POL00394877

[TITLE * MERGEFORMAT]

[SUBJECT * MERGEFORMAT]

Document Title: [TITLE * MERGEFORMAT]

Document Type: Architecture (ARC)

Release: Not Applicable

Abstract: This document describes the security framework proposed for HNG-X. It does not go into technical details but covers the principles, process and standards that should be used during the project.

Document Status: APPROVED

Author & Dept: [AUTHOR * Caps * MERGEFORMAT]

Internal Distribution:

External Distribution:

Approval Authorities:

Name	Role	Signature	Date
Mark Wiltshire	Systems Integration Director		
Bill Reynolds	HNG-X Programme Manager		

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

(*) = Reviewers that returned comments

Documents are uncontrolled if printed or distributed electronically. Please refer to the Document Library or to Document Management for the current status of a document.

Uncontrolled If Printed Or Distributed

POL00394877

0 Document Control

0.1 Table of Contents

[TOC \O "1-3
" \H \Z \T "POA APPENDIX HEADING 1,1,POA APPENDIX HEADING 2,2"]

0.2 Figures and Tables

[TOC \t "Caption,3"]

POL00394877

0.3 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	09/11/2006	First Draft	
0.2	24/11/2006	Draft for review	
1.0	16/02/2007	Version for approval.	

0.4 Review Details

Review Comments by :	
Review Comments to :	[HYPERLINK "mailto:jim.sweeting[GRO] & & [HYPERLINK "mailto:PostOfficeAccountDocumentManagement[GRO
Mandatory Review	
Role	**Name**
HNG-X Solution Design	Tom Northcott (or nominees)
HNG-X Security	Bill Membery
HNG-X Infrastructure Design	Nial Finnegan (or nominees)
HNG-X Solution/Infrastructure Design	Tom Northcott/ Nial Finnegan (for nominated child topic architecture and HLD authors)
Service Transition	Graham Welsh
HNG-X Security Architect	Jim Sweeting
HNG-X Test Design	Peter Robinson
Optional Review	
Role	**Name**
HNG-X Development	Gill Jackson
HNG-X Integration	
Service Network	Alex Kemp
Service Support	Peter Thompson
HNG-X System Test	Gaynor Simpson
HNG-X SV&I Manager	Denise Morris
HNG-X RV Manager	Sheila Bamber
VI Manager	
TE Manager	Harjinder Hothi
HNG-X Testing	Peter Dreweatt
Head of Service Management	
SSC	Mik Peach
Business Continuity	Tony Wicks
HNG-X Service Transition	Graham Mockridge
HNG-X Data Centre Migration	Andy Tait
Systems Integration Director	Mark Wiltshire
HNG-X Solution Architect	Dave Johns
HNG-X Design (Reference Data)	Duncan MacDonald
HNG-X Architect (Integration)	Andrew Clifford
HNG-X Architect (Platforms and Storage)	Mario Stelzner
HNG-X Architect (Support Services)	Alan Holmes
HNG-X Architect (Customer Services)	Rob Baulk
HNG-X Architect (Branch Database)	Nasser Siddiqi
HNG-X Architect (Branch Access Layer)	Wille Faler
HNG-X Design (Batch Applications)	Roger Barnes
HNG-X Architect (Migration)	Keith Banks
HNG-X Architect (Counter)	Jeremy Worrell

POL00394877

HNG-X Architect (Network)	Mark Jarosz
Optional Review	
HNG-X Architect (Online)	Andy Williams
HNG-X Architect (Counter Business Applications), Overall Solution Architecture	Giacomo Piccinelli
HNG-X Infrastructure System and Estate Management	Glenn Stephens
HNG-X Infrastructure System and Estate Management	Colin Mills
HNG-X Infrastructure System and Estate Management	Elma Neil
HNG-X Infrastructure System and Estate Management	Ian Bowen
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	**Name**
Project Manager	David Hinde
Technical Author	Trish Morris

0.5 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)			Fujitsu Services Post Office Account HNG-X Document Template	Dimensions
ARC/APP/ARC/0004			HNG-X Architecture - Branch Access Layer	Dimensions
ARC/APP/ARC/0008			HNG-X Branch Database Architecture	Dimensions
ARC/APP/ARC/0009			Counter Business Applications Architecture	Dimensions
ARC/GEN/REP/0001			HNG-X Glossary	Dimensions
ARC/NET/ARC/0001			HNG-X Network Architecture	Dimensions
ARC/SOL/ARC/0001			HNG-X Overall Solution Architecture	Dimensions
ARC/SYM/ARC/0001			System and Estate Management – Overall Architecture	Dimensions
ARC/SYM/ARC/0003			HNG-X System and Estate Management Monitoring	Dimensions
DES/GEN/STD/0001			HNG-X Host Applications Database Design And Interface Standards	Dimensions
RS/POL/002			Horizon Security Policy	PVCS
RS/POL/003			Horizon Access Control Policy	PVCS

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

POL00394877

0.6 Abbreviations

Abbreviation	Definition
APOP	Automated Payment Out-Pay
APS	Automated Payment Service
CMA	Computer Misuse Act
DES	Data Encryption Standard
DPA	Data Protection Act
DRS	Data Reconciliation Service
DWh	Data Warehouse
FOIA	Freedom of Information Act
FSA	Financial Services Authority
IDS/IPS	Intrusion Detection System/Intrusion Prevention System
IMS	Internet Managed Services
IPSEC	Internet Protocol Security
LFS	Logistics Feeder Service
NPS	Network Banking Persistent Store
PAF	Postal Address File
PAM	Pluggable Authentication Module
RADIUS	Remote Authentication Dial-In User Service
RDDC	Reference Data Distribution Service
RDMC	Reference Data Management Centre
RDT	Reference Data Testing
RIPA	Regulation of Investigatory Powers Act
SAS	Secure Access Server
SEIM	Security Event and Information Management
SSL	Secure Sockets Layer
TACACS	Terminal Access Controller Access Control System
TDES	Triple DES
TES	Transaction Enquiry Service
TPS	Transaction Processing Service
VPN	Virtual Private Network

POL00394877

0.7 Glossary

See [REF ARCGENREP0001 \h].

Term	Definition

0.8 Changes Expected

Changes

0.9 Accuracy

Fujitsu Services endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

0.10 Copyright

POL00394877

1 Introduction

ABSTRACT: Contains a definition of what "architecture" means in relation to IT systems. Lists the sources of requirements and provides a high-level introduction to the document.

1.1 Definition

This document describes the security framework proposed for HNG-X. It does not have detailed technical information but covers the principles, process and standards that should be used during the project.

This document uses the Open Group description of an architecture which is:

"The structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time."

The first draft of this document concentrates on the "principles and guidelines governing their design and evolution over time."

Security, when correctly implemented, is not a block on business activity and progress, on the contrary it must be in place as a business enabler to allow change to take place as quickly as the business requires, but in a secure and controlled fashion.

It is very important therefore that a set of guiding principles are agreed and established, and embedded into the planning, change management and operational processes of HNG-X. These principles will ensure that the appropriate level of risk management is performed and the controls that are then put in place will be secure, cost-effective, appropriate to the requirements and will allow business change to take place quickly and securely thereby ensuring the greatest possible cost benefits,

1.2 Requirements Sources.

The security architecture document has been developed from the following sources;

1) Post Office requirements
   a) Source document: [**HNG-X Security Requirements Vsn 0.2**]
2) Compliance requirements.
   a) Legislation
      i) Computer Misuse Act, Data Protection Act, Freedom of Information Act, Regulation of Investigatory Powers Act.
   b) Regulation
      i) FSA
   c) Standards
      i) ISO27001
3) Fujitsu requirements

POL00394877

2 Business Drivers

ABSTRACT: Contains a list of the key business drivers identified and extrapolated from existing documentation and conversations relating to the initiation of the HNG-X project.

2.1 Explicit Business Drivers

#	Explicit Business Driver
ED1	To reduce operational costs. (Cost Control)

2.2 Implicit Business Drivers

#	Implicit Business Drivers
ID1	Protecting the reputation of Post Office Ltd, ensuring that it is perceived as competent in its sector
ID2	Providing support to the claims made by Post Office Ltd about its competence to carry out its intended functions
ID3	Protecting the trust that exists in business relationships and propagating that trust across remote electronic business communications links and distributed information systems
ID4	Maintaining the confidence of other key parties in their relationships with Post Office Ltd
ID5	Maintaining the operational capability of Post Office Ltd's systems
ID6	Maintaining the continuity of service delivery, including the ability to meet the requirements of service level agreements where these exist
ID7	Maintaining the accuracy of information
ID8	Preventing losses through financial fraud
ID9	Detecting attempted financial fraud
ID10	Providing the ability to prosecute those who attempt to defraud Post Office Ltd
ID11	Ensuring that the solutions provided for securing electronic business services include a clear and unambiguous definition of responsibilities and liabilities for all parties at every stage of the transaction
ID12	Ensuring that information processed in Post Office Ltd's systems can be brought to a court of law as evidence in support of both criminal and civil proceedings and that the court will admit the evidence, and that the evidence will withstand hostile criticism by the other side's expert witnesses.
ID13	Ensuring that the information security approaches used in HNG-X directly support compliance by Post Office Ltd with commercial contracts to which Post Office Ltd is a party

