completing the CP according to CP Creation Criteria (Ref:- PGM/CHM/MAN/0002)
- Ensure that all changes raised are targeted at a specific Maintenance Release Slot or Major Release where software delivery is required.
- Identification (with Change Owner) of an appropriate Technical Sponsor and Service Delivery Manager
- Assisting with compiling and completing summary information for presentation to the CCB.

10.1.2.3 Technical Sponsor / Service Delivery Manager

The Technical Sponsor is the named individual who approves all the technical content of the CP and the Service Delivery Manager is the named individual who will lead on the Service Delivery aspects of the Change.

Collectively their responsibilities are:-

- Confirming that the requirement is clearly documented.
- The technical solution meets the requirement and is in line with the solution architecture and does not compromise the integrity of the solution.

FUJ00232654

- Ensure that a migration path to the proposed change is documented.
- Ensuring the solution is clearly documented within the CP.
- Participating in a Design Approval Board (DAB) as required.

10.1.3 Segregation of Duties

Accountability of individuals is essential and segregation of duties will be enforced where deemed necessary.

It is the responsibility of Line Management to facilitate such separation and to brief staff on any special responsibilities in order to reduce opportunities for unauthorised modification or misuse of information or services.

Specific requirements for banking keys are described within CS/OLA/051/052 and CS/OLA/051/053 for POA Network Banking Key Management.

10.1.4 Separation of Development, Test and Operational Facilities

Security testing is a critical part of the HNG-X programme. It is vitally important to ensure that the security principles have been followed and that the subsequent security controls have been deployed correctly.

The test environments are

- Solution Validation & Integration (SV&I) (Ref:- DEV/INF/LLD/0032)
- Live System Test (LST) (Ref:- DEV/INF/LLD/0112)

IRE19 will host the Live System Test (LST) and Systems Validation and Integrity (SV&I) test environments during normal (IRE11 Live) operation. Test systems shall only share logical network connection with operational systems in carefully controlled circumstances.

The security testing process is an iterative one, beginning with stringent and exhaustive component testing of individual platform foundation builds and software, as they are released for system testing.

During each subsequent phase of testing, it is expected that the security testing load will change as the initial tests will not need to be repeated and the testing focus will move to cover integration features and the validation of firewall rules and access control lists.

Development, test, and operational facilities must be separated wherever possible to reduce the risks of unauthorised access, or changes, to operational systems.

10.2 Third Party Service Delivery Management

10.2.1 Service Delivery

The POA engages with a number of 3rd Parties to deliver Services to POL and engage with Procurement in accordance with the Fujitsu UK&I BMS Procurement Master Policy (CMP24), associated processes and systems manage the POA's supplier relationships.

The Ariba system is the standard toolset for the Managed Procurement Cycle and Contracting with Suppliers processes and is the central repository for all 3rd Parties engaged by the POA and the system allows the POA to capture all evidence of compliance with and approval of the project steps belonging to these processes. It also captures Third Party Governance and Supplier Performance Management.

FUJ00232654

10.2.2 Monitoring and Review of Third Party Services

Within the POA, the management of 3rd Party Suppliers is governed by the Supplier Management for Non-Procurement Supplier Managers (Ref:- I-Mco1.3) to ensure the continuous ongoing management, assessment and evaluation of the performance of POA Suppliers.

Service Delivery Managers hold monthly meetings with Suppliers and produce a monthly report. These are in turn sent to the MI Systems Lead who collates the findings and produces a monthly Service Review Book and Dashboard which is presented monthly to POL at the Service Review Meeting.

10.2.3 Managing Changes to Third Party Services

All changes to third party contracts will be managed in accordance with POA Change Management procedures as documented in Paragraph 10.1.2.

FUJ00232654

10.3 System Planning and Acceptance

10.3.1 Capacity Planning

The HNG-X Capacity Management and Business Volumes (Ref:- PA/PER/033) documents the process of managing the business workload volumes that the HNG-X system will support and the capacity required to support this workload under contract extension.

The following agreed principles under which business volumes and capacity will be managed include:-

- Post Office estimates the business volumes that the system needs to support. As part of this assessment they need to decide how much headroom or contingency for unexpected growth in volumes is required.
- Fujitsu Services will support the Contracted Volumes and implement the infrastructure needed to support that level of business volumes. This infrastructure may be implemented in several phases if all of the additional capacity is not needed initially.
- Appropriate lets are given against Service Levels if the business volumes are exceeded.
- The Service Management Relationship will periodically review the actual business volumes handled by the system and projected future volumes, to allow sufficient notice to be given to allow any additional capacity to be installed.
- Fujitsu Services shall maintain the capacity model that is shared with Post Office. This allows the impact of changes to be jointly assessed.

10.3.2 System Acceptance

Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system, including any security requirements, carried out prior to acceptance.

This is delivered under Project Management within the established Corporate Customer Solution Lifecycle (CSLC).

The CSLC defines how Fujitsu Services follows a lifecycle of ten stages from early prospecting, through contract approval and signature, to project delivery and subsequent ongoing service delivery.

Within the Fujitsu's POA ISMS there are a number of activities that are required to occur within the overall System Acceptance process. Key activities are captured as:-

10.3.2.1 Project Initiation Review

The purpose of this formal Project Initiation Review is to confirm and ensure that all project requirements, including definitions and control mechanisms are in place for full implementation of the plan/timetable and that the project has a sound basis to proceed.

In addition, the Service Readiness Checklist should be used to guide preparation for acceptance and introduction of the final solution into the live service environment.

Although this is the first formal documented project initiation review within the business delivery procedure, it is expected that the definition will have evolved with the appropriate level of verification from project delivery managers during the bidding cycle.

This is the formal confirmation, which authorises the definitive Project Initiation Document.

FUJ00232654

10.3.2.2 Design Approval Board

The CISO is a member of the Design Approval Board (DAB) which provides technological and financial approval based on strategic solutions, products, and technologies. The DAB assesses the submitted design and offers adjudication to the Designer.

10.3.2.3 Operational Readiness Review

The purpose of an Operational Readiness Review is to verify the readiness status of all activities and work streams within a programme, to ensure the successful transition into delivery.

These reviews will cover the following areas:-

- Confirm the appropriate organisational structure
- Confirm that effective governance is in place, both with the customer and internally.
- Demonstrate that requirements are fully understood, the technical solution, management and governance of any third parties and the associated risks.

10.3.2.4 Service Readiness Review

The purpose of a Service Readiness Review is to ensure that projects deliverables are ready for release into the live environment.

FUJ00232654

10.4 Protection against Malicious and Mobile Code

10.4.1 Controls against Malicious Software

HNG-X Architecture – Security Architecture (Ref:- ARC/SEC/ARC/0003) describes that the HNG-X uses the Sophos anti-virus product and is implemented on all Microsoft Windows 2003 Data Centre platforms and Microsoft Windows XP Support Workstations connected to a Data Centre network (i.e. from a remote site).

Anti-virus signatures and updates will be subject to LST testing to ensure their integrity and will be applied using the Tivoli software distribution system rather than the Sophos management tools to ensure consistency of delivery to system-managed platforms.

Anti-virus software will not be deployed onto either the existing Horizon Windows NT Counters or onto any HNG-X Counter.

Remote support workstations that are not under the control of the HNG-X Data Centre will be updated as required by the Fujitsu Corporate Security Policy document.

10.4.2 Controls against Mobile Code

Mobile code is software code which transfers from one computer to another computer and then executes automatically and performs a specific function with little or no user interaction.

Fujitsu will use generally industry accepted practises in the management of mobile code and will apply suitable controls within operating systems policies and end user browser settings.

The HNG-X Secure Coding Guidelines (Ref:- DEV/APP/WKI/1979) provides a set of secure coding guidelines for developers and designers producing executable code and application configurations for HNG-X.

HNG-X Java Coding Standards (Ref:- DEV/APP/WKI/0005) provides guidelines that should be used on projects that use Java as an implementation language.

These guidelines aim to address the task of writing good maintainable code by defining requirements for the mechanical aspects of implementation, such as, layout, comments, naming conventions etc.

Specifically, the objectives of these guidelines are:

- To establish a common layout of source code. A common layout makes it easier for developers familiar with these guidelines to maintain code that they are unfamiliar with.
- To improve the quality of code so that it is easier to understand, easier to test, and easier to maintain. For example, by specifying how some language constructs should be used common pitfalls can be avoided.
- To create well commented source code that will form part of the documentation of the system.

FUJ00232654

10.5 Backup

10.5.1 Information Backup

Data backups are an essential component of HNG-X and are potentially critical in ensuring data availability in the event of data corruption or system failure.

Data corruption may occur as a result of user error, application error, middleware error, hardware failure or firmware bugs. Data corruption means that the data is no longer readable, or is no longer the data that was written.

In the context of POA HNG-X very little data cannot be recovered from "precursor" data that is data in an upstream system or from a previous processing step.

The Backup and Recovery sub-system delivers the functionality required to recover from data corruption and forms part of the overall solution architecture, as required by

- Section 6, “Availability” - HNG-x Solution Architecture Outline (Ref:- ARC/SOL/ARC/0001)
- Section 5.2.6, “Data Recovery” - System Qualities Architecture (Ref:- ARC/PER/ARC/0001)

A number of backup patterns are used in order to suit the application recovery requirements, and also to maximise the reuse of existing Horizon solutions where appropriate, as these are tried and tested solutions and the overall backup solution is described in HNG-X Backup and Recovery HLD (Ref:- DES/SYM/HLD/0015).

There is no "off-site" storage of data at a third party site. IRE11 and IRE19 are used to hold duplicate copies, and all replication is via the core network or the SAN. There is no requirement to transfer media between IRE11 and IRE19, all such transfer is performed via the SAN.

10.5.1.1 Symantec Netbackup

The HNG-X NetBackup Support Guide (Ref:- DEV/GEN/SPG/0005) provides a work instruction for Netbackup Operators performing Symantec NetBackups on HNG-X and POLMI.

10.5.1.2 Oracle Recovery Manager

Recovery Manager is a standard Oracle product that is used to backup the Branch Database, Branch Support Database, Network Persistent Store Database and APOP Database to Oracle Automatic Storage Management disks.

The Host Branch Database Support Guide (Ref:- DES/APP/SPG/0001) and the Network Persistence Store (NPS) Database Support Guide (Ref:- DEV/APP/SPG/0027) have a backup and recovery sections and depending upon requirements either a Full (Level 0) or Incremental (Level 1) database backups are written to both the IRE11 and IRE19 SANs.

FUJ00232654

10.6 Network Security Management

10.6.1 Network Controls

The network architecture provides facilities to securely transmit data, to provide remote access and to segment networks. In addition analysis and reporting facilities are provided to report against SLAs and to enable base-lining and trending to be performed.

The following facilities are supplied by the service;

- Provides secure network capabilities
- Provides secure remote access facilities.
- Provides network segmentation.
- Enables network analysis and reporting.
- Controls and manages network access control.

Detailed information on the HNG-X network infrastructure is contained in the HNG-X Network Architecture (Ref:- ARC/NET/ARC/0001)

10.6.2 Security of Network Services

Network-based intrusion detection is deployed as part of the HNG-X Data Centre infrastructure. This will provide notification of an attempted compromise of systems within the Data Centre, through malicious activity or malicious code.