POL00394877

#	Implicit Business Drivers
ID14	Ensuring that Post Office Ltd is at all times compliant with the laws and industry sector regulations, and that the information security approach in the system directly and indirectly supports legal compliance
ID15	Maintaining the confidentiality, integrity and availability of information that is stored, processed and communicated by HNG-X.
ID16	Protecting against the deliberate, accidental or negligent corruption of personal and business information that is stored, processed and communicated by HNG-X
ID17	Ensuring that an entity that makes a business transaction cannot later deny having made the transaction, and that the entity will be bound by the contractual obligations associated with making the transaction
ID18	Ensuring that all users can be held accountable for the actions that they take in making use of their access privileges
ID19	Ensuring that access privileges are designed and implemented in such a way as to minimize the risk of a single individual having excessive power that could be abused without being easily detected.
ID20	Providing assurance of the correct functioning of the HNG-X system
ID21	Providing for the setting of policy and the control and monitoring of compliance with policy by the authorities vested with the responsibility for corporate governance in the system environment
ID22	Protecting other parties with whom Post Office Ltd has business dealings from abuse, loss of business or personal information
ID23	Ensuring that the employees using the system are only granted authorised access within need-to-know and need-to-use privileges
ID24	Ensuring that the security of HNG-X is dependent only on its system security measures and not on the security competence of any other organisation
ID25	Ensuring that the granularity of system security services is appropriate to business need.
ID26	Preserving the ability of authorised business users to maintain a high level of productivity
ID27	Ensuring that information security interfaces are easy and simple to use
ID28	Utilising, where possible, commercial off-the-shelf products to build information security solutions
ID29	Ensuring that security services can be extended to all user locations, to all interface types and across all network types that will be used to support delivery
ID30	Ensuring that system security solutions comply as far as possible with internal and external standards and best practices
ID31	Ensuring that the security architecture is independent of any specific vendor or product and is capable of supporting multiple products from multiple vendors

POL00394877

#	Implicit Business Drivers
ID32	Ensuring that the security architecture remains compatible with new technical solutions as these evolve and become available, and with new business requirements as these emerge, with a minimum or redesign.
ID33	Adapting the security architecture to counter new threats and vulnerabilities as they are discovered.
ID34	Ensuring accurate information is available when needed
ID35	Minimising the risk of loss of key customer relationships

POL00394877

3 Scope and Constraints

ABSTRACT: Contains a description of the scope and constraints for the development, implementation and operation of the HNG-X system. Includes reference to key non-functional requirements as constraints.

3.1 Scope

1) Produce a technical security architecture that informs and guides the development, implementation and operation of the HNG-X system and activities relating to this purpose, (including change management);

   a) of the HNG-X infrastructure.

   b) of HNG-X application software.

   c) of the HNG-X operational support functions.

3.2 Constraints

Established from Post Office Ltd's non-functional requirements - source document **HNG-X Security Requirements Vsn 0.2.** See Appendix A.

POL00394877

4 Principles

ABSTRACT: Lists and describes the principles guiding the secure development, implementation, operation and change of the HNG-X system.

These principles apply to the design, development, test, implementation and operation of all components of the HNG-X system. The extent to which they are applied is subject to a risk analysis to assess the threats and vulnerabilities present in the system. The controls used to mitigate the identified risks are then selected as appropriate.

The controls to be used could be devices such as firewalls or intrusion detection systems. They could be policies, standards and/or guidelines. They could also be coding and testing guidelines/standards.

Principle and Explanation

1 A risk based approach is used to development, design, operations and changes.

When a solution is being planned and designed, the Risk Management Policy and guidelines must be used to establish the potential threats, vulnerabilities and risks applicable to the solution.

Threat scenarios should be created to further develop and explore possible vulnerabilities in the system or design.

Security controls are only as strong as the weakest link, therefore the risk assessment focuses priority and resources on the risks with the largest impact and identifies the weak links in the chain.

The risk assessment method chosen will differentiate between two types of attacks;

1) *'Theoretical' attacks, those that need an expert knowledge in lab conditions to modify an entity protected by a security control, even if this serves no practical purpose.*
2) *'Real world' attacks, those that are likely to be used for malicious purposes such as service disruption, information gathering or fraud.*

This is to ensure that the risk assessment is conducted efficiently and considers threats and vulnerabilities that are likely to have the biggest impact.

2 Control access to, from and within the HNG-X infrastructure.

Access to the HNG-X infrastructure from external entities must be controlled following the guidance in the Access Control Policy and using a combination of network, platform and application access controls.

Access within the HNG-X system must be controlled using a combination of network, platform and application access controls following the guidance in the Access Control Policy.

Security domains are defined within HNG-X that describe groups of security entities with similar security requirements. Access between domains must be controlled.

3 Ensure anomalous activity is detected and responded to.

Incidents and events must be detected and managed to ensure that HNG-X is available and operating in line with agreed SLAs.

The impact of an incident is greatly reduced through rapid and effective incident response. This requires that incidents are contained and detected quickly.

POL00394877

Principle and Explanation

4 Ensure systems are maintained to reduce vulnerability.

Systems must be configured correctly, patched and updated following the guidance in the Incident Management Policy to ensure that HNG-X is available and operating in line with agreed SLAs.

Standard policies, operating procedures and standards will be written for HNG-X to provide guidance on reducing and managing vulnerability through risk assessment, secure builds, patching and malicious code management. These policies, operating procedures and standards with contain appropriate validation methods, linked to change management, to ensure consistency of deployment.

5 Ensure compliance with all relevant legislation, regulation and standards.

All relevant legislation, regulation and standards must be identified and their requirements established in accordance with the guidance in the HNG-X Compliance Policy.

6 Ensure traceability to a business requirement.

All security controls must be traceable back to a specific business requirement.

7 Consider the "big picture" when developing solutions.

Can the solution be used elsewhere or for other purposes. Do not deploy "point solutions" without considering what else is already available or where else the proposed solution could be used.

8 Least Privilege

Restrict access using the principle of "that which is not explicitly granted is denied" or a "default deny" stance by granting only the permissions necessary to carry out the action being performed. These permissions could be application, platform, network or management, (through policy), 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.

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

9 Defence in Depth

Use a layered approach to security to provide multiple controls for prevention and detection. These controls will include application, platform, network and management controls. Controls and their relevance will be established by risk assessment, the results of which must be documented.

10 Data Validation

Subject to risk assessment, data should be validated in all locations where processing of, or access to, the data occurs. For example; it may be necessary to validate input at the counter and then validate again by the application middleware. This will ensure that SQL injection, application buffer

POL00394877

Principle and Explanation

overflow or similar attacks will be unsuccessful.

11 Secure Defaults

All default settings, particularly passwords and SNMP communities must be changed in line with the HNG-X Security Policy guidance on passwords, before the system is deployed into live.

12 No Security by Obscurity

Information hiding, as a sole or primary security control, is not an acceptable method of implementing security. For clarity, this does not refer to the use of properly designed and configured encryption and decryption technologies.

There will be no need for a security mechanism to be hidden so that it is effective. i.e. In the case of cryptography, the algorithms used can be well known as it is the key, when used with the algorithm, that provides the security.

13 Check at the Gate

Check access as early as possible. Detect and prevent unauthorised access as early as possible.

14 Fail Secure

System failure should not allow the system to be compromised. Within the limits of the technology and availability requirements, any component of the system that fails due to error or malicious activity should fail secure. This failure event must be detected as early as possible so that suitable containment and remediation activities can be carried out.

15 Harden Systems and Applications

All systems and infrastructure must be 'hardened' to an appropriate level. This is a process of setting file, program and access permissions appropriately, removing unnecessary services and software, applying up to date patches and configuring additional software where the risks to the target warrant it. (Such as installing anti-malware software).

16 Don't Reveal Excess Information

Handle errors gracefully. Don't reveal information unnecessarily. Standard web, application and database server error messages should be modified or replaced where necessary so as to avoid the leakage of potentially damaging information.

17 Simple is Good

The simpler a design is, the easier it is to maintain, secure and operate. This is following the principle of "as simple as it needs to be, but no simpler"!

18 Don't Trust Services

Assume external services are insecure. Conduct and document a risk assessment on any external services. Validate input from external services. Control access from external services.

19 Don't Trust Infrastructure.

Assume external infrastructure is insecure. Conduct and document a risk assessment on any

POL00394877

Principle and Explanation

external connections. Control access from external infrastructure. Control physical and logical access between security domains within HNG-X.

These principles will be adopted during the design, development and implementation of the HNG-X system but will not apply to the migration of existing Horizon systems that are being migrated "as-is".

POL00394877

5 Architecture Description and Road Map

ABSTRACT: Lists the new documents to be produced and briefly describes their content. Contains a description of the architecture framework specific to HNG-X by defining the control objectives, security strategy, various models and trust relationships developed from the business drivers and the non-functional requirements. Also contains a high-level roles and responsibilities matrix.

5.1 Security Strategy

The security strategy for HNG-X uses the Prevention => Containment => Detection => Response model.

Item	Description
Prevention	Use a combination of security controls such as physical, network, platform and application access control, system hardening and vulnerability management to reduce vulnerability.
Containment	Restrict the spread of malware or malicious activity using network segmentation, anti-malware controls and physical, network and platform access control.
Detection	Quickly detect the presence of malicious activity or malware in any domain of HNG-X through the use of anti-malware, intrusion detection and security event management controls.
Response	Automatic or manual incident response to mitigate the activity using pre-configured activities, intrusion prevention and incident response procedures.

This strategy provides defence in depth protection to the HNG-X system through the application of layered security controls.

This model applies to both infrastructure and software development.

To reduce complexity and implementation times, the approach taken for applications and services is to use internal Fujitsu services where appropriate and to buy and integrate COTS products.

5.1.1 Business Applications and Services

HNG-X Overall Solution Architecture X (ARC/SOL/ARC/0001), defines multiple business applications and capabilities as listed below ;

1) Counter Applications
2) Data Centre Applications and Services
   a) Legacy Host Databases – TPS, APS, LFS, DRS, TES
   b) External Online Services – Banking, Streamline, ETU, DVLA
   c) Internal Online Services – APOP, PAF, Help Pages, Counter Training Web Services, Help Desk.
   d) Enquiry and Admin – APOP (Enquiry and Administration), TES (Enquiry only)
   e) Reference Data – RDMC, RDT
   f) Batch – APOP, APS, DRS, DWh, LFS, TES, TPS

POL00394877

g) Near Real-Time – Track and Trace, LFS, RDMC

h) Support Services – Audit, MID/TID Management, Estate and System Management

3) Information Management

a) NPS, TES, DWh, APOP, DRS, TPS, APS, LFS, RDMC, RDDS, Branch Database

5.1.2 Security Domains

There are a number of defined security domains with the HNG-X security model. For data to move from one domain to another requires that they pass through an enforcement point. This enforcement point can be an infrastructure control such as a firewall, or can be an application control such as a validation check, digital signature check or access control check.

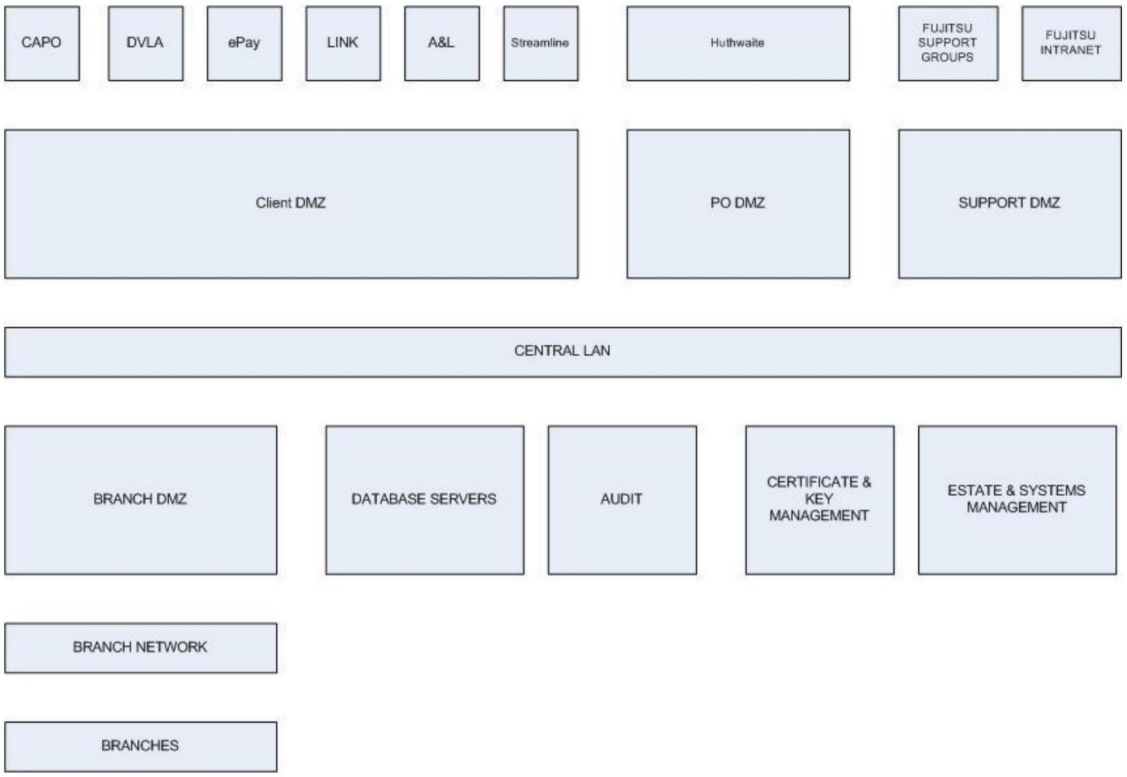


Figure [SEQ Figure * ARABIC] – Security Domains

For example, in the above diagram, to pass from a Counter in a Branch to the Branch Database in the Database Servers domain, will require the traffic to pass through multiple enforcement points; from the personal firewall on the Windows XP Counter to the firewalls between the Branch DMZ domain and the Database Servers domain.

The following systems are in each domain

POL00394877

Domain	Systems
Branches	Counter
Branch Network	Branch Router, WAN Routers
Branch DMZ	Data Centre Routers, Data Centre Firewalls, VPN Termination, Branch Access Layer Application Servers, Branch Router RADIUS Authentication Server, SYSMAN Gateways.
Database Servers	Branch Database, TES, NPS, DRS, TPS, DWh
Audit	Audit Server, Audit Workstation, Audit Atalla Device
Certificate and Key Management	Certificate Server, Key Management System, Signing Server?
Estate and Systems Management	Tivoli, Anti-Virus Server
Support DMZ	RSA Authentication Servers?, SAS Servers
Post Office DMZ	POL MIS, POL FS, TES Application Server
Clients DMZ	Client Agents, Network Banking Atalla Devices?, FTMS Agents.
Central LAN	DNS Servers, Active Directory Servers,

5.2 Platforms and System Layers

The definition of a platform in this document is taken from *HNG-X Architecture - Platforms and Storage* (ARC/PPS/ARC/0001);

Platform Foundation: the combination of HNG-X approved hardware and a HNG-X approved operating system for the purpose of hosting an HNG-X application, service or function in the HNG-X data centre; the platform foundation is provisioned through an automated process

Platform: a type of server hosting a business application or infrastructure service that is part of the HNG-X solution and hosted in the HNG-X data centres, a platform can have multiple instances and is build from a Platform Foundation

Each system or device can be further subdivided into four additional layers and by using these it is possible to define both the functions that take place at that layer and the security strategy for each layer.

The four layers are;

- Application
- Data
- Operating System
- Network

These layers are defined as below;

POL00394877

5.2.1 Application

This is the data processing and presentation layer utilising the services provided by the software and by the other three layers of the model.

The strategy for the application layer is to prevent security incidents by ensuring that data is entered correctly, processed correctly and is validated. This will be achieved through strict control of the application development process and specific application security testing.

Exceptions detected by the application will be logged and an alert raised when the appropriate criteria have been met.

Any passwords stored or transmitted at this level of the architecture must be encrypted or otherwise obscured by using symmetric, (AES, TDES), or asymmetric encryption, (RSA), or by using a salted hash algorithm.

Applications must only run in a user context that provides them with the rights and permissions they need. This applies to COTS and bespoke software and applications.

During the detailed design stage, an analysis will be performed to assess the rights needs for the Counter application, Tivoli agent, SSH daemon and Fujitsu bespoke software to ensure they do not have excessive rights. This analysis will be documented with reasons for the decisions.

When this analysis establishes that administrative or super-user rights are required, their use is permitted.

The hardening process will set the rights and permissions required by the platform.

5.2.2 Data

The data layer is responsible for the storage and management of application, platform and network information.

The principle strategy for this layer is prevention. This will be achieved through the deployment of Database access control with individual role-based accounts for each class of user to restrict the users that can access the database, to control what actions those users can perform and to log all administrative and other human accesses and command execution on a database to ensure an audit trail exists.

Oracle databases will be configured in a secure fashion following the guidance contained in the Oracle Database Security Checklist document attached as Appendix B.

The main classes of users at this level will be;

- Application – Those accounts used by the web services middleware tier to access the Branch Database and accounts used by other systems for database access to either Oracle or SQL Server Databases.
- System Administrators – Those operational support users with responsibility for managing the database systems.
- Database Administrators – Those operational support users with responsibility for specific databases.

For new databases, access for these users will be provisioned and controlled by the Identity and Access Management service. Existing databases will be evaluated on an individual basis.

Application and transaction audit and event data are also managed at this level.

No new SQL Server databases are anticipated for HNG-X however existing SQL Server databases will be reviewed in line with guidance from Microsoft on securing SQL Server.

POL00394877

5.2.3 Operating Systems

The major operating systems in HNG-X are Windows 2003 Server, Red Hat Enterprise Linux 4, Solaris 10 and, during migration, Windows NT4.

Using the security strategy of prevention, containment, detection and response requires that a secure build, (the platform foundation), is created which is suitably hardened by removing unnecessary software from the system, applying the latest relevant patches, setting file, application and user permissions following the guidance in the Vulnerability Management section of this document.

Any passwords stored or transmitted at this level of the architecture will be encrypted or otherwise obscured by using symmetric encryption algorithms such as AES or TDES, asymmetric encryption such as RSA, a seeded hash algorithm or by using a recognised and approved authentication method such as Kerberos. This is in addition to any network layer protection for data transmission.

5.2.4 Network

The network layer provides physical and logical network services for the other three layers. This includes storage area networking.

The strategy for this layer is to prevent attack originating from outside the HNG-X infrastructure through the use of a secure perimeter consisting of firewalls and intrusion detection and prevention.

Attacks within the HNG-X infrastructure will be prevented, contained and detected using network segmentation, access control lists, firewalls, intrusion detection and intrusion prevention security controls.

Each control device or system will log to the Security Event Management service.

Network device access control will be provided by the Identity and Access Management service using RADIUS/TACACS.

5.3 Control Objectives

The control objectives used in this document come from ISO27001 – The International Standard for Information Security Management Systems and are employed as a method of providing a consistent and abstracted approach to solving security issues.

The security requirements of HNG-X are mapped to the appropriate control objectives as documented in Appendix A.

5.4 Documentation Set

Additional documentation will be produced to define the structure and support the design of the HNG-X infrastructure and applications. These documents include topic architecture documents, SRSs, HLDs and LLDs.