This capability is provided using McAfee Intrushield IPS appliances as defined in the IDS LLD (Ref:- DEV/INF/LLD/0051).

Although these devices are capable of Intrusion Prevention they are deployed in passive mode as IDS sensors on selected traffic paths. The traffic paths to be monitored were identified by risk assessment during the IDS design phase and are documented in the IDS Appliance LLD.

As part of the System design process for new services, additional paths may be included in the monitoring with updates to the IDS Appliance LLD as required.

The appliances will allow the monitoring of multiple physical network segments from a single appliance. The appliances are designed to prevent traffic flowing between sensor ports. I.e. it is not possible for the appliance to act as a Router and connect networks, thereby bypassing other security controls.

In addition to raising alerts of malicious activity, the IDS sensors will send feed event logs into the secure event management service, to provide an audit trail and to enable additional event correlation with Firewall, Router and other network device logs.

10.6.2.1 Tivoli Event Management System

Intrusion attempts will be detected through the use of the Tivoli event management system and specifically, alerts raised as a result of failed attempts to logon or to access data with invalid permissions.

10.7 Media Handling

FUJ00232654

10.7.1 Management of Removable Media

The Removal and or Destruction of Electronic Media (Ref:- SVM/SDM/PRO/0039) defines the procedures for handling the removal and or destruction of electronic media that is faulty, or requires replacement that holds (or may have held) Sensitive information.

This procedure is consistent with the Fujitsu UK & Ireland Business Management System Security Policy Manual requirements which also place the following policy requirements upon the POA:-

- Transferring data within Fujitsu UK&I or between Fujitsu UK&I and other parties such as customers, vendors or partners is an important part of business and must be achieved without loss, unauthorised disclosure or damage.
- Loss or unauthorised disclosure of data/media can result in significant reputational damage, fines for Fujitsu, customers or suppliers from the Information Commissioner's Office, breach of contract, loss of existing business and exclusion from future bids.
- Where the system writing the media is capable of encrypting the media then encryption is mandatory.
- Data owned by customers or other third parties must be handled according to relevant contractual requirements or other formal agreements.
- Customer data must not be stored on removable media with the exception of :
  - Agreed system backups;
  - during agreed data migration; or
  - as part of a documented operational process agreed with the customer
- Removable media intended for individual employee use, such as memory sticks or backup drives must be managed appropriately.

10.7.2 Disposal of Media

The reuse, resale and safe disposal of redundant IT equipment within the POA is provided by Fujitsu's Supply and Lifecycle Services based in Warrington under the Manage Recycle Service (Ref:- SC002).

The Service cover all aspects associated with the recycling and refurbishment of IT equipment; from cleaning, auditing, data purging, testing and disposal and in addition Supply and Lifecycle Services provides a guarantee of compliance with all environmental legislation.

Removal and or Destruction of Electronic Media (Ref:- SVM/SDM/PRO/0039) defines the procedures for handling the removal and or destruction of electronic media that is faulty, or requires replacement that holds (or may have held) Sensitive information.

10.7.3 Information Handling Procedures

Data handling guidance is a corporate responsibility and is captured in Fujitsu UK & Ireland Business Management System Security Policy Manual.

10.7.4 Security of System Documentation

System documentation can contain information where unauthorised disclosure could have significant impact, such as application procedures, data structures, access controls etc. and as such must be suitably classified and protected accordingly.

FUJ00232654

The Configuration Plan for HNG-X (Ref:- PGM/CM/PLA/0001) provides an overview of the processes to be used to provide version control and Configuration Management of all Software, Document Management and Change Management configuration items (CI's) used within the POA solution.

System documentation is held within Dimensions and has access controls applied to it.

Only members of staff working specifically on the Account are given access which is controlled by the Business Management Function.

FUJ00232654

10.8 Exchange of Information

10.8.1 Information Exchange Policies and Procedures

All forms of information exchange including email, telephone conversations, meeting notes and minutes, relevant to the scope of this policy, are subject to the high level statements made in the Fujitsu UK&I BMS Security Master Policy (Ref:- CPM20), Fujitsu UK&I BMS Security Policy Manual, the POA Information Security Policy (Ref: - SVM/SEC/POL/0003) and this ISMS Manual.

10.8.2 Exchange Agreements

The exchange of information and software with external organisations will be subject to formally agreed controls appropriate to the classification of the information.

The principle forum for the exchange of Information Security related information is the ISMF which is governed by the ISMF Terms of References (Ref:- SVM/SEC/STD/0031) and recorded in the ISMF Minutes (Ref:- SVM/SEDC/MAM/0003).

The exchange agreements for software used for HNG-X are governed by commercial agreements and software ownership is governed by the terms of the Contract with POL.

10.8.3 Physical Media in Transit

The Fujitsu UK & Ireland Business Management System Security Policy Manual requires that media is to be transported by courier is to be secured according to classification rules and/or any relevant contract.

To date all Post Office interaction with SLS has been via project based work and disposal procedures is set via a definition of Service and Sentencing Rules.

10.8.3.1 Post Office Managed Switch Deployment

The Sentencing Rules for POMS equipment capture that the SLS Recycle Administration Team do not arrange the transport for any collections.

Hardware being returned to SLS is arranged by POA Staff and is via the courier TNT and the following guidelines have been issued to Engineers

- Goods must be well packaged and boxes/totes all sealed. Goods will not be accepted at the TNT depot from the engineer if this is not the case.
- All boxes must have an “Engineer Manifest Sheet” attached to the outside of the box, clearly marked with Project/customer name and Goods Return Note (GRN) number. Do not attempt to return anything without obtaining a GRN number from the project team.
- Ensure all hardware is listed on the “Engineer Manifest Sheet” this enables Warrington to easily identify any missing items whilst in transit.

10.8.3.2 PIN Pads

The Post Office Chip and Pin Project Sentencing Rules (Ref:- RCYSRPOfCP-WOW) identify that collections are arranged through the courier TNT.

FUJ00232654

10.8.4 Electronic Messaging

As required by the Fujitsu UK & Ireland Business Management System Security Policy Manual all employees using Fujitsu UK&I e-mail system are subject to Fujitsu UK&I regional employee acceptable use and e-mail usage policies.

10.8.5 Business Information Systems

As required by the Fujitsu UK & Ireland Business Management System Security Policy Manual all employees using Fujitsu UK&I business information systems are subject to Fujitsu UK&I regional employee acceptable use policies.

FUJ00232654

10.9 Electronic Commerce Services

10.9.1 Electronic Commerce Security

The HNG-X solution meets the requirements of Post Office CR-957, (CCN 1202), introduced as a result of the Payment Card Industry Data Security Standard as described in HNG-X Architecture – Security Architecture (ARC/SEC/ARC/0003).

10.9.1.1 PCI-DSS Definition

The PCI-DSS definition of Sensitive Authentication Data and Cardholder Data is as below.

	Data Element	Storage Permitted	Protection Required	PCI DSS REQ. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

* These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).

10.9.1.2 Sensitive Authentication Data and Cardholder Data

Post Office requirements in relation to sensitive authentication data and cardholder data as defined by the PCI-DSS, the following requirements will be met for Horizon-Online Counters.

- No full track, (magnetic stripe or chip), images will be stored post-authorisation.
- No PIN or PIN Block information will be stored post-authorisation.
- No CVV2, CVC2 or CID information will be stored. (This data is used for card not present transactions which the Horizon-Online system does not currently perform)
- PANs will be hashed, encrypted or otherwise obfuscated by overwriting.

10.9.1.3 Audit Tracks

As described in Horizon (On-Line) Architecture – Support Services (Ref:- ARC/SVS/ARC/0001) Audit Tracks generated after the implementation of CP4305 do not contain the PAN in clear text. Instead there is an encrypted version of the PAN and, in a separate field, a securely hashed version of the PAN. Audit Tracks that were generated pre CP4305 continue to contain a clear text version of the PAN.

10.9.2 On-Line Transactions

FUJ00232654

As captured in the HNG-X Architecture – Security Architecture (ARC/SEC/ARC/0003) the solution has been designed to ensure that for online transactions.

- No card full track information is stored anywhere in the system
  - The Network Banking Service requires that the full track image is available for up to 5 days, post-authorisation, in the event that reversal is required.
- No Sensitive Authentication Data is stored post-authorisation for card transactions.
  - The Network Banking Service requires that the full track image is available for up to 5 days, post-authorisation, in the event that reversal is required.
- No Sensitive Authentication Data is stored post-authorisation for card transactions.
- Any PAN stored in the system will either be in hashed format, encrypted along with the expiry data and issue number, or will otherwise be obfuscated by overwriting

10.9.3 Publicly Available Information

This paragraph refers to the equivalent ISO/IEC 27001:2005 Control and is considered out of scope for the Services being provided by Fujitsu on the POA.

FUJ00232654

10.10 Monitoring

10.10.1 Audit Logging

Within the HNG-X system, Fujitsu Services are required to provide facilities to produce, store and present to (customer) auditors for analysis Audit Track data in support of the security policy and audit requirements laid down for the system.

The Horizon (On-Line) Architecture – Support Service (Ref:- ARC/SVS/ARC/0001) states that within HNG-X, audit data is collected from a number of subsystems. The basic types of audit data that is collected are:

- Counter application messages as received by the Branch Access Layer and stored in the Branch Database message journal table. This will include counter transactions and events
- Data transferred across HNG-X system boundaries. E.g. Bulk file transfers to and from Post Office and their clients
- Host database systems audit and archive data. In this context database audit data refers to the saving of logs of updates applied to the databases, and database archive data refers to the saving of old data that has been purged from the primary databases.
- HNG-X system events – including security events
- Logging of activities undertaken by administrative users during maintenance of the system
- System scheduler logs

Audit data may be requested by a number of different end users, for a number of different reasons. These include:

- Post Office Auditors in connection with Fraud investigations – in which case the data may be presented as evidence in court.
- Fujitsu Services Post Office Account Security Operations Team monitoring compliance with security requirements
- Post Office users handling enquiries regarding banking transactions
- Fujitsu Services System Support Centre for diagnostic information

The Audit system is comprised of:

- An Audit Server located at each campus – these operate Active/Active
- An EMC Centera storage array located at each campus
- A number of audit workstations situated at Bracknell & Lewes.
- Dedicated HP Atalla Network Security Processors situated at Bracknell & Lewes.

Each Audit Server is responsible for gathering Audit Tracks from subsystems and securing them on the local Centera array (secure long term storage). This data is subsequently replicated to the Audit Server at the other campus to ensure that two copies of all Audit Tracks are maintained.

As well as gathering and storing audit data on EMC Centera, the Audit Server provides services to retrieve data from the Audit Archive. These services are utilized by the Audit Workstations.

The Audit server hosts two Microsoft SQL Server 2000 databases, which are resident on its local storage:

FUJ00232654

- The Sealer database which is used to manage the Gathering & storage of Audit tracks
- The ARQ database which is used to manage the Audit track retrieval process

10.10.2 Monitoring System Use

The Enterprise Management software suite, known as SYSMAN3, is an integration of Software Distribution, Asset Management, Event Monitoring, Remote Support and Remote Diagnostics, based around IBM Tivoli software.