5.4.1 Policy

This policy documentation set will include;

1. Principal Policies
    a. Master Security Policy
        i. The master security policy is the top level document of the policy accredited document set, (ADS). This document describes the high-level reasons for information security, the principles to be followed and acts as a master index to

POL00394877

the other policy documents that are created. The audience for this document is all operational users and support personnel together with any third parties wishing to access the HNG-X infrastructure.

b. Access Control Policy

   i. The access control policy is split into two parts – Network access control and Platform access control. The document details the HNG-X policy for managing access to the HNG-X environment including users, passwords, systems, devices, clients and other third parties.

c. Risk Management Policy

   i. Defines and explains risk, threats, threat sources, threat scenarios, vulnerabilities, risks assessment and how and when they should be conducted.

d. Security Test and Acceptance Policy

e. Incident Management Policy

   i. Incident detection, management and response.

f. Vulnerability Management Policy

   i. Malware.

   ii. Patching and updating.

g. Compliance Policy

   i. Regulation – (FSA)

   ii. Legislation – (DPA, RIPA, CMA, FOIA)

   iii. Standards – (ISO27001, PCI)

   iv. Internal Standards and Guidelines – (System Hardening, Database Configuration, Access Control.)

h. Secure Software Development Policy

   i. Principal security considerations and principles.

   ii. Java specific guidance.

   iii. Testing and verification.

5.4.2 Additional Documentation

Additional documentation will be produced to support the development and delivery of the HNG-X solution. These documents include;

#	Document	Description
[AUTONUM * Arabic]	Security Functional Spec	Technical description of the security controls in the HNG-X solution.
[AUTONUM * Arabic]	Topic Architectures	Architecture descriptions of specific areas of the solution
[	High Level Designs	[HLD] Design document describing the next level of detail

POL00394877

#	Document	Description
AUTONUM * Arabic]		down from the architecture documents. There may be multiple HLDs to each architecture document.
[AUTONUM * Arabic]	Low Level Designs	[LLD] Design document describing the next level of detail down from the HLDs. There may be multiple LLDs to each HLD.

5.5 Secure Network Architecture

5.5.1 Service Description

The secure 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 baselining and trending to be performed. The service controls security-related incidents.

The following facilities are supplied by the service;

- Provides secure network capabilities using encrypted Virtual Private Networks, (VPNs).
- Provides secure remote access facilities.
- Provides network segmentation.
- Enables network analysis and reporting.
- Controls and manages network access control.

5.5.2 Requirements

Ref:	Description
SEC-3062	The logical security perimeter of the HNG-X system shall be defined and agreed with Post Office Information Security.
SEC-3150	{CISP 8.5.1a} The Horizon network configuration shall permit traffic to flow between HNG-X and external systems or services only as agreed by PO Ltd.
SEC-3152	{CISP 8.5.1b} Unauthorised logical access from non-Horizon systems and networks shall be prevented. This shall include but shall not be limited to, unauthorised access from any of the following: Any public networks used. Networks connecting to Third Parties. Networks connecting Horizon to PO Ltd and/or Royal Mail Group. Other systems operated by the domain supplier on behalf of itself or other clients.
SEC-3156	{CISP 8.5.1c} Controls shall protect against denial-of-service attacks originating from non-Horizon systems including those listed in Requirement SEC-3152.
SEC-3160	All HNG-X systems shall use private IP addresses which shall not be exposed across the system boundary.
SEC-3162	{CISP 8.5.1e} Network management staff within each domain shall be alerted to any attempt to reach the HNG-X systems in their domain from unauthorised network addresses.
SEC-3165	Individual attempts to breach network security controls shall be treated as a minor security breach. A concerted attempt or a successful breach of network security controls shall be treated as a major security breach.
SEC-3167	{CISP 8.5.1g} Data over Wide Area Networks shall be encrypted unless specifically agreed in the relevant Technical Interface Specification or where otherwise specifically agreed by Post Office Limited Information Security. The Fibre Optic link between Data Centres is not considered to be a Wide Area Network. The

POL00394877

Ref:	Description
	requirement applies to transaction data between branches and the data centre(s).
SEC-3168	WAN Encryption key management shall be independent of network configuration such that the confidentiality of Post Office traffic is not compromised by a single configuration error of either the WAN or the encryption system.
SEC-3169	{CISP 8.5.1h} The system design shall require that no encrypted data is to pass through any HNG-X firewall layer other than certain defined fields in the application level protocol (e.g. encrypted PINs) except where data is subsequently decrypted and passes through another firewall layer. Other cases may be authorised by Post Office Information Security where a risk assessment has identified that the requirement for confidentiality outweighs the requirement for system availability and integrity.
SEC-3170	All proposals for encrypted data to pass through any HNG-X firewall layer shall be subject to risk assessment to determine if the requirement for confidentiality outweighs the requirement for system availability and integrity.
SEC-3172	Cases requiring encrypted data to pass through any HNG-X firewall layer shall only be authorised by Post Office where a risk assessment has identified that the requirement for confidentiality outweighs the requirement for system availability and integrity.
SEC-3174	{CISP 8.5.1j} Test systems shall only share logical network connection with operational systems in carefully controlled circumstances. Test systems shall be configured to connect in this manner for the minimum duration necessary to support testing. The logical connection shall only be permitted after an assessment has confirmed that live operation will not be adversely impacted or as otherwise agreed by Post Office Limited.
SEC-3176	All RADIUS servers that authenticate network access shall be secured and segregated into logical network segments by carrier access method and be externally visible to authorised domain users only.
SEC-3189	{CISP 8.5.1k} The use of wireless technologies within or associated with HNG-X systems or services shall be excluded with the sole exception of mobile public telecommunications services provided by UK licensed public telecommunications operators or as otherwise agreed by Post Office.
SEC-3192	Any mobile backup or secondary network produced within the {CISP 8.5.1k} specification of the requirement shall be secured to the same level as the primary network.

5.5.3 Control Objectives

Ref.	Description
A10.4.1	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.
A10.6.1	Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
A10.6.2	Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.
A10.9.1	Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.
A10.9.2	Information involved in on-line transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
A11.1.1	An access control policy shall be established, documented, and reviewed based on business and security requirements for access.
A11.4.1	Users shall only be provided with access to the services that they have been specifically authorized to use.
A11.4.5	Groups of information services, users, and information systems shall be segregated on networks.
A11.4.6	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business

POL00394877

Ref.	Description
	applications.
A11.4.7	Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.
A11.5.2	All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.
A11.7.1	A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.
A12.6.1	Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

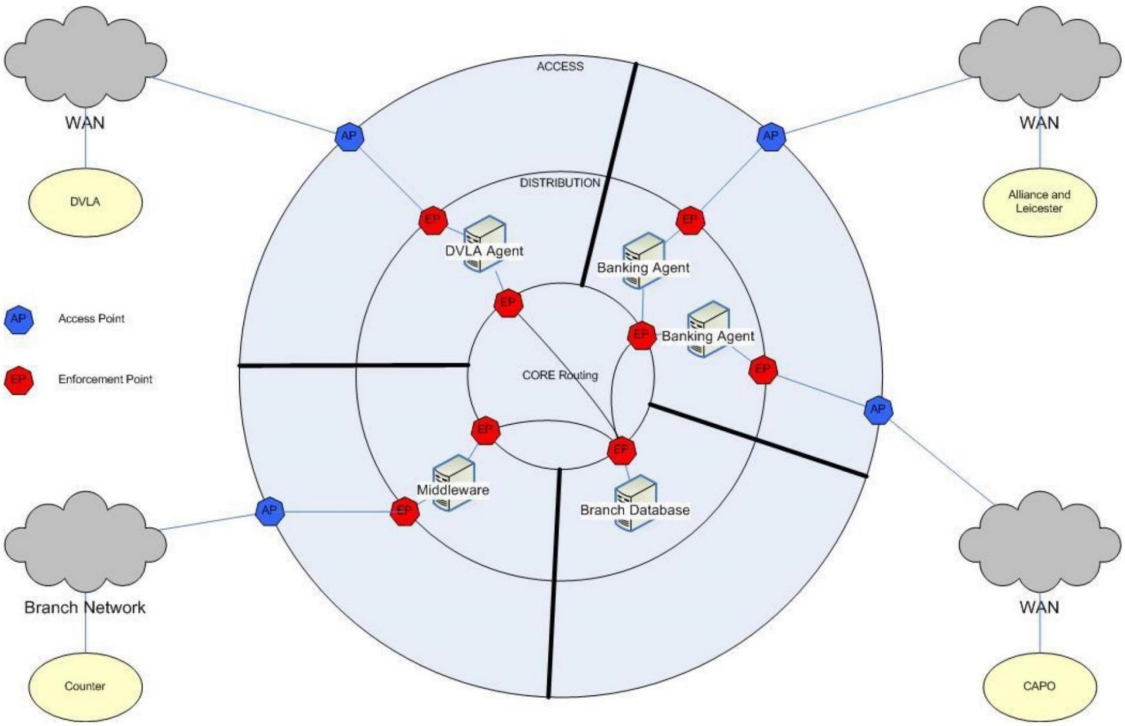
5.5.4 Implementation

There are three main tiers in the network model for HNG-X as illustrated in the diagram;

- Access
- Distribution
- Core

Within each of these tiers there are a number of sub-domains that provide network level access control. Security controls are enforced in the Distribution layer and it is not possible to pass from one sub-domain to another without passing through an enforcement point and the Core.

The Core tier is responsible for intra-data centre routing



POL00394877

Figure [SEQ Figure * ARABIC] – Secure Network Architecture - tiers

5.5.4.1 Intrusion Detection

Network-based intrusion detection is deployed throughout the HNG-X infrastructure, to provide immediate notification of an attempted compromise of the HNG-X infrastructure and systems.

Network IDS appliances will be deployed in the Access tier to provide early warning of attempted intrusion and to block attacks originating using the intrusion prevention capability of the appliances. Appliances will also be deployed in the Distribution tier to protect the core systems of HNG-X and to provide alerts of malicious activity internal to the HNG-X infrastructure.

The appliances will be sized to 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.

Management of the IDS appliances will be provided by Core Services and will be provisioned using a connection to the IMS LAN.

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.

To reduce processing overhead on core HNG-X systems, host based IDS is not being deployed. However, all hosts and network devices will send event logging information to the secure event management service which will process the logs in real-time and raise alerts based on anomalous events in the log files.

5.5.4.2 Counter Support Access

Remote support access to the Counter will be provided through the implementation of an SSH service running on the Counter which can then be accessed from the Secure Access Servers, (SAS), in the Data Centre. The SSH server on the Counter is configured with the SAS Server SSH public keys so that connections to the Counter are restricted to only those originating from the SAS servers. This will allow access to a command prompt on the Counter for the retrieval of logs and other data using secure copy, (SCP).

All support user access will be audited at a command line level to ensure an audit trail of administrator activity is available.

Firewall rules will be configured to ensure that the SSH and SCP traffic can only be initiated from the SAS servers.

Access control for the SAS servers is provided using two-factor authentication by the Identity and Access Management service.

5.5.4.3 Branch Network

From a security perspective, the Branch network is assumed to be insecure and therefore application transaction traffic between the Counter and the Data Centre is encrypted using 128 bit SSL encryption generated using standard Java VM APIs. This connection validates the identity of the Data Centre using the Data Centre certificate and the authorised CA list configured on the Counter.

This connection is established prior to the application login prompt appearing for the user, to ensure that any authentication information is encrypted. For normal business user logon, the password is not transmitted across the network. For password changes, the password is also encrypted independently of the network encryption to ensure protection after this traffic exits the SSL tunnel in the Data Centre.

POL00394877

Post-HNG-X migration Tivoli management traffic will be encrypted using AES256 bit encryption to protect it during transmission and storage.

An IPSEC tunnel will be created between the Data Centre and the Branch Router for management traffic. This tunnel will be initiated when required for management purposes. It will not be possible to connect to the Branch Router for management purposes using anything other than an IPSEC tunnel from the WAN side of the Router. Local access from the Branch LAN is not permitted although access to Router log files stored on one of the Counters, will be provided through the Counter Application.

Network Intrusion Detection/Prevention appliances will be deployed as described in section [REF _Ref152172121 \r \h] [REF _Ref152172121 \h] This will check all traffic from the Branch to the Data Centre after it has been decrypted and all traffic going to the Branch from the Data Centre before it is encrypted. Exceptions to this include SSH traffic originating from the SAS servers to the Counters, however this traffic will be audited at a command line level so that all traffic across this encrypted link will be recorded. Any use of other support tools such as SCP or SFTP will also be recorded to ensure an audit trail is available in the event of an incident. For the purposes of this document it is assumed that this is acceptable to Post Office Information Security and meets the requirement as expressed in SEC-3169 and SEC-3170.

Initially the intrusion prevention features of the appliances will be disabled to ensure that valid traffic isn't blocked. As there will be a limited set of messages coming from the Counter / Branch, the intrusion prevention facility will be tuned during the migration and early months of full operation to further protect the Data Centre. Tuning will be based on the number and type of events noted during this period.

The IDS forwards events to the Security Event Management solution to ensure that alerts are raised quickly and efficiently.

5.6 Secure Branch Access Layer Architecture

5.6.1 Application

Branch users will be authenticated using data in the Branch Database.

Middleware application software will be developed to ensure data are validated on entry to the application where this is established as necessary by risk assessment during development. Field lengths, data types, Counter IDs, session tokens and digital signatures will be checked and only accepted if valid.

The application will be developed to ensure that only valid transaction formats can be processed by the system. This means that attempted buffer overflow and SQL injection style attacks will be blocked. How this will be achieved will be established during detailed design.

The decision as to where and to what extent this validation is done will be established during the design phase, as a result of the risk assessment conducted as part of the software development process adopted for the HNG-X project.

Application passwords will be protected by SSL in transit over public networks. The password is also encrypted independently of the network encryption, (using AES or TDES encryption), to ensure protection after this traffic exits the SSL tunnel in the Data Centre.

Role based accounts will be maintained to provide Database access and these accounts will be configured with only the permissions necessary to perform the functions required by the application.

The application software will be developed using the Java language and will follow coding guidelines expressed in the existing Post Office Account Development Methodology and associated documents.

In particular the software will ensure that data are validated to prevent buffer overflow attacks, SQL Injections attacks, (largely negated through the use of PreparedStatement) and Cross-Site scripting attacks.

POL00394877

5.6.2 Data

- Refer to *HNG-X Branch Access Layer Architecture* (ARC/APP/ARC/0004).

5.6.3 Platform

- Refer to *HNG-X Branch Access Layer Architecture* (ARC/APP/ARC/0004).

5.6.4 Network

- Refer to *HNG-X Branch Access Layer Architecture* (ARC/APP/ARC/0004).

5.7 Secure Database Architecture

5.7.1 Application

For new applications connecting to a new Oracle Database, the connection will be established using an Oracle user configured with the minimum privileges necessary to provide the required functionality. These permissions will be established based on an access control matrix that will be created by the application developers.

These database users will be managed by the Identity and Access management service and will be controlled using an agent installed on the Oracle Database server.

Existing Horizon databases will be migrated 'as-is' with a view to providing access control through the Identity and Access Management service as the systems are upgraded.

- Refer to *HNG-X Host Applications Database Design And Interface Standards* (DES/GEN/STD/0001)
- Refer to *HNG-X Branch Database Architecture* (ARC/APP/ARC/0008)

5.7.2 Data

Existing Horizon databases will be migrated 'as-is' with a view to providing access control through the Identity and Access Management service as the systems are upgraded.

5.7.2.1 Microsoft SQL Server

It is not expected that there will be any new deployments of Microsoft SQL Server in HNG-X. Existing SQL Server databases will be reviewed in line with Microsoft guidance on securing SQL Server.

5.7.2.2 Oracle

New Oracle Databases will be secured following the guidance contained in Appendix B - Oracle Database Security Checklist.

A list of database roles and an access control matrix matching roles to permissions will be established for each new database. The database roles will be consistent across all new databases. Existing databases will be migrated to the new structure during the migration phase.

1) Step 1: Install only what is required.
2) Step 2: Lock and Expire Default User Accounts
3) Step 3: Change Default User Passwords

POL00394877

a) Change default passwords of administrative users
b) Change default passwords of all users
c) Enforce password management

4) Step 4: Enable Data Dictionary Protection
5) Step 5: Practice the principle of least privilege
   a) Grant necessary privileges only
   b) Revoke unnecessary privileges from the public user group
   c) Grant a role to users only if they need all privileges of the role
   d) Restrict permissions on run-time facilities
6) Step 6: Enforce access controls effectively and authenticate clients stringently
   a) Authenticate client properly
7) Step 7: Restrict Operating System Access
8) Step 8: Restrict Network Access
   a) Use a firewall
   b) Protect the Oracle listener
   c) Monitor who accesses your systems
   d) Check network IP addresses
   e) Encrypt network traffic
9) Step 9: Apply all security patches

Database users will be provisioned using the Identity and Access Management.

- Refer to *HNG-X Host Applications Database Design And Interface Standards* (DES/GEN/STD/0001)
- Refer to *HNG-X Branch Database Architecture* (ARC/APP/ARC/0008)

5.7.3 Platform

Database support and operational user access will be controlled using the Identity and Access Management service.

The Oracle Database platform will be hardened following the guidance in the Vulnerability Management section of this document relating to Red Hat Enterprise Linux 4.

Command line auditing of database access will be implemented.

- Refer to *HNG-X Host Applications Database Design And Interface Standards* (DES/GEN/STD/0001)
- Refer to *HNG-X Branch Database Architecture* (ARC/APP/ARC/0008)

5.7.4 Network

- Refer to section [REF _Ref151374713 \r \h] [REF _Ref151374716 \h] in this document.
- Refer to *HNG-X Host Applications Database Design And Interface Standards* (DES/GEN/STD/0001)

POL00394877

5.8 Secure Counter Architecture

5.8.1 Application

To prevent replay attacks, the counter application must use a nonce or seed value that is unique for every transaction. This will prevent an attacker replaying a previously captured transaction as the application server would reject the repeated nonce value.

Data transmission is protected between the Counter application and the Data Centre through the use of SSL. This control encrypts the traffic between the Counter application and the Data Centre thereby protecting the username and logon information as well as transaction information. It also makes a "man in the middle" attack extremely difficult as an attacker would need to obtain a copy of the Data Centre certificate private key in order to intercept the traffic stream.

The Counter will be configured to only accept valid certificates issued by the HNG-X Certificate Authority and will also check for new Certificate Revocation Lists, (CRLs), prior to the establishment of the SSL session with the Data Centre. The CRLs will be distributed using the Tivoli software distribution mechanism when needed.

Application passwords will be protected by SSL in transit over public networks. The password is also encrypted independently of the network encryption, (using AES or TDES encryption), to ensure protection after this traffic exits the SSL tunnel in the Data Centre.

In the development of the login and session management modules of the Counter application standard cryptographic APIs will be used using RSA for digital signatures and using TDES or AES for data encryption.

The Counter Application will use an underlying Windows NT/XP user context that only provides the application with the minimal set of rights and privileges it needs to run.

- Refer to *HNG-X Counter Business Applications Architecture* (ARC/APP/ARC/0009).