The HNG-X System and Estate Management: Monitoring (Ref:- ARC/SYM/ARC/0003) defines the Monitoring functions of SYSMAN3.

Service Monitoring will be performed by event flow; events may be collected in both an active and passive manner, and alerts may be created by sampling, aggregating, correlating or apply other rules on the raw incoming events.

Active monitoring will be achieved by agents looking for known stimuli and raising events via the relevant Event Logs. The IBM Tivoli Monitoring and TEM suite of programs will be used for active monitoring within the solution.

Passive monitoring is the process of collecting events that are already created within the environment (e.g. in the Unix Syslog or Windows Event Log etc.).

The events selected, after the rules are applied at the source, will be forwarded through the network infrastructure to an event collection layer which we may define as event sink. The others will remain in the underlying source but are not forwarded.

10.10.2.1 Tivoli Event Management System

Intrusion attempts will be detected through the use of the Tivoli Event Management (TEM) system and specifically, alerts raised as a result of failed attempts to logon or to access data with invalid permissions.

10.10.2.2 File Integrity Monitoring

File Integrity Monitoring is provisioned by Tripwire and is integrated within the HNG-X systems management tools for event and incident management and for software distribution and is in place to meet the requirements of Post Office in support of PCI Compliance.

FUJ00232654

10.10.3 Protection of Log Information

HNG-X Architecture – Security Architecture (Ref:- ARC/SEC/ARC/0003) describes that all events from each Data Centre Platform Instance system event log are read in real-time and captured by the Tivoli software.

Each entry to the file is read, converted into Tivoli Common Format and forwarded to the Tivoli collection layer as soon as it has been written.

The log files are then securely managed by the Tivoli event management system through a combination of user, file and database access control. This is in addition to the infrastructure access control provided by the Horizon-Online infrastructure such as segregated networking.

The Tivoli system has inbuilt role based access control facilities and these will be implemented to ensure that the users of the system, (administrative or otherwise), can only access the tools and functions that they need.

The administrative users of the Tivoli system will use the Identity and Access Management service for access control and will require a token to be able to logon to the system.

Non-administrative users, (such as Helpdesk staff), will have a set number of Tivoli tasks that can be executed on specific systems and will have very restricted command line access for obtaining specific diagnostic or log data.

10.10.4 Administrator and Operator Logs

As captured in HNG-X Architecture – Security Architecture (Ref:- ARC/SEC/ARC/0003) event analysis and alerting take place in real-time and detailed event correlation reduces the number of events seen by the operator.

Furthermore the Horizon (On-Line) Architecture – Support Service (Ref:- ARC/SVS/ARC/0001) states that within Horizon (Online), audit data is collected from a number of subsystems. The following categories of audit data are collected:

- Counter application messages received by the Branch Access Layer. This will include counter transactions and events
- Data transferred across Horizon (Online) system boundaries. E.g. Bulk file transfers to and from Post Office and their clients
- Solaris Host database systems audit and archive data. In this context database audit data refers to the saving of logs of updates applied to the databases, and database archive data refers to the saving of old data that has been purged from the primary databases.
- NPS database audit data containing a record of banking transactions.
- Horizon (Online) system events – including security events
- Logging of activities undertaken by Fujitsu Services Post Office Account staff during maintenance of the system
- System scheduler logs

FUJ00232654

10.10.5 Fault Logging

10.10.5.1 Fujitsu Corporate Assets

All faults with Fujitsu assets are to be reported to the Fujitsu Services 7799 Helpdesk in line with the requirements set out in the Fujitsu UK&I BMS Manage Incidents Policy (Ref:- SM-5).

10.10.5.2 Service Delivery Units / 3rd Party HNG-X Assets

Hardware or Software errors within the HNG-X environment are reported to the Service Desk and managed to closure in accordance with the POA Operations Incident Management Procedure (Ref:- SVM/SDM/PRO/0018).

Where hardware device support is provided by other Service Delivery Units / 3rd Parties then the Systems Management & Global Cloud (SMC) contact them directly in accordance with (document to be provided by SMC)

10.10.6 Clock Synchronisation

As documented in HNG-X Network Architecture (Ref:- ARC/NET/ARC/0001) time clocks within the service will be synchronised with a reliable time source.

It is further documented in HNG-X System and Estate Management – Overall Architecture (Ref:- ARC/SYM/ARC/0001) that there is a hierarchical solution consisting of several layers (or strata):

- The first stratum is the primary time source. This needs to be a highly reliable and the choice is the GPS satellite network. A data centre resident GPS time server uses rooftop antenna to receive signals from the satellite.
- The secondary stratum is the data centre which contains all the server platforms and network appliances.

These platforms poll the primary time server using version 3 of the NTP protocol as defined in RFC 1305 and requesting the time in UTC format. The NTP product on the platform is configured to achieve millisecond accuracy but will also protect against large clock shifts in a single request after the first synchronisation on reboot.

10.10.6.1 Non Branch HNG-X Network Components

All Data Centre components use a GPS receiver as the NTP time source. Non Data Centre components use Access tier switches as NTP time source.

10.10.6.2 Branch Router

The Branch Router uses an NTP Server on the Boot platform.

FUJ00232654

11 Access Control

11.1 Business Requirement for Access Control

11.1.1 Access Control Policy

The Fujitsu UK & Ireland Business Management System Security Policy Manual has a clear statement that, “Access must be controlled to Fujitsu UK&I sites, logical and physical assets, business processes and functionality”.

Access may be the result of direct user action, or automatically initiated activities and Access Control is the fundamental requirement in managing these access activities to information or services on information processing systems to preserve the Confidentiality, Integrity and Availability of POA and POL business information, services and processes on the basis of business and security requirements.

11.1.1.1 Key Principles

- Physical and logical access to all areas, systems and networks must be controlled and consistent, with access granted selectively, and permitted only where there is a specific need ensuring that there is segregation of access control roles, e.g. access request, access authorization, and access to assets.
- The methodology behind the granting of access must work on the principle that “access should be denied unless specifically permitted” and the principle of “least privilege” must apply to restrict the access rights of users whether human or non-human.
- Access shall be governed by the classification level of information and the requirement for separation and segregation of duties. The higher the classification the more selective the granting of access shall be.
- Users must only be provided with access to the facilities and services that they have been specifically authorized to use and permitted only where there is a specific need taking account of any Legal and Contraction obligations that may apply. (Note:- Some users may be permitted to carry out more than one major function, so are permitted to take more than one “role”).
- All users and applications must be authenticated to IT systems and his authentication must identify them as individuals. (Note:- All access to POA Systems will be monitored).
- Initial default accounts must be renamed where possible and initial default passwords must always be replaced by secure passwords.
- The safety and security, including confidentiality, of access credentials is the responsibility of the each individual issued with the credentials and of those issuing the credentials.

11.1.1.2 Help Desk Environment

FUJ00232654

- Help Desks must maintain the information required to authenticate the callers and their Branches/offices as required for the type of call. If the call needs to be passed onto another internal POA help desk, the call must be forwarded only after the initial authentication has been carried out.

- Wherever authorisation is given orally, normally over a telephone link, additional verification methods must be used. This is achieved by asking callers to confirm their branch code, post code and telephone number.

11.1.1.3 Third Party Considerations

- There must be a demonstrable need for Third Party access and all access to POA information processing facilities by third parties must be controlled.

- A risk assessment must be carried out to determine the security implications and control requirements for any forms of physical and electronic access by third parties.

- On-site third parties must be identified and documented.

- All security requirements resulting from third party access or internal controls must be reflected in the third party contract. Where there is a special need for confidentiality of the information, non-disclosure agreements must be used.

- Access to information and information processing facilities by third parties must not be provided until the appropriate controls have been implemented and a contract has been signed defining the terms for the connection or access.

11.1.1.4 Exceptions

- Any exceptions to the policy must be documented and signed off by the CISO.

FUJ00232654

11.2 User Access Management

11.2.1 User Registration

The User Access Process on the Account is based on the creation and control of a registry of all personnel who work on the account and shall be consistent with User Registration Management Procedure (Ref:- ISN006654).

As documented in the Post Office Account User Access Procedure (Ref:- SVM/SEC/PRO/0012) the User Access Process on the Account is based on the creation and control of a registry of all personnel who work on the account.

This register is controlled by the Account Security Operations Team, and is maintained and updated on a regular basis in line with requests being submitted and tracks all personnel working on the account, the system access they have been given and any security clearance level that they have been granted.

The user registry holds the information about each individual who has been granted access and the systems that they have been granted access to. In addition it contains details of the authoriser, approver and dates that this access was granted last reviewed and revoked

11.2.2 Privilege Management

The Post Office Account User Access Procedure (Ref:- SVM/SEC/PRO/0012) ensures users access is reviewed, reported and audited to ensure that it is functioning effectively and efficiently.

Specifically the POA Security Operations Team shall undertake a monthly review of the access granted to individuals and its continued appropriateness:

- The POA Security Operations Team shall produce details of all users contained in the registry and their access levels and shall email these to the relevant Line/Assignment Managers.
- Line/Assignment Managers shall review whether the current access of their employees is still in line with their job role.
- Line/Assignment Managers shall consider whether any users require their access be amended
- Line Mangers shall confirm each employee's current access rights requirements and shall email these details to the POA Security Operations Team within 10 working days of receipt of the original e-mail from CSPOA Security Operations Team.

If required the Operations Security Manager (OSM) shall provide a monthly update of Privilege Management at the Information Security Management Forum (ISMF).

FUJ00232654

11.2.3 User Password Management

Passwords within the HNG-X environment are managed as per Microsoft standards within Active Directory as outlined in the HNG-X Architecture – Security Architecture (Ref:- ARC/SEC/ARC/0003).

Active Directory group policy is configured to enforce the requirements of the Fujitsu UK & Ireland Business Management System Security Policy Manual, including but not exclusively the following:

- Force users to change temporary passwords at the first log-on
- Enforce password changes
- Maintain a record of previous user passwords and prevent re-use

By design Microsoft Active Directory will ensure passwords are stored securely and not transmitted in an unencrypted form.

11.2.4 Review of User Access Rights

The Security Operations Team conducts a regular review of user access rights and privileges at regular intervals for users who have access to POA Systems and its continued appropriateness.

As captured in the Post Office Account User Access Procedure (Ref:- SVM/SEC/PRO/0012) the POA Security Team achieve this by:

- Account Security Operations Team shall produce details of all users contained in the registry and their access levels and shall email these to the relevant Line Managers.
- Line Managers shall review whether the current access of their employees is still in line with their job role.
- Line managers shall consider whether any users require their access be amended.
- Line Mangers shall confirm each employee's current access rights requirements and shall email these details to Account Security Operations Team within 10 working days of receipt of the original e-mail from Account Security Operations Team.
- The Security Operations Team will review all human accounts that have live access for accounts that have been unused for a period of 90 days or over these will be disabled and the line manager contacted to confirm if situation with the user. Report findings will be detailed in the monthly Operational Security dashboard report and reported upon at the ISMF and recorded in the ISMF Minutes (SVM/SEDC/MAM/0003).