5.8.2 Data

The Counter is intended to act effectively as a terminal to the HNG-x system in a complete departure to how the current Riposte system within Horizon operates. As a result the Counter will provide no cryptographic protection of any information within the file-store, nor will business transaction data be written to the local disc.

In addition, local log files will not contain any sensitive data and data written to the platform swap file by the operating system, will be dealt with as detailed in section 5.8.3.1.

- Refer to *HNG-X Counter Business Applications Architecture* (ARC/APP/ARC/0009).

5.8.3 Platform

- Refer to *HNG-X Counter Architecture* (ARC/APP/ARC/0003).

During migration the Counters in use will consist of a reducing estate of existing Horizon Counters and an increasing estate of HNG-X Counters running the HNG-X Counter application and a Java Virtual Machine on a Windows NT platform.

POL00394877

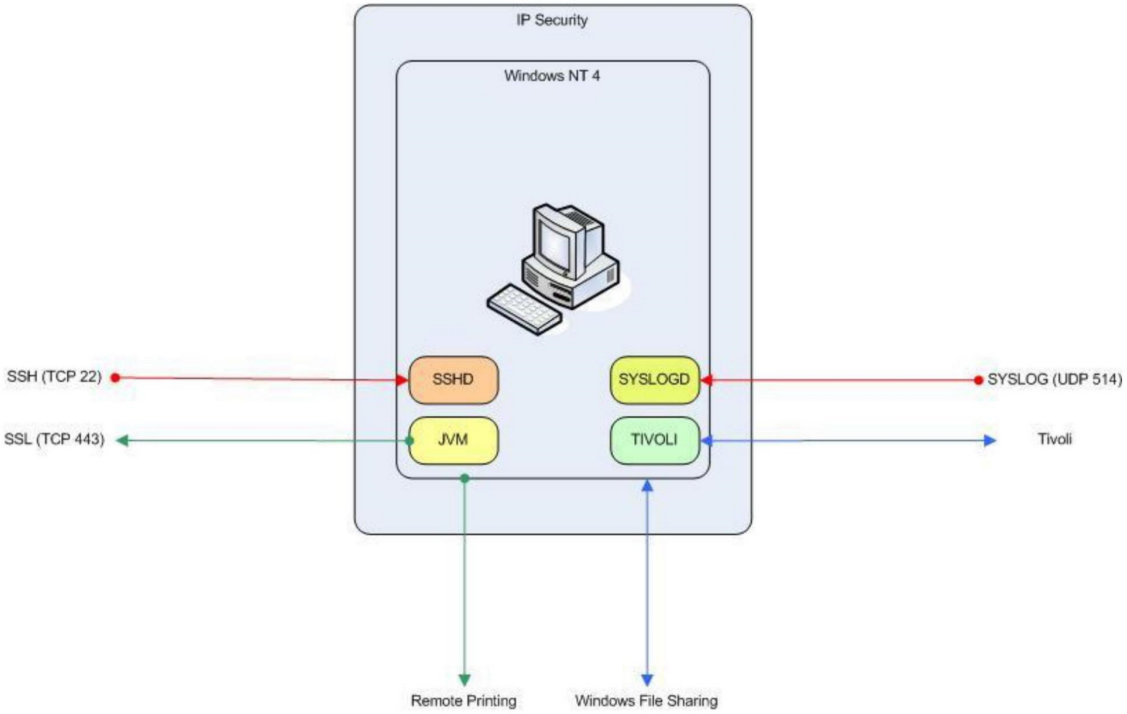


Figure [SEQ Figure * ARABIC] – Windows NT HNG-X Counter

Following full migration the entire estate will be running the HNG-X Counter application and a Java Virtual Machine on a Windows XP platform.

As part of the migration process, once the Windows XP HNG-X Counter system has been fully implemented, any remaining obsolete Windows NT HNG-X Counter information, (applications or data), will be securely overwritten.

Access to the Counter is managed and controlled by the Branch Database and not by the directory service. The Counter is therefore implemented as a stand-alone Windows XP system with no domain membership. This is to ensure the Counter application, middleware and Branch Database are not dependent on an external system for their operation.

With the Branch Database controlling and managing access for the Counter application then the resilience applied to the Branch Database does not need to be repeated on another system as there is no external directory service. In addition, as all business users are dependent on the Branch Database being available for the system to operate, there are no outside dependencies for system availability.

Anti-Virus software is not required on the Counter as the system will be operating in a restricted environment with no access to email or Internet access. The system platform will be hardened using guidance from a number of sources including the *Windows XP Security Guide* and *800-68 Guidance for Securing Microsoft Windows XP Systems* (NIST).

POL00394877

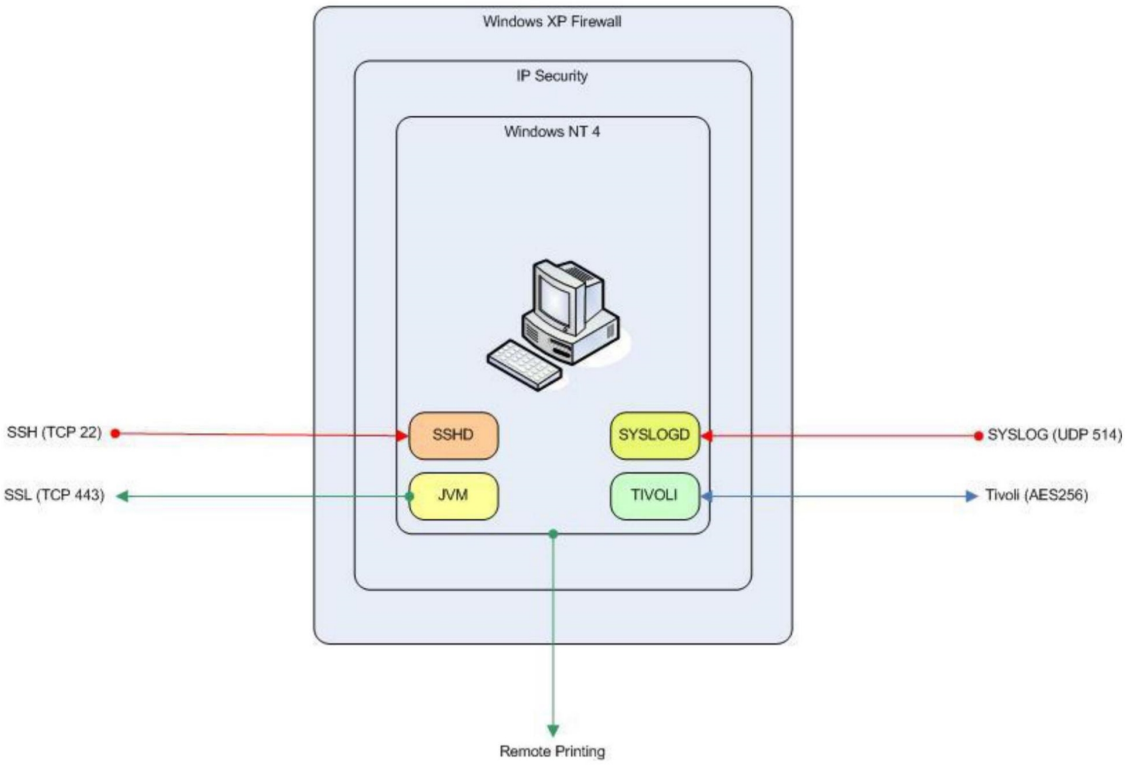


Figure [SEQ Figure * ARABIC] – Windows XP HNG-X Counter

The main features of the hardening process are listed below. Exact details of which services, patches, access rights and permissions will be established during the development of the base secure build for Windows XP and Windows 2003.

1) Counters are configured as stand-alone systems with no domain membership.
2) All unnecessary services and applications are removed.
3) All relevant patches for Windows XP and Java are applied.
4) User rights and permissions are configured to restrict access.
5) Service and application rights and permissions are configured to restrict access.
6) Auditing is turned on including command line auditing for super-user access via SSH. Local access is provided and controlled through the Counter application.
7) IP security is configured to restrict traffic that can access the counter.
8) Personal firewall software configured on each Counter to restrict access to the system from other systems.

Support access to the Counter is provided using SSH from the Data Centre SAS server. This access is secured as described in the Secure Network section of this document.

POL00394877

5.8.3.1 Other Controls

1) Counter application user runs with minimal privileges. The exact privileges required will be established at the design stage.
2) A risk assessment will be performed as part of the detailed design process to establish the extent to which application and system cache, pagefile and other temporary storage areas should be cleared and/or securely overwritten on the Counter. Platform level memory caching is not included in this definition. The system will be configured not to dump memory to disk in the event of a system crash unless forced for operational support purposes. Exact details will again be established during the design phase as a result of risk assessment.
3) No sensitive data such as PINs, PIN blocks or PANs are written to the Counter hard-drive by the application unless necessary for logging. In this case the sensitive data will be obfuscated through over-writing, encryption or hashing by the Counter application. Details of how this will be achieved will be established during the design phase.

5.8.4 Network

1) Private IP addresses, (RFC1918 range), configured for each Counter in a Branch.
2) Branch router firewall configured with basic access control lists to restrict traffic flowing between the Branch and the Data Centre.
3) Personal firewall software configured on each Windows XP Counter that restricts application access and controls which applications can run.
4) SSL encryption is instigated between the Counter and the Data Centre to protect application traffic in transit. This authenticates the Data Centre to the Counter but has no role in authenticating the Counter to the Data Centre.
5) Alerts configured for activated firewall rules.

POL00394877

6 Principal Security Services

ABSTRACT: Lists and describes the principal security services provided for HNG-X. Each principal service is broken down into its key components and described in more detail.