Additionally the Account Operational Security will audit access rights and roles with each functional area. This will be carried out on a biannual basis as minimum and will report findings in the Operational Security monthly dashboard report.

FUJ00232654

11.3 User Responsibilities

11.3.1 Password Use

All Fujitsu staff are required to follow good security practices in the selection and use of passwords in accordance with the Fujitsu UK & Ireland Business Management System Security Policy Manual.

This is further enforced as passwords within the HNG-X environment are managed as per Microsoft standards within Active Directory (as previously mentioned in the HNG-X Architecture – Security Architecture (Ref:- ARC/SEC/ARC/0003).

Active Directory group policy is configured to enforce the requirements of the Fujitsu UK & Ireland Business Management System Security Policy Manual, including but not exclusively the following:

- Enforce a choice of quality passwords
- Enforce password changes
- Force users to change temporary passwords at the first log-on

11.3.2 Unattended User Equipment

Equipment that is accessible by unauthorised people is vulnerable to disclosure, misuse, tampering and theft.

All Fujitsu staff are required to follow good security practices to protect unattended user equipment that they use in accordance with the Fujitsu UK & Ireland Business Management System Security Policy Manual.

11.3.3 Clear Desk and Clear Screen Policy

All Fujitsu staff are required to follow good security practices and adhere to the clear desk policy for papers and removable storage media and a clear screen policy in accordance with the Fujitsu UK & Ireland Business Management System Security Policy Manual

FUJ00232654

11.4 Network Access Control

11.4.1 Policy on Use of Network Services

The Post Office Account User Access Procedure (Ref:- SVM/SEC/PRO/0012) is controlled by the POA Security Operations Team, and is maintained and updated on a regular basis in line with requests being submitted and tracks all personnel working on the account, the system access they have been given and any security clearance level that they have been granted.

The user registry holds the information about each individual who has been granted access and the systems that they have been granted access to.

11.4.2 User Authentication for External Connections

11.4.2.1 Remote User Access Authentication

Remote users must use Microsoft Remote Desktop Client (RDP) in order to logon to AD domain through the SSN terminal servers.

To log on to the network, the user must insert their token into the free USB port. Windows recognizes insertion of the smart card into the reader, as an alternative to the standard CTRL+ALT+DEL key sequence, to initiate a logon. The user is then prompted for their user PIN, which controls access to his private data stored on the smart card. Since the PKI credentials and/or passwords are stored on the card or token, the user can roam within the network, providing scope for a very flexible deployment of systems and users.

Once logged into Windows network, Windows assigns a ticket to the user which grants access to network resources based on user's role. User should no longer be challenged to provide their user credentials for accessing any kerberized services.

Any attempt to start RDP session from a SAS/SSN server to another Microsoft Terminal Server, challenges the user for authentication, as currently Microsoft does not support pass-through authentication. In order to take advantage of pass-through authentication, commercial third party products were considered, but rejected by the business.

11.4.2.2 Third Party Access

A number of third parties connect to the Data Centres using diverse connectivity mechanisms and not all are owned or managed by Fujitsu.

Third parties will connect to a Transit LAN. The Transit LAN is considered to be the boundary between the HNG-X network and any externally administered organisation that HNG-X connects to. The transit LAN exists both for security and to provide an unambiguous demarcation between HNG-X and that organisation.

This clearly defined demarcation is necessary to assist fault and service resolution, to facilitate technical interface specification and to prevent administrative conflicts or inter-penetration between HNG-X and an external organisations network.

This demarcation exists at the physical for routers or switches, at the logical for addressing and routing and at the service level for the traffic between application endpoints that traverse it. The Transit LAN should not be confused with the DMZ; the Transit LAN is the exposed and unpopulated perimeter of the HNG-X network, beyond which no further controlled network devices exist.

FUJ00232654

As documented in the HNG-X Technical Network Architecture (Ref:- ARC/NET/ARC/0001) six Transit LAN models are identified as available for use:

- Remote High Availability Transit with Layer 2 Provision
- Remote High Availability Transit without Layer 2 Provision
- Remote Solitary Transit with Layer 2 Provision
- Local High Availability Transit with Layer 2 Provision
- Wide Are Transit
- Internal Transit

11.4.3 Equipment Identification in Networks

As described in HNG-X Technical Network Architecture (Ref:- ARC/NET/ARC/0001) the Network protocol is IP Version 4 (RFC 791). The semantics of an IP address may be both locality and identity. For example the Data Centre application interprets the source IP of an incoming TCP connection from a branch as the identity of the endpoint and assumes persistence of this identity. Conversely address pools are used in the case where the need to attribute identity does not apply, for example PPP interface addresses for Wireless Wide Area Network (WAN).

For each 3rd party with which HNG-X exchanges IP data grams a Peering IP address space is defined. Each such Peering IP address space will either be under administrative control of the 3rd party or under HNG-X control and shall be specified in the relevant Technical Interface document. It will also be defined / referenced in any OLA/SLA or contractual agreements for mitigation purposes and incident management.

In the 3rd party case they specify the address space. In the HNG-X case the IP address space is allocated as for non-peering HNG-X IP addresses stated above.

11.4.4 Remote Diagnostic and Configuration Port Protection

In order to ensure that only authorised devices may be connected to any component of the HNG-X system, (with the exception of passive devices within the Branch) all network devices will be configured with either a static MAC address allowing only the authorised host to connect, or a single-entry dynamic-learned MAC permission as documented in HNG-X Technical Network Architecture (Ref:- ARC/NET/ARC/0001).

Prior to Live operation, all MAC addresses will be recorded and validated, and all ports not connected will be administratively shut down. This position will be monitored with network management event reporting.

11.4.5 Segregation in Networks

There are a number of defined security domains with the HNG-X security model and therefore data traffic will always be either intra-domain traffic or inter-domain traffic.

The only permitted connections to the POA network must be:

- Intra-domain traffic – Data traffic moving between systems in the same domain.
- Inter-domain traffic – Data traffic moving between systems in different domains.

There is a third class of traffic consisting of data moving into and out of the HNG-X infrastructure.

FUJ00232654

Intra-domain traffic may be unrestricted because the systems share a LAN segment, or may be restricted through the implementation of logical separation, (using Virtual Local Area Networks (VLANs)), or physical separation, (using separate network segments in the same domain).

Inter-domain traffic must pass through an enforcement point that restricts data flow based on its source, destination, protocol, port, type or content/format. This can be a firewall, router or other in-line control point, such as an IPS system. (i.e. The control is physically part of the data path).

A network segment however, whether it is a logical or physical network segment, must be entirely in a domain and cannot span domains. There is no restriction on the number of network segments, firewalls or other network security controls that can be in a security domain.

The security domain model can therefore be viewed as a method of logically grouping network subnets to assist in the development of Firewall and Router Access Lists.

Domains can also span physical locations. For example, the Key Management Domain contains Data Centre systems as well as workstations in remote locations such as Bracknell and Lewes.

The use of this domain model ensures that network segmentation can be implemented to tightly control communication to, from and between HNG-X platform instances.

Separation between environments is controlled using a combination of preventive and detective controls such as access control, firewall rules, BladeFrame configuration, switch configuration and event monitoring.

The HNG-X Platform Hardware Instance List (Ref:- DEV/GEN/SPE/0007) contains a definitive mapping of platform instances to security domains.

11.4.6 Network Connection Control

Within each Data Centre, the HNG-X network is segmented following the Security Domain model as documented in HNG-X Architecture – Security Architecture (Ref:- ARC/SEC/ARC/0003).

The security domain model provides a framework for the network architecture and designs, such that the flow of data around the network is controlled following the principle of least privilege.

The purpose of network segmentation is to reduce the scope of any potential attack. By restricting the ‘attack surface’ to a limited number of systems, any damage caused as a consequence of an attack, can be kept to a minimum.

The network segmentation is achieved using a combination of physical and virtual controls. Dependent on the Security Domain and any specific contractual agreements with third parties, the network segmentation is enforced using VLANs, Stateful Inspection Firewalls, Access Control Lists and physical separation.

Each different network media type is authenticated using a dedicated RADIUS server instance for network device access, with different Challenge-Handshake Authentication Protocol credentials per Branch Router.

Each human support user accessing a network device is authenticated using the Identity and Access Management Service.

11.4.7 Network Routing Control

All access in and out of the HNG-X environment must be restricted to the required traffic from/to the authorised sources/destinations for business and system traffic using routers and firewalls.

FUJ00232654

The HNG-X network is divided into 11 Security Domains. The term Security Domain is defined to mean a collection of platforms and network components grouped together based on type, perceived vulnerability and risk rating. Even so, it may be necessary to restrict traffic between platforms in a common Security Domain (intra-domain traffic) through the implementation of logical separation, (using VLANs), or physical separation, (using separate network segments in the same domain).

Any traffic which crosses network domain (inter-domain traffic) boundaries must pass through an enforcement point that restricts data flow based on its source, destination, protocol, port, type or content/format. This can be a firewall, router or other in-line control point, such as an IPS system. (i.e. The control is physically part of the data path).

The Domain structure places a logical ring around the logical Security Perimeter of the HNGx Network in the Data Centres, but this perimeter extends beyond the Data Centre in some cases. More specifically, this perimeter can be best described as the collection of devices managed (or monitored) by Fujitsu Services, At the boundary of these managed devices a firewall (hardware or software-based) will be located, and the perimeter will be secured according to firewall guidelines laid out in HNG-X Technical Network Architecture (Ref:- ARC/NET/ARC/0001).

FUJ00232654

11.5 Operating System Access Control

11.5.1 Secure Log-on Procedures

Access to operating systems will be controlled by in-build Operating Systems procedures that request the user to log-on using approved, valid credentials.

HNG-X Architecture – Security Architecture (Ref:- ARC/SEC/ARC/0003) describes that all human access to any component of a platform will be controlled using strong authentication. The strong authentication solution uses the Vintella Pluggable Authentication Module (PAM) module from Quest Software to enable UNIX and Linux systems to become objects in Active Directory.

A hardware security token is also used, in conjunction with Active Directory, which uses a combination of the hardware token, public key cryptography and a user passphrase to provide secure authentication.

Before a user can access the system, they must have been provided with a security token, containing the appropriate credentials, by the security manager.

11.5.2 User Identification and Authentication

As captured in HNG-X Architecture – Security Architecture (Ref:- ARC/SEC/ARC/0003) the Horizon-Online environment is managed using an Active Directory tree which controls access to resources through the Windows 2003 Kerberos and Lightweight Directory Access Protocol implementations.

UNIX and Linux systems are managed through the same Active Directory tree utilising a PAM installed on each UNIX system.

Database access is managed through the implementation of scripts to create database users. This approach means that a role-based access control matrix will be created for each database using a standard set of roles across all databases.

Interactive access to a database will be controlled by the directory service in the following way. Access to a SQL Server database on a Microsoft platform instance will use native authentication and the user will therefore effectively have already been authenticated when the logged into the Active Directory domain. Access to an Oracle database will use the ops$_<username> concept which passes authentication of the user to the underlying operating system. This also means that the user needs a strong authentication token to logon to the Active Directory domain, prior to connecting to the database.

However, in each of these cases, the users username and access rights within the database will have been setup externally to Active Directory and will be managed using a script-driven manual process.

Access to a database over the network, (such as from an application or from a management tool), will be controlled through a combination of database access rights and network permissions. In all cases, over the network access to any database will still require that the user be setup within the database and access permissions provided accordingly. Users of any management tool will also have needed to authenticate themselves to Active Directory prior to using the tool.

11.5.3 Password Management System

FUJ00232654

Passwords within the HNG-X environment are managed as per Microsoft standards within Active Directory (as previously mentioned in the HNG-X Architecture – Security Architecture (Ref:- ARC/SEC/ARC/0003).

Active Directory group policy is configured to enforce the requirements of the Fujitsu UK & Ireland Business Management System Security Policy Manual, including but not exclusively the following:

- Enforce a choice of quality passwords
- Enforce password changes
- Force users to change temporary passwords at the first log-on
- Maintain a record of previous user passwords and prevent re-use
- Passwords not displayed on the screen when being entered

By design Microsoft Active Directory will ensure passwords are stored securely and not transmitted in an unencrypted form.

11.5.4 Use of System Utilities

Management domains using system management applications will also provide access and role control appropriate to the operational functions they offer.

Where appropriate, this will utilise the capabilities of Active Directory.

This is defined in the HNG-X System and Estate Management Overall Architecture {ARC/SYM/ARC/0001}.

11.5.5 Session Time-out

The Fujitsu UK & Ireland Business Management System Security Policy Manual states that Fujitsu UK&I will time out sessions and automatically log out the user if no activity is detected after a pre-defined length of time.

11.5.5.1 Microsoft Remote Desktop Client (RDP) Connections

The Microsoft Remote Desktop Client used the Remote Desktop Protocol (RDP) to logon to AD domain through the SSN terminal servers has a session time-out set of 15 minutes of inactivity.

11.5.6 Limitation of Connection Time

The Fujitsu UK & Ireland Business Management System Security Policy Manual states that Fujitsu UK&I will provide restrictions on connection times at the application level where necessary.

FUJ00232654

11.6 Application and Information Access Control

11.6.1 Information Access Restriction

A key principle with the HNG-X Architecture – Security Architecture (Ref:- ARC/SEC/ARC/0003) is that of Least Privilege

Access must be provided using the principle of “that which is not explicitly granted is denied” or a “default deny”, by only granting the permissions necessary to carry out the action being performed. These permissions include application, platform, network and management, (through policy and process), or any combination necessary to perform the action.

This approach assumes that, subject to risk assessment and given the limitations of an operating system or other software, any entity such as a user, an application, a device or an object within application code has no permissions to perform any action before permissions are granted. This assumes that the default configuration of all systems is to deny access. It is very important to ensure that the permissions matrix is developed correctly to ensure that all entities have the access they need to perform their function.

11.6.2 Sensitive System Isolation

The HNG-X Architecture – Security Architecture (Ref:- ARC/SEC/ARC/0003) describes the principles of Security Tiers and Domains to reduce the likelihood of a compromise and to ensure that a compromise of one Platform Instance does not immediately result in the compromise of the entire estate and campus. This model groups together platforms based on type, perceived vulnerability and risk rating.

There are three tiers in this model, adopting the standard architecture for web applications, with the most exposed platforms in Tier 1 and the least exposed in Tier 3. Exposed, in this context, means the type of connection the platform instance has with the outside world.

A security domain model has been designed to effectively segregate the HNG-X infrastructure, such that systems with a similar criticality level are grouped together and systems exposed to a similar level of risk are grouped together.

Traffic passing between security domains must be controlled to only allow the relevant protocol and port necessary for the service being accessed.

FUJ00232654

11.7 Mobile Computing and Teleworking

11.7.1 Mobile Computing and Communications

Fujitsu UK & Ireland Business Operations, Information and Technology Group Internal IT Policy (Ref:- ITG-PO1) captures that there is a single approved method for full remote access into the Fujitsu UK&I network, consisting of the Cisco Remote Access client and the iPass Connect software.. This solution is for the use of individuals using Fujitsu PCs, not for connecting sites or remote offices.

Only standard-build Fujitsu UK&I devices may be connected to CVPN and the security software on the remote device is checked for conformant settings during logon.

As defined in HNG-X Technical Network Architecture (Ref:- ARC/NET/ARC/0001) that once authenticated onto the Fujitsu UK&I network all remote users must use Microsoft Remote Desktop Client (RDP) in order to logon to AD domain through the SSN terminal servers.

There is guidance on the Fujitsu UK& I Security Portal for Fujitsu staff working from Home or Away from the office. The Home Working requirements are captured in Paragraph 11.7.2.

11.7.1.1 Travel

- Never leave equipment unattended in a public place
- Avoid leaving equipment in your car
- Most hotels provide safes, either in rooms or at reception; use these to store valuable equipment and information when not in use
- Avoid displaying any sensitive information on your laptop screen in a public place, you never know who may be looking over your shoulder

11.7.1.2 Overseas Travel

Fujitsu subscribes to a Country Risk Forecast provided by a company called Control Risks. This provides two main services:

- **Country Risk Forecast** - an independent analysis of the latest international political, security and travel developments in over 200 countries worldwide.

- **CityBrief** - concise online travel and security information on 300 major business destinations worldwide.

Fujitsu Staff travelling overseas are also recommended to seek advice from the UK Foreign and Commonwealth Office or, if based outside the UK, from their relevant Government department.

11.7.1.3 Mobile Phones

Fujitsu advocates flexible working and as such issues a large amount of mobile phones to their employees.

The use of these mobile phones is governed by the Information and Technology Group Fujitsu Managed Mobile Service Security Policy (Ref:- ITGSM-05)

11.7.2 Teleworking

FUJ00232654

Fujitsu does employ some members of staff whose default working location is from home and the principles for home based working are captured in A Managers Guide to Home Based Working.

There is further guidance on the Fujitsu UK& I Security Portal for Fujitsu staff working from Home or Away from the office. The Working away from the Office requirements is captured in Paragraph 11.7.1.

11.7.2.1 Home

- Carry out work in a dedicated and lockable work area (where possible) designating a particular room or area of the room solely for that use.
- The work area should minimise and control unexpected interruptions from family or visitors
- Exercise a clear desk policy when out of the room, unless you are able to strictly control and secure access to the work area
- Keep all your backups safe and secure, preferably away from your usual place of work When papers are no longer required bring the documents into a Fujitsu location for secure disposal
- Ensure that valuable equipment is locked away when it is not in use for a long period of time

FUJ00232654

12 Information Systems Acquisition, Development and Maintenance

12.1 Security Requirements of Information Systems

12.1.1 Security Requirements Analysis and Specification

No one approach to software development will meet the needs of every project. The influence of the customer, the project size, the teams experience and location are among many factors that must be acknowledged in defining the most productive process for a project.

Fujitsu uses an architectural approach to methodologies. Recognising that all methodologies address a common set of concerns, Fujitsu has a methodology framework which allows a project-specific methodology to be dynamically created from a set of predefined "best practices" which provide the most appropriate approach to meeting the project's needs.

Apt is a flexible Application Lifecycle Management (ALM) framework within which specific methodologies can be composed from predefined practices, and within which the most appropriate tools can be combined to support the project practitioners.

Waterfall is a sequential and structured approach to software development that enables linear solution progression through discrete, thorough and easily understood phases.

12.1.1.1 HNG-X Design & Build Methodology

The HNG-X Design & Build Methodology (HNGxDBM) lifecycle complements the Fujitsu UK&I BMS ADBM Build and Unit Test (Ref:- CADBM1.2) and Waterfall approach.

The HNG-X Design & Build Methodology Requirements and Design (HNGxDBM) process (Ref:- PGM/PAS/PRO/0002) defines the activities required for the Post Office Account to understand, confirm and document the Post Offices' and internal requirements for the new application development in sufficient detail that a correct and valid solution can be built.

Once all the Business Requirements are analysed a Design Proposal is created using the Design Proposal Template (DES/GEN/TEM/2213).

This will be a description of the design which will:-

- Describe the business and service outcomes that this solution must deliver
- Provide a high level description of the proposed technical and operational solution
- Support dialogue with the Business and Service Requirements stakeholders in order to demonstrate compliance to their requirements.
- Identify the primary technologies that will be used to deliver the solution
- Elaborate on the areas of business change and their impact on the HNG-X Solution and Services
- Identify any impact on the existing HNG-X Architecture and core Solution Designs
- Identify the how the Functional and Non-Functional requirements will be met
- Identify the nature of any Security solution changes

FUJ00232654

- Identify the nature of any impact on existing contractual obligations or measures
- Identify how the solution will be delivered into live service and the manner by which on-going service operation will be achieved

If products are bought in, a formal evaluation and procurement process must be followed. Contracts with suppliers must address the security requirements.

FUJ00232654

12.2 Correct Processing in Applications

12.2.1 Input Data Validation

The HNG-X Design & Build Methodology (HNGxDBM) Code, Build and Component Test process (Ref:- PGM/PAS/PRO/0003) defines the activities required for the Post Office Account to build solution components, based on an understanding of agreed requirements, test them as individual components, integrate those components with others developed internally or by third parties and then conduct component integration testing.

The process details the activities that are necessary to:

- Plan the testing to be carried out on the individual component and any required combinations of components
- Develop the code on the basis of the LLD and applicable coding standards
- Undertake code reviews to determine standards compliance and identify code defects
- Conduct component level testing to identify defects

A Component Test Plan is generated and code review undertaken using the HNG-X Generic Code Review Template (Ref:- DEV/GEN/TEM/0003) to generate comments / defects.

12.2.2 Control of Internal Processing

The HNG-X Design & Build Methodology Implementation & Support Documentation Process (Ref:- PGM/PAS/PRO/0007) states the requirement for a Support Guide (SPG), which will provide technical support staff with information to enable them to manage the transition to the new system and the subsequent support of that system.

The Support Guide includes, but is not limited to, the following

- What errors the software can produce and the events / activities that produce them
- What to do with errors when they are produced.
- List of known deficiencies (with expected clearance dates) and workarounds in place to overcome known deficiencies.

12.2.3 Message Integrity

The HNG-X Design & Build Methodology Code, Build and Component Test process (Ref:- PGM/PAS/PRO/0003)) describes the activities required for the POA to build solution components, based on an understanding of agreed requirements, test them as individual components, integrate those components with others developed internally or by third parties and then conduct component integration testing. .

The process details the activities that are necessary to:

- Undertake code reviews to determine standards compliance and identify code defects
- Conduct component level testing to identify defects

12.2.4 Output Data Validation

FUJ00232654

The HNG-X Design & Build Methodology Code, Build and Component Test process (Ref:- PGM/PAS/PRO/0003) defines the activities required for the Post Office Account to build solution components, based on an understanding of agreed requirements, test them as individual components, integrate those components with others developed internally or by third parties and then conduct component integration testing.