The services below are used by the component parts of HNG-X and by each other to provide and deliver security functionality.

6.1 Identity and Access Management

6.1.1 Service Description

The identity and access management service provides facilities to create, modify and remove users, groups, roles and access permissions. The service controls access at an application and platform level including both local and remote access. This includes access to operational support, system support and data processing systems.

Management in the following list means provisioning, de-provisioning, authenticating and authorising;

1) Operational support users are managed using a directory service.
2) Branch business user access is managed using the Branch Database. This includes Engineers on site visits to the Branch.
3) Accounts used solely by applications are provisioned using the directory service but are not authenticated and authorised by the service. These are local accounts to the system being accessed. (For example, local database accounts used by the Branch Access Layer to access the Branch Database. These accounts will be provisioned using the directory service and a script to create the users, as local users, in the Branch Database.)

The following facilities are supplied by the service;

- Provides identification
- Provides authentication
- Provides authorisation
- Provides accounting.
- Provides non-repudiation
- Provide role based access control.
- Provides network access control.
- Enables the addition, removal and change of users, groups and roles.
- Enables the addition, removal and change of network systems and devices.
- Enables segregation of duties.
- Controls and enables local and remote access for HNG-X.

6.1.2 Implementation

The service is implemented using a number of different technologies and is split between business users and operational users.

POL00394877

Business users are defined as those users that utilise the functionality of the system from Post Office or Royal Mail locations or on behalf of the Post Office to perform a business function.

Operational users are defined as those users that provide operational support and management of the HNG-X system itself.

6.1.2.1 Branch Users

These are users of the Counter Application such as the Sub-Postmaster and Counter Clerk.

6.1.2.1.1 Requirements

Ref:	Description
SEC-3199	Logon to Counter Terminals must provide equivalent security to that provided by logon via native operating systems.
SEC-3203	The Horizon Access Control Policy RS/POL/003 shall apply but shall be updated to reflect the change in policy due to HNG-X or other agreed security requirements.
SEC-3204	Such update shall include at least the following password requirements: Minimum password length of 7, Minimum password history length of 4
SEC-3207	Branch Terminals shall include a single user action that, in between customer sessions, cleanly terminates the clerk session and presents a new clerk login screen. During a customer session, the clerk must first complete or cancel the session in accordance with business rules.
SEC-3209	HNG-X shall have controls in place to prevent user bypass of the standard application.

6.1.2.1.2 Control Objectives

Ref:	Control Objective
A11.1.1	An access control policy shall be established, documented, and reviewed based on business and security requirements for access.
A11.2.1	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.
A11.2.2	The allocation and use of privileges shall be restricted and controlled.
A11.2.3	The allocation of passwords shall be controlled through a formal management process.
A11.2.4	Management shall review users' access rights at regular intervals using a formal process.
A11.3.1	Users shall be required to follow good security practices in the selection and use of passwords.
A11.4.1	Users shall only be provided with access to the services that they have been specifically authorized to use.
A11.5.1	Access to operating systems shall be controlled by a secure log on procedure.
A11.5.2	All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.
A11.6.1	Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.

POL00394877

6.1.2.1.3 Authentication and Authorisation

Branch user authentication and authorisation is a function of the Counter, Branch Access Layer and the Branch Database. This is to ensure that the line of business application is a closed functional group where the components of the group, (namely the Counter Application, the application server and the Branch Database), are not dependent on other components for their operation.

Refer to Section 2.4.5 - Authentication/Authorisation Architecture in *HNG-X Branch Access Layer Architecture* (ARC/APP/ARC/0004) for a description of the authentication / authorisation process.

6.1.2.2 Operational / Support / Other Business User

These users are the customer service, third-party support and remote business users of the system such as SSC, SMG, other third-parties and users of systems such as TES-QA.

6.1.2.2.1 Requirements

Ref:	Description
SEC-3203	The Horizon Access Control Policy RS/POL/003 shall apply but shall be updated to reflect the change in policy due to HNG-X or other agreed security requirements.
SEC-3204	Such update shall include at least the following password requirements: Minimum password length of 7, Minimum password history length of 4
SEC-3211	It shall not be possible to install any application or operating system extension except under the control of properly authorised and authenticated systems administrators carrying out authorised and audited changes.

6.1.2.2.2 Control Objectives

Ref:	Control Objective
A11.1.1	An access control policy shall be established, documented, and reviewed based on business and security requirements for access.
A11.2.1	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.
A11.2.2	The allocation and use of privileges shall be restricted and controlled.
A11.2.3	The allocation of passwords shall be controlled through a formal management process.
A11.2.4	Management shall review users' access rights at regular intervals using a formal process.
A11.3.1	Users shall be required to follow good security practices in the selection and use of passwords.
A11.4.1	Users shall only be provided with access to the services that they have been specifically authorized to use.
A11.5.1	Access to operating systems shall be controlled by a secure log on procedure.
A11.5.2	All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.
A11.6.1	Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.

POL00394877

6.1.2.2.3 Authentication and Authorisation

Throughout the HNG-X infrastructure the same authoritative source of authentication and authorisation data is used to manage access control for operational users. The purpose of this approach is to:

1) Reduce the number of passwords required for support purposes
2) Ensure better audit and logging facilities for authentication and authorisation
3) Streamline the process for adding, changing and removing authentication and authorisation information
4) Provide a standard API to applications
5) Provide a standard method of authentication and authorisation throughout the estate.

To facilitate this approach a number of assumptions have been made. These assumptions are subject to confirmation during the detailed design stage;

- Kerberos will be used for Authentication.
  - This ensures that password details are never transmitted in the clear over the network, both at initial logon and when subsequently accessing system and network resources.
- LDAP will be used for Authorisation.
  - This provides fine-grained role-based authorisation.
- Windows 2003 Active Directory will be used for the Windows estate, (Excluding Counters).
- The proposed approach will offer satisfactory performance. This will be established during the detailed design phase.
- The system will be designed to be resilient and available. Details of the technologies to be used will be established during the design phase.
- Solaris 10 and Red Hat Enterprise Linux systems will authenticate using a PAM through the Windows Active Directory service.

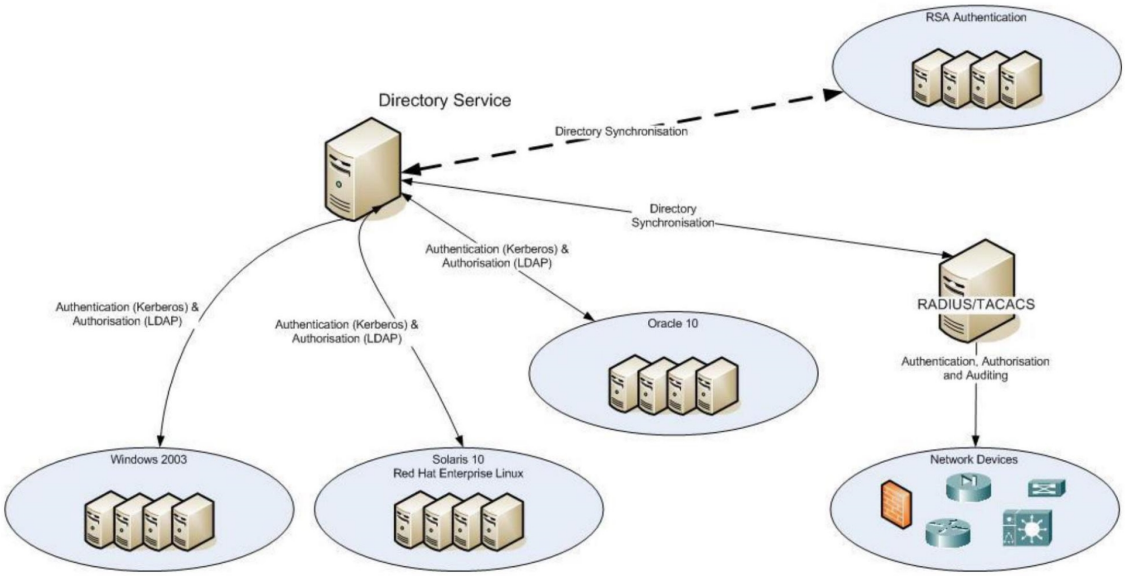


Figure [SEQ Figure * ARABIC] – Operational User Authentication and Authorisation

POL00394877

The Windows environment is managed using an active directory tree which controls access to resources through the Windows 2003 Kerberos and LDAP implementations.

The UNIX environment is managed through the same Active Directory tree utilising a Pluggable Authentication Module, (PAM), installed on each UNIX system.

Access to databases systems is provisioned using the Identity and Access Management service. Database access is provided through the implementation of scripts to create database users using the underlying OS user as a source.

This approach means that the Oracle Advanced Security option is not required for each database, but does mean that a role-based access control matrix will need to be created for each database using a standard set of roles across all databases.

Remote access using two factor authentication will be provisioned through the RSA Authentication Server as for Horizon. The RSA Authentication Server will synchronise with the directory service to ensure user data are up to date and consistent.

All administrative and super-user access to any component of a platform will also be controlled using two-factor authentication.

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

Platform event information detailing account logons & logoffs, object access, account management, privilege use and directory service access, (and their failures), are all logged using the Event and Incident Management service.

Network shares will also use the directory service for authentication and authorisation.

6.2 Secure Event Management Service

6.2.1 Service Description

The secure event management service acts as a subsystem of the overall event management solution. There are two alternative approaches to be explored during the detailed design phase;

1) Through the deployment of log analysis and event correlation appliances and software, (currently expected to be Tivoli Security Operations Manager or Network Intelligence appliances), logs will be fed from the main event management system using a database link to aggregate and analyze device log information.