The process details the activities that are necessary to:

- Plan the testing to be carried out on the individual component and any required combinations of components
- Develop the code on the basis of the LLD and applicable coding standards
- Undertake code reviews to determine standards compliance and identify code defects
- Conduct component level testing to identify defects

A Component Test Plan is generated and code review undertaken using the HNG-X Generic Code Review Template (Ref:- DEV/GEN/TEM/0003) to generate comments / defects.

FUJ00232654

12.3 Cryptographic Controls

12.3.1 Policy on the Use of Cryptographic Controls

Services will comply with Post Office Cryptographic standards, contractual and relevant regulatory requirements, including PCI-DSS, for the handing of cryptographic key material and staff are to follow all UK and European standards regulations and directive detailing where and how encryption algorithms may be used as captured in the HNG-X Crypto Services HLD (Ref:-DES/SEC/HLD/0002)

Government specified algorithms and key lengths must be used where POL identifies that they are specifically required by HM Government.

- All cryptographic key lengths shall be at least 128 bits for symmetric keys and at least 1024 bits for asymmetric keys where the associated cryptographic control protects the integrity or confidentiality of Horizon Online Business Data, Reference Data or Application Software.

- PCI requirements state that for PCI Card holder data all Keys shall be AES 256 or TDES 128 bit TDES in length.

Approved keys must be protected in line with Government Specified Algorithms requirements as directed by POL Ltd.

Digital signatures provide a means of protecting the authenticity and integrity of electronic documents. All keys used for signing data must be afforded levels of protection equal to or greater than the highest levels of data signed.

Encryption key management must be independent of network configuration such that the confidentiality of POL traffic is not compromised by a single configuration error of either the WAN or the encryption system.

All cryptographic keys must be protected against unauthorised use, modification, loss, and destruction. In addition, secret and private keys need protection against unauthorized disclosure.

Equipment used to generate, store and archive keys must be physically protected.

It must be possible to recover the system to a secure operating state from the compromise of any key that could directly or indirectly expose plain text PIN values.

12.3.2 Key Management

A structured approach to Key Management will be implemented across all Services provided to POL and is described in more detail in the HNG-X Key Management High Level Design (Ref:-DES/SEC/HLD/0003) and the HNG-X Key Management Support Guide (Ref:-DES/APP/SPG/0004).

The HNG-X Key Management solution has simplified Key Management for the Post Office. The HNG-X Key Management system replaces the Horizon Key Management.

12.3.2.1 Keys

Keys are managed using the HNG-X Key Management Workstation (on the KSN platform), stored on the NPS database and fetched from the NPS database via the Key Service (KSS

FUJ00232654

application on the KMN platform) to the Key Service Client (KSC) located on the various HNG-X business application platforms (e.g. Network Banking Services). The KSC passes the keys to the Crypto Application Programming Interface (API) for use by the business applications.

12.3.2.2 Master File Key

The Master File Key is protected by being stored on the networked HSM (Hardware Security Module) devices introduced for HNG-X. New functionality is introduced at HNG-X to enable the networked HSMs to be shared and used by the business applications that require PAN encryption and decryption services. The business application's Crypto APIs use the HSM Access Service API to access the HSMs. The HSMs are used with the Secure Configuration Assistance and the Key Management Workstation to generate the AKB keys.

12.3.2.3 Traffic Keys

The delivery includes sensitive keys protected by Traffic Keys (TK) specific to the key destination. The TKs themselves are unprotected and must be delivered to each target server by a separate secure mechanism (ie:- delivered manually via a key disk or stored on NPS and delivered by the KSC/KSS mechanism).. In both cases the TK is requested by a Key Store Service at server start-up and held by that service for use within the Horizon-specific cryptographic layer..

FUJ00232654

12.4 Security of System Files

12.4.1 Control of Operational Software

The HNG-X Design & Build Methodology Integration Process (Ref:- PGM/PAS/PRO/0009) describes the activities undertaken to collect and prepare system components that are to be released into the test or live environment.

This process is applicable to integration and release activities during the HNG-X development project and will be reviewed and updated to reflect the different constraints applicable to integration and release in a live environment at that time.

Furthermore, Fujitsu personnel engaged in the provision of the Services to the POA must only use proprietary software within the terms of the licence conditions. Unauthorised copying or distribution of software and documentation is prohibited.

The Account configuration management system will maintain an inventory of all proprietary software used by all services.

The Account Change Management Processes must be utilised at all times to ensure that no changes are made to operational software without authorisation and a regression facility.

12.4.2 Protection of System Test Data

All test data and test cases for POA services will be stored in a change control system and will be protected and controlled as captured in HNG-X DBM System Design, Code, Build & Component Test Process (Ref:- PGM/PAS/PRO/0003)

Operational databases or live data must not be used for testing purposes. Where live information needs to be used, for testing realism the data will be sanitised, where possible, before being used in the test environment.

Operational information will be securely erased from test application systems immediately after the testing is complete.

12.4.3 Access Control to Program Source Code

The HNG-X Design & Build Methodology Implementation & Support Documentation Process (Ref:- PGM/PAS/PRO/0007) states the requirement for a Support Guide (SPG), which will provide technical support staff with information to enable them to manage the transition to the new system and the subsequent support of that system.

The Support Guide includes, but is not limited to, the following

- Code Source Repository – location of code with the repository which is required by the Software Support

FUJ00232654

12.5 Security in Development and Support Processes

12.5.1 Change Control Procedures

Changes to the provision of services, must be formally managed, taking account of the criticality of business, systems and processes involved and the re-assessment of risks.

The Fujitsu POA has a dedicated Change Management function governed by the Fujitsu Manage Change Policy (Ref: SM-3) and Manage Change Process (Ref: C-MSv1.5).

Information Security is an integral component of the POA Change Management function and is evidenced by the Account Security Management participation in Change Boards (PCCB & CCB).

The CCB has the total authority and responsibility to accept, reject or defer a Change Proposal (CP) irrespective of its origination (Customer or Internal) and as such acts on behalf of the POA Management Team.

12.5.2 Technical Review of Applications after Operating System Changes

Prior to any operating system upgrade or change, a review of all application control and integrity procedures must be carried out to ensure that they cannot be compromised by the proposed changes.

The HNG-X Design & Build Methodology Integration Process (Ref:- PGM/PAS/PRO/0009) describes the activities undertaken to collect and prepare system components that are to be released into the test or live environment.

When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

A roll-back capability must be included in any change.

12.5.3 Restrictions on Changes to Software Packages

The security strategy outlined in HNG-X Architecture – Security Architecture (Ref:- ARC/SEC/ARC/0003) is that in order to reduce complexity and implementation times, the approach taken for security applications and services is to use internal Fujitsu services when appropriate and to buy and integrate COTS products rather than develop them internally.

Specific exceptions to this rule have been made in the area of cryptography and key management where the solution has been redeveloped for the cryptographic API, (Ref:- DES/SEC/HLD/0002), and a key management solution has been developed in the absence of commercial alternatives.

FUJ00232654

12.5.4 Information Leakage

12.5.4.1 Obfuscation of Logs

The End to End Application Support Strategy (Ref:- SVM/SDM/PRO/0875) stipulates that certain log files must be processed to obscure personal details that exist within before they can be passed to support teams outside the European Union.

As new log files are generated by system enhancements development units need to be aware of the Data Protection Act (DPA) and ensure that information in any new log files is either benign in DPA terms or that appropriate changes are made to the obfuscation tool.

Areas currently identified as potentially containing personal data are captured in Obfuscation of Counter/BAL-OSR Data For 4LS (Ref:- DES/APP/DPR/0008) and include

- Counter OSR / BAL message log file
- Counter application log file
- Database exports (e.g. CSV exports – Message Journal Exports)
- Screen captures of live system data*
- Audit data extracts (content of message journal)*

**Not handled by obfuscation tool*

In order to allow the use of such information offshore an obfuscation tool has been developed for use on the log files that are known to contain sensitive information before passing to any external support team. The tool has now been integrated into Peak.

12.5.4.2 Obfuscation Tool

The HNG-X Tool for Obfuscation of Counter/BAL-OSR Data: Support Guide (Ref:- DEV/GEN/SPG/0023) document gives guidance on the use and support of the Counter and HBS Obfuscation Tool.

The delivered tool includes the rules required to obfuscate all log files identified in *Obfuscation of Counter/BAL-OSR Data for 4LS* (DES/APP/DPR/0008):-

- Counter message log
- BAL message log
- Counter Post Office Counter log
- Database dump file brdb_rx_rep_session_data.cvs
- HBS Message log
- HBS Application log

Audit logs are not supported by this tool.

Although sensitive data is already obfuscated to comply with PCI when generated, this tool will be used to remove personal identification data that may be logged according to PCI but which must not be sent offshore to India. An individual piece of data may not be sufficient alone to identify a person but combined with other data might be.

The tool obfuscates any individual piece of data that might, in combination with other data, identify a person although it does not check whether any other such data exists.

FUJ00232654

12.5.5 Outsourced Software Development

The POA outsources some Software Development to GDC India. Where this occurs it is provisioned under a documented “Statement of Works” ie:- Statement of Work Post Office Account Fourth Line Support &System Management Centre From the India GDC (Ref:- PO SMC 4LS GDC SoW).

The Statement of Work (SoW), for the provision of services (resources) by the Fujitsu India Global Delivery Centre (GDC) for the Post Office Account (Account), is performed in accordance with the terms and conditions set forth in the Master Services Agreement effective 30th January 2009 between the Fujitsu India Global Delivery Centre (GDC), Fujitsu Consulting India Private Ltd. (FCI), and Fujitsu UK & Ireland, Fujitsu Services Ltd (UK&I).

The GDC are required to adhere to the specific Security Policies in place between the Fujitsu UK&I Post Office Account and the GDC.

FUJ00232654

12.6 Technical Vulnerability Management

12.6.1 Control of Technical Vulnerabilities

The vulnerability management service ensures security patches and updates are maintained at the appropriate level. The service provides secure platform builds that have been hardened to reduce the vulnerability of the standard platform. The service provides protection against malware in the form of Viruses, Trojans, and Worms etc. and detects and prevents malicious code and malicious activity on the network. This service supplies the assurance that possible platform and application vulnerabilities have been reduced to a minimum.

The following facilities are supplied by the service;

- Provides System Hardening
- Provides Vulnerability Management.
- Provides Patch Management.
- Provides Malware Management.
- Controls Vulnerabilities within HNG-X.

The vulnerability management service consists of a number of components that work together to identify and reduce vulnerabilities in HNG-X. This includes vulnerabilities caused by configuration errors as well as software bugs.

12.6.1.1 Vulnerability Scanning

The McAfee Foundstone vulnerability scanning appliance will be deployed into each Data Centre. This appliance will be configured to scan all systems, (including network devices), on a regular basis.

The scanner will always be configured to run non-destructive scans but will be configured with appropriate credentials, on the scanned platform, to enable in-depth Operating System scanning.

Reports will be produced from the vulnerability scanning server as input to the audit process and for analysis by the Security Operations Team.

The vulnerability scanner will be used as a security testing tool during the development phases of the HNG-X project.

The design of the vulnerability scanning server is covered in the HNG-X Vulnerability Management HLD (DES/SEC/HLD/0008)

12.6.1.2 Patch Management

To reduce vulnerability to exploitation and ensure that all systems within the HNG-X environment have the relevant and appropriate patches applied within a reasonable timeframe, there will be a patch management system described in full in the HNG-X Patch Management Process (Ref:- SVM/SEC/PRO/0009) with the design for the patch management system is described in the HNG-X Patch Management HLD (Ref:- DES/SEC/HLD/0006).

This system will provide mechanisms for

- Gathering patches and updates to major operating systems and applications
- Evaluating and filtering the patches and updates

FUJ00232654

- Testing the patches and updates
- Deploying the patches and updates.

The Patch Approval Board is a virtual team that meets monthly and reviews the HNG-X Patch Deployment Spreadsheet and seeks agreement on the patch set to be deployed and in what timescale for example an emergency fix or include at next release.

The team is able to use the criteria established by the manufacturer of the product to assist in making its decision, these take account of the following:

- How likely it is that the vulnerability will affect the operating systems, applications, databases, or network equipment.
- How easy or difficult it is for someone to make use of the vulnerability and use it to create a threat to the POA operating systems, applications, databases, or network equipment, its simplicity.
- The severity of the damage that can occur if this patch is not applied its impact.

The filtered patches will then go through LST testing and be distributed to the target platforms using the Tivoli software distribution mechanism.

Data integrity of each patch or update, (and of software distribution in general), is assured using a file hashing mechanism. This does not give the same level of protection as a digital signature, but in conjunction with the other policy, procedure and technical security controls, it assures that the software installed is the software delivered by the configuration and release management system.

Due to the technical and management security controls in place throughout the Horizon-Online infrastructure, there is considered to be a greater threat from the installation of corrupted code than that from malicious code.

The software distribution mechanism is described in detail in HNG-X System and Estate Management Software Distribution and Asset Management (Ref:- ARC/SYM/ARC/0002)

FUJ00232654

13 Information Security Incident Management

13.1 Reporting Information Security Events and Weaknesses

13.1.1 Reporting Information Security Incidents

An Information Security Incident is defined as "an adverse event or series of events that compromises the confidentiality, integrity or availability of POA information or information technology assets, having an adverse impact on Fujitsu reputation, brand, performance or ability to meet its regulatory or legal obligations."

Information security events must be reported through the POA Service desk as required by the Security Incident Reporting Process described in the POA Operations Incident Management Procedure (Ref:- SVM/SDM/PRO/0018), or via 7799 for supporting systems in accordance with Fujitsu UK&I BMS Security Incident Process (Ref:- I-IS1.1) as quickly as possible. This Process also state that it is an incidents arising from Fujitsu Corporate assets that may affect the support of POA must be reported to the Operational Security Manager.

Incidents that threaten Cardholder Data and Sensitive Authentication Data must also be acted upon as outlined in the POA Operations Incident Management Procedure.

All security incidents reported to the Service Desk must be logged and given a reference and handled in accordance with the incident management process.

All POA Staff will be made aware of their responsibility to report any information security events and suspected breaches as quickly as possible.

13.1.2 Reporting Security Weaknesses

It is recognised by the POA Security Management Team that no system can be 100% secure and the POA may be vulnerable to unknown Security Weaknesses.

As required by the Fujitsu UK&I BMS Security Policy Manual if POA staff identify or suspect that a security weakness exists anywhere in the systems being supported by the Account (including any identified by the Vulnerability Management Service), then they must report these matters to the Account Security Management Team via Line Management at the earliest opportunity in order to prevent Information Security Incidents.

All staff must be aware that they should not, in any circumstances, attempt to prove a suspected weakness themselves. If such a course of action resulted in a security Incident then it may be treated as a disciplinary issue.

FUJ00232654

13.2 Management of Information Security Incidents and Improvements

13.2.1 Responsibilities and Procedures

The management of Incidents is captured in the POA Operations Incident Management Procedure (Ref:- SVM/SDM/PRO/0018). This procedure identifies some key roles within the POA for Information Security Incident Management:

13.2.1.1 Service Desk Agent

The Service Desk Agents provide a single point of contact for users, dealing with the management of routine and non- routine Incidents, Problems and Requests.

13.2.1.2 Incident Manager

The Incident Manager's principle responsibility is to drive the Incident Management process, monitor its effectiveness and make recommendations for improvement. The key objective is to ensure that service is improved through the efficient resolution of Incidents.

13.2.1.3 Incident Resolver

The Incident Resolver is to accurately diagnose and resolve Incidents and Problems within SLA, and to assess, plan, build/test and implement Changes in accordance with the Change Management Process. This role will typically be fulfilled by the support teams and service delivery units

13.2.2 Learning from Information Security Incidents

The POA Quality Management and Security Review Board (QMSR) which meets quarterly will be the forum for evaluating and conducting any lessons learnt from Information Security Incidents.

Findings shall be incorporated into the Information Security Policy review and potentially escalated to the ISMF.

13.2.3 Collection of Evidence

The POA Operations Incident Management Procedure (Ref:- SVM/SDM/PRO/0018) describes that where a follow-up action against a person or organisation after an Information Security incident involves or may involve legal action (either civil or criminal), evidence will be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). Legal action may also be initiated by 3rd parties e.g. by regulatory bodies or controllers of potentially compromised sensitive information.

Should it be considered necessary the incident might be passed to an external investigator or forensics team, who will ensure that any data required for evidential purposes is captured and investigated using a systematic approach which ensures that an auditable record of evidence is maintained and can be retrieved

In some cases, where a compromise to card data is involved, two Forensic Investigation teams may be involved. One team operating on behalf of POL gathering the required audit logs to use

FUJ00232654

to analyse and investigate the problem. A second Forensic Investigations team may be imposed to investigate on behalf of the card acquirer and card schemes. In all incidences where a Forensic Investigation is involved, the Forensic Investigators will be shadowed by POL's Legal and Security Teams.

Incident investigation procedures must ensure that evidence is collected such that it is admissible and of sufficient weight by keeping original documents, copies of information held on hard discs, removable media and log files.

13.2.3.1 Audit Track Retrieval and Analysis

The Horizon (On-Line) Architecture – Support Service (Ref:- ARC/SVS/ARC/0001) describes in detail that the outputs of Audit Track retrieval is initiated by a request (either from within Fujitsu Services or Post Office) for access to audit data. This data may be provided either in its raw form, i.e. a simple copy of the Audit Track files or may be subject to some filtering and analysis by authorised Post Office Account staff before being sent back to the requestor.

Audit Track retrieval and analysis are services are provided to users by the Audit Extractor Client application on the Audit workstation. The audit client application interacts with the Audit servers to perform certain actions.

In summary the workstation supports the following end user services:

- Management and Monitoring of Audit Record Queries (ARQs)
- Online extraction of data from the Audit Archive
- Seal Checking to ensure extracted files have seals intact
- Server based tools to filter Audit Tracks
- Workstation based tools to analyze and present audit data in required format
- Decryption of encrypted PANs relating to Banking or Debit/Credit card transactions

The vast majority of Audit Track retrieval requests are for Post Office branch transaction and event data. Thus the services provided on the Audit workstation are optimized to handle these types of request.

The Audit Extractor Client is implemented as a Microsoft Visual Basic 6 application.

More detail of the design of Audit track Retrieval and Analysis is available in Audit Data Retrieval High Level Design (DES/APP/HLD/0029).

FUJ00232654

14 BUSINESS CONTINUITY MANAGEMENT

14.1 Information Security aspects of Business Continuity

14.1.1 Including Information Security in the Business Continuity Management Process

Fujitsu are committed to Business Continuity as demonstrated by the Fujitsu UK&I BMS Business Continuity Master Policy (Ref:- CPM31).

This Corporate policy advocates that actual or potential Major/Serious incidents that may affect the Activities that support Fujitsu UK and Ireland key products and services by preparing, maintaining and testing Business Continuity Plans (using the Manage Continuity of Fujitsu UK & Ireland Business Process (Ref:- I-AB 1.9)), executing those plans, when business interruptions occur and proactively reducing the impact that incidents will have on the Activities and the key products and services, where it is appropriate to do so.

The POA Business Continuity Manager is responsible for ensuring that a process is implemented to minimize the impact on the Account and delivery of services and recover from loss of information assets. This process will identify the critical business processes and integrate the Information Security management requirements of Account business operations with other continuity requirements.

The HNG-X Business Continuity Framework (Ref:- SVM/SDM/SIP/0001) recognises that a principle requirement specified within schedule B2 of The Agreement is the provision of Business Continuity Plans which conform to an overall 'Service Continuity Framework' which include Information Security.

The POA CISO and / or the Information Security Risk and Assurance Lead will be involved in the development and maintenance of the processes, and any continuity plans, by contributing as a reviewer on any changes to any Business Continuity Plans, to ensure that Information Security requirements are adequately addressed.

The Account Security Management Team shall also send representation to the Post office Infrastructure, Networks and Business Continuity Operational Review Forum.

14.1.2 Business Continuity and Information Security Risk Assessment

Events that can cause interruptions to business processes shall be identified in Business Continuity Tests.

The likelihood and impact of such interruptions and any consequences for Information Security shall be recorded in accordance with the HNG-X Information Security Risk Management Procedure (Ref:- SVM/SEC/PRO/0033).

A coordinated approach between Business Continuity and the Account Security Team is required to measure the Information Security Risk exposure.

14.1.3 Developing and Implementing Continuity Plans including Information Security

FUJ00232654

The POA Business Continuity Manager must ensure that effective business continuity plans are agreed and maintained. The POA Security Management Team under the direction of the CISO should ensure that Information Security is an integral part of the overall business continuity process to reduce the risks from deliberate or accidental threats to deny access to vital services or information including deliberate loss of confidentiality and integrity of POA assets.

The HNG-X Business Continuity Framework (Ref:- SVM/SDM/SIP/0001) captures that there shall be four Continuity Plans for HNG-X and by definition Information Security will have a footprint is all of the following:

- HNG-X Services Business Continuity Plan (Ref:- SVM/SDM/PLA/0002)
- HNG-X Support Services Business Continuity Plan (Ref:- SVM/SDM/PLA/0001)
- HNG-X Security Business Continuity Plan (Ref:- SVM/SDM/PLA/0031)
- HNG-X Engineering Service Business Continuity Plan (Ref:- SVM/SDM/PLA/0030)

These plans must be maintained, to enable internal operations and business services to be maintained following failure or damage to vital services, facilities or information.

14.1.4 Business Continuity Planning Framework

The POA maintains a framework of Business Continuity Plans in HNG-X Business Continuity Framework (Ref:- SVM/SDM/SIP/0001).

The Business Continuity Framework defines the methodology agreed between Fujitsu Services (Post Office Account) and POL for handling all aspects of Business Continuity.

It is the objective of the HNG-X Business Continuity Framework and associated Business Continuity Plans to satisfy both Contractual and internal Corporate requirements for Business Continuity as required by Fujitsu UK&I BMS Business Continuity Master Policy (Ref:- CPM31).

The HNG-X Business Continuity Framework covers the following areas.

- Provide a baseline definition of the Business Continuity Framework and Business Continuity Plans as specified in Schedule B2.
- Provide a detailed definition of Fujitsu Services (POA) deliverables associated with business continuity and the methods of review and assurance.
- Define the contents and format of the Business Continuity Plans.
- Define the overall test strategy adopted for testing of the Business Continuity Plans.
- Define the management processes for the management of Major Business Continuity Incidents.

14.1.5 Testing, Maintaining and Re-assessing Business Continuity Plans

Schedule B2 of the 'Agreement' requires that there are contingency plans in place for the HNG-X 'Applicable Services' and Schedule 1 defines 'Applicable Services'.

The strategy adopted by the POA Business Continuity Manager is to deliver the requirement of testing 'Applicable Services' by verifying the operational continuity of the HNG-X operational services and related infrastructure.

This testing will provide the necessary assurance that all possible business continuity risks have been identified and that appropriate plans are in place to mitigate against such risks.

FUJ00232654

The HNG-X Business Continuity Test Plan (Ref:- SVM/SDM/PLA/0003) brings together the testing requirements of all Post Office Account Business Continuity plans and documents the schedule and methodology to be adopted for both initial and on-going tests.

The POA Business Continuity Management Team produces an annual Business Continuity Test Schedule Planner (Ref:- NSN). Tests will be conducted either through procedural walk-through or through full activation of the contingency plans. Where appropriate, and when agreed, POL will participate in tests which require their input.

The POA Business Continuity Manager is responsible for ensuring that the Business Continuity Plan is regularly reviewed.

FUJ00232654

15 COMPLIANCE

15.1 Compliance with Legal Requirements

15.1.1 Identification of Applicable Legislation

As documented in Fujitsu Way Code of Conduct Global Business Standards (Paragraph 2) Fujitsu are required to comply with legislative requirements and technical and commercial standards in its own right as a business organisation.

The Fujitsu Post Office Account (POA) is required to ensure that it is compliant with requirements placed upon it by its stakeholders.

Stakeholders cascade policies, standards, contractual and legislative requirements onto POA and POA is then required to capture these and manage how it will implement them through a series of controls or rules. POA is also required to monitor and measure how successful the implementation of these controls are and based on these results to review them.

The extensive remit of the obligations placed on POA requires an overall strategy and framework so that the Account can manage all its compliance requirements.

The Quality and Compliance Framework (Ref:- PGM/PAS/MAN/0004) identifies key areas needed to ensure it meets the obligations of its stakeholders and they are planned, operated, managed, monitored and reviewed.

To supply services to POL POA uses shared resources from within the whole of Fujitsu; therefore POA is mandated to follow the frameworks, process and procedures documented by Fujitsu Governance & Compliance, Fujitsu Quality Management and Fujitsu Development Assurance.

Inputs to the Quality and Compliance framework can be broken down into the following areas:

- Legislation & Regulations
- Customer Standards
- Fujitsu Standards
- POA Standards

These are the building blocks of governance as they are the basis for all controls that POA must build into its solutions, services, management and reviews.

POA stakeholders are the sources of these requirements and are individuals and organizations which affect the support or provision of POA services to POL and its other customers.

Advice and guidance on Fujitsu's legal responsibilities is provided by Fujitsu Group Legal department.

FUJ00232654

15.1.2 Intellectual Property Rights (IPR)

Fujitsu Way Code of Conduct Global Business Standards (Paragraph 4) captures Fujitsu's commitment to protect IPR.

The Copyright, Designs and Patents Act 1988 states "The owner of the copyright has the exclusive right to copy the work." It is illegal to copy software without the copyright owner's permission.

Proprietary software must be used within the terms of the licence conditions and unauthorised copying of software and documentation is prohibited.

Where practicable the POA will use vendor-supplied software packages without any modifications. However, if changes are deemed necessary, these should first be requested and agreed within the Account and then only implemented under agreement with the original supplier.

Whilst it would be preferably that the changed software should be issued as an upgrade from the supplier it is recognised that any bespoke modifications may be outside the supplier's software lifecycle.

The POA will not permit any unauthorised modified or non-standard software components to be incorporated.

An inventory of all proprietary software used by the Services will be maintained.

15.1.3 Data Retention and Protection of Organisational Records

As captured in Fujitsu's Documentation and Record Standards (Ref:- Group/Q&BE/03) a record is defined by ISO 9000 as being *"a document stating results achieved or providing evidence of activities performed"* that can be used to document traceability and provide evidence of verification, preventive and corrective action.

Records stored electronically and hard copy retained for the contractual period will be accessible throughout the required retention period and will be safeguarded against loss due to future technology change as referenced in the Audit Trail Specification CR/FSP/006.

Data will be retrievable to meet legal requirements as requested by a court of law, e.g. records required can be retrieved in an acceptable timeframe and in an acceptable format.

15.1.4 Data Protection and Privacy of Personal Data

It is Fujitsu' clearly stated policy to comply with all laws and regulations relating to the protection of personal data in all countries in which it transacts business and to maintain a high standard of compliance in all its worldwide operations as captured in Data Protection Master Policy (CPM 36).

All applications handling personal data on individuals must comply with data protection legislation and principles. POA shall process personal data only in accordance with the instructions of each Data Controller as set out in the Agreement and applicable provisions of CCDs dealing with such processing.

15.1.5 Prevention of Misuse of Information Processing Facilities

It is a clearly stated Fujitsu Policy that users shall be deterred from using information processing facilities for unauthorized purposes as captured in Fujitsu UK & Ireland Business Management

FUJ00232654

System Security Policy Manual and the policy on the Acceptable Use of IT Within Fujitsu Services.

Under the Computer Misuse Act, it is an offence to access or modify material without proper authority, or to access material with intent to commit further offences. Warning notices to this effect must be displayed to potential users prior to system log-on.

15.1.6 Regulation of Cryptographic Controls

Services will comply with Post Office Cryptographic standards, contractual and relevant regulatory requirements, including PCI-DSS, for the handing of cryptographic key material and staff are to follow all UK and European standards regulations and directive detailing where and how encryption algorithms may be used as captured in the HNG-X Crypto Services HLD (Ref:-DES/SEC/HLD/0002)

Government specified algorithms and key lengths must be used where POL identifies that they are specifically required by HM Government.

- All cryptographic key lengths shall be at least 128 bits for symmetric keys and at least 1024 bits for asymmetric keys where the associated cryptographic control protects the integrity or confidentiality of Horizon Online Business Data, Reference Data or Application Software.

- PCI requirements state that for PCI Card holder data all Keys shall be AES 256 or TDES 128 bit TDES in length.

FUJ00232654

15.2 Compliance with Security Policies and Standards and Technical Compliance

15.2.1 Compliance with Security Policies and Standards

Compliance with the requirements defined in the POA Information Security Policy is mandatory. The policy is to be applied throughout POA for the secure management and operation of all systems and Services designed, built, implemented, operated, used, supplied or managed by the Fujitsu POL Account.

Regular audits are carried out under the direction of POA CISO and/or POA Programme Assurance Manager, to verify that POA is operating in accordance with its security policy and procedures.

Security Audits can also be initiated by POL, its clients or regulators either in response to a specific incident or on a regular basis.

These audits will form part of an overall assurance programme and will be scheduled, co-ordinated, reported and corrective action plans acted on as part of an Integrated Audit Schedule (Ref:- PGM/PAS/PLA/0014) which is maintained by the POA Quality Manager.

Where relevant, POA will comply with customer security requirements as expressed in the Community Information Security Policy.

15.2.2 Technical Compliance Checking

POA information systems must be regularly checked for compliance with security implementation standards and regulatory requirements.

Technical compliance checking involves the examination of operational systems to ensure that hardware and software controls have been correctly implemented and is a requirement of The Quality and Compliance Framework (Ref:- PGM/PAS/MAN/0004).

This type of compliance checking requires specialist technical assistance. It shall be performed manually (supported by appropriate software tools, if necessary) by an experienced system engineer, or by an automated software package which generates a technical report for subsequent interpretation by a technical specialist.

Compliance checking also covers, for example, penetration testing, which might be carried out by independent experts specifically contracted for this purpose. Caution should be exercised in case success of a penetration test could lead to a compromise of the security of the system and inadvertently exploit other vulnerabilities.

Any technical compliance check shall only be carried out by, or under the supervision of, competent persons authorised by the Account CISO.

Technical compliance checking will form part of an overall assurance programme and will be scheduled and co-ordinated as part of the Integrated Audit Schedule (Ref:- PGM/PAS/PLA/0014) which is maintained by the POA Quality Manager.

FUJ00232654

15.3 Information Systems Audit Considerations

15.3.1 Information System Audit Controls

Fujitsu Services are required to provide facilities to store audit data and subsequently present it for analysis as described in the Horizon (On-Line) Architecture – Support Services (Ref:- ARC/SVS/ARC/0001).

This is in support of the audit requirements laid down for HNG-X Technical Security Architecture (Ref:- ARC/SEC/ARC/0003).

Audit data may be requested by a number of different end users, for a number of different reasons. These include:

- Post Office Auditors in connection with Fraud investigations – in which case the data may be presented as evidence in court
- Fujitsu Services Post Office Account Security Operations Team monitoring compliance with security requirements
- Post Office users handling enquiries regarding banking transactions
- Fujitsu Services System Support Centre for diagnostic information

Within Horizon (Online), audit data is collected from a number of subsystems. The following categories of audit data are collected:

- Post Office Auditors in connection with Fraud investigations – in which case the data may be presented as evidence in court
- Counter application messages received by the Branch Access Layer. This will include counter transactions and events
- Data transferred across Horizon (Online) system boundaries. E.g. Bulk file transfers to and from Post Office and their clients
- Solaris Host database systems audit and archive data. In this context database audit data refers to the saving of logs of updates applied to the databases, and database archive data refers to the saving of old data that has been purged from the primary databases.
- NPS database audit data containing a record of banking transactions.
- Horizon (Online) system events – including security events
- Logging of activities undertaken by Fujitsu Services Post Office Account staff during maintenance of the system
- System scheduler logs

15.3.2 Protection of Information System Audit Tools

As described in the Horizon (On-Line) Architecture – Support Services (Ref:- ARC/SVS/ARC/0001) The Audit Data Gathering and Storage facilities must be generic and extensible; in particular any new applications introduced into the Horizon (Online) system should interface to the Audit Server.

Tools to extract and prepare data for analysis are provided together with facilities to manage internal Post Office Account data retrieval activities. Access, by Post Office Account staff, to the retrieval and extraction facilities is via the user interface provided on the Audit Workstation

FUJ00232654

Access to the Audit servers and workstations is limited to authorised personnel and is policed using two factor authentication and the Horizon (Online) Identity and Access Management System.

The Audit Workstation provides facilities for authorised Fujitsu Services staff to access the Audit Server in order to retrieve Audit Track data from the Audit Archive and to either select or prepare Audit Track data for presentation to Post Office or in support of internal audit activities. The Audit workstation is dedicated to this task & provides no other facilities.

Browse and filter tools are configured on the Audit Workstation enabling subsequent searches/filters on files to be performed.

There is no automated synchronisation between the Audit Data Extraction and the Audit Data filtering facilities