2) Through the enhancement of the existing event management system to include logs from all platforms and devices in the HNG-X infrastructure, (including firewalls, IDS/IPS systems and the Identity and Access Management System), with the addition of a reporting capability using appropriate software.

The following facilities are supplied by the service;

- Provides log aggregation, correlation and analysis.
- Enables security event alerting and reporting.
- Enables compliance reporting with standards and regulation such as ISO 27001.

POL00394877

6.2.2 Requirements

Ref:	Description
SEC-3162	{CISP 8.5.1e} Network management staff within each domain shall be alerted to any attempt to reach the HNG-X systems in their domain from unauthorised network addresses.

6.2.3 Control Objectives

Ref.	Description
A.10.10.1	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.
A.10.10.2	Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.
A.10.10.3	Logging facilities and log information shall be protected against tampering and unauthorized access.
A.10.10.4	System administrator and system operator activities shall be logged.
A.10.10.5	Faults shall be logged, analyzed, and appropriate action taken.
A.13.2.3	Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

6.2.4 Implementation

Security Event and Information Management, (SEIM), is a key detective control in the HNG-X security strategy acting as a central aggregation point for logs from all network devices, (such as switches and routers), security devices, (such as firewalls, VPN terminators and the IDS), platforms, (Windows 2003, Red Hat Enterprise Linux and Solaris 10) and Database, (Oracle 10g).

This solution works together with the SYSMAN event management solution to provide security related intelligence in the analysis, alerting and reporting of log event information.

This service utilises the existing Tivoli event management infrastructure to forward critical security events in real-time and less critical events as a batched process

Platform / Application	Method
Windows 2003	Tivoli
Windows NT	Tivoli
Red Hat Enterprise Linux	Tivoli
Solaris 10	Tivoli
Oracle	Tivoli
Network Devices, (inc. IDS), and Firewalls	Syslog

POL00394877

Event analysis and alerting take place in real-time and detailed event correlation reduces the number of events seen by the operator.

Events to be logged will be established during the design phase however it is necessary to ensure that the following are included in the logging set on all relevant devices and systems;

Systems	Log Information
Firewalls / Routers with Access Control Lists	Packet Accepts Packet Drops Config Changes Successful user logon and logoff. Failed user logon and logoff.
Windows 2003 / Solaris 10 / Red Hat Linux / Oracle 10	Successful user logon and logoff. Failed user logon and logoff. Permission changes User additions / Deletions

Reporting from the secure event management solution will be used to spot trends, carefully crafted attacks taking place over a long period of time and for reporting to provide compliance with regulation, legislation and standards.

The event management infrastructure will be replicated in the DR/Test Data Centre.

- Refer to *System and Estate Management – Overall Architecture (*ARC/SYM/ARC/0001)
- Refer to *HNG-X System and Estate Management Monitoring* (ARC/SYM/ARC/0003)

6.3 Information Integrity and Confidentiality.

6.3.1 Service Description

The information integrity and confidentiality service ensures that sensitive and personal information is protected in an appropriate fashion for the appropriate length of time in both transit and storage. In conjunction with the identity and access management service the service controls the visibility of information throughout the HNG-X infrastructure and beyond.

The following facilities are supplied by the service;

- Provides a Certificate Authority
- Provides secure key generation, distribution and management
- Enables non-repudiation.
- Enables secure communications.
- Enables data confidentiality and integrity.

POL00394877

6.3.2 Requirements

Ref:	Description
SEC-3168	WAN Encryption key management shall be independent of network configuration such that the confidentiality of Post Office traffic is not compromised by a single configuration error of either the WAN or the encryption system.
SEC-3216	Once entered by a cardholder, plain text PINs shall be processed only in a physically secure device as defined in ISO 9564. At all other times, PINs shall be encrypted as defined in ISO 9564.
SEC-3217	Any new PIN processing devices at Data Centres must also comply with FIPS 140-2 Level 3 [DN: This is a LINK requirement - we have a concession for the present Atalla modules but Post Office Limited cannot guarantee it will be renewed if the modules are replaced as part of HNG-X].
SEC-3218	Any cryptographic key knowledge of which could directly or indirectly reveal plain text PINs must be managed in accordance with ISO 11568
SEC-3219	PIN encipherment keys must not be used for any other cryptographic purpose.
SEC-3235	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 HNG-X Business Data, Reference Data or Application Software unless otherwise agreed with Post Office Information Security. Note: Post Office is highly unlikely to agree to any shorter keys lengths (even for COTS products). For the avoidance of doubt, access to the TES Query service is not covered by this requirement but by requirement SEC-3236.

6.3.3 Control Objectives

Ref.	Description
A12.3.1	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
A12.3.2	Key management shall be in place to support the organization's use of cryptographic techniques.
A.12.3.1	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
A.12.3.2	Key management shall be in place to support the organization's use of cryptographic techniques.
A15.1.6	Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.

6.3.4 Implementation

There are two main components of the Information Integrity and Confidentiality service;

1) Key Management and Distribution
2) Certificate Management and Distribution

For management of keys and certificates for;

1) Data Centre certificates, (RSA - asymmetric)
2) PIN block and PIN pad.
3) Data encryption, (AES or TDES).
4) Network Banking.
5) Application code signing, (RSA - asymmetric).
6) SSH Support
7) IPSEC keys for Branch Router management.

POL00394877

8) Tivoli encryption, (AES or TDES)
9) Router CHAP secrets.

A Certificate Authority, (CA), server will be implemented on an isolated network segment, (using firewall rules), for the generation of Data Centre SSL certificates. These certificates will be used for identifying the Data Centre to the Counter.

The certificate generated will have a lifetime of a maximum of 12 months and will be an RSA asymmetric key pair, this will be confirmed during the detailed design stage.

If required, i.e. In the event of a Data Centre Certificate compromise or the creation of another valid certificate due to a compromise of the CA, a Certificate Revocation List, (CRL), will be distributed to the entire Counter estate using Tivoli. Counters will be configured to check the certificate's issuing CA against an internal approved CAs list and also against the CRL.

The certificate will then be stored at the SSL termination point.

A Key Management workstation, (KMNg), will be created to manage cryptographic keys.

Automatic key management may be required to facilitate Tivoli software distribution.

Both the CA and the KMNg will be implemented on an isolated network in a physically secured area. Logical access to the systems will be controlled and administered using the Identity and Access Management Service. Console access will be the only way of using the CA and remote access will not be possible.

All actions performed on the system will be recorded to establish an audit trail.

6.4 Vulnerability Management

6.4.1 Service Description

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, 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 intrusion detection, prevention and logging.
- Provides vulnerability management.
- Provides patch management.
- Provides malware management.
- Maintains asset database
- Controls vulnerabilities within HNG-X.

POL00394877

6.4.2 Requirements

Ref:	Description
SEC-3129	All hosts and terminals carrying Operational Business data shall be protected on an ongoing basis against malware attacks. Such protection shall be demonstrated in the design to be commensurate with the risk as anticipated by Fujitsu.
SEC-3133	All new developments will protect databases from SQL injection attacks mounted through data centre perimeter controls such as firewalls.
SEC-3137	A risk assessment will be undertaken for retained functionality in the area of SQL injection attacks under HNG-X.
SEC-3138	Risks identified in the area of SQL injection attacks will be managed under Change Control
SEC-3185	The provision of messaging capability shall not permit active or scripted code to be carried within the message body that may be executed upon Branch Terminals or intermediate systems.
SEC-3187	The HNG-X messaging system shall not permit messages to carry any attachments except where such attachments have been specifically validated by Post Office Information Security.

6.4.3 Control Objectives

Ref.	Description
A.7.1.1	All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.
A10.4.1	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.
A.10.4.2	Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.
A12.6.1	Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

6.4.4 Implementation

The purpose of the hardening process is to remove unnecessary services and applications thereby reducing the vulnerability of the system and reducing the operational overhead in maintaining the system

6.4.4.1 System Hardening

The main features of the hardening process are listed below. Exact details of which services, patches, access rights and permissions will be established during the development of the base secure build for each operating system. Generic hardening steps are;

1) All unnecessary services and applications are disabled and removed.
2) All relevant patches for the platform foundation are applied.
3) User rights and permissions are configured to restrict access using the 'least privilege' principle.
4) Service and application rights and permissions are configured to restrict access using the 'least privilege' principle.
5) Auditing is turned on including command line auditing for remote and console super-user access.

POL00394877

6) IP level security is configured to restrict traffic that can access the counter.

Following hardening of the platform foundation, an additional hardening step will be undertaken, when necessary, to harden the platform. This will involve hardening instructions relating to Oracle and SQL Server databases for example.

Guidance from the following sources will be used to establish secure platform foundation builds for each operating system.

Guidance	Applies To
Windows XP Security Guide v2.2 for Windows XP	Counter
Windows 2003 Security Guide for Windows 2003	Windows 2003 Servers
Solaris Security Toolkit v4.2	Solaris 10.
Red Hat Enterprise Linux 4 Security Guide	Red Hat Enterprise Linux 4
Fujitsu secure base-build for Windows NT4	Windows NT4
Oracle Database Security Checklist	Oracle 10

- A base secure platform foundation will be established for each operating system.
- Antivirus software will be installed on all server platforms to mitigate the risk of malware.
- Platforms will log to the Security Event Management service for real-time event correlation, analysis and alerting.
- Platform access control will be provided by the Identity and Access Management service.

6.4.4.2 Anti-Malware

An asset database will be maintained to record system configurations including system patch levels. This will enable the relevance of newly released vulnerability alerts and patches to be efficiently assessed for relevance and impact.

A Sophos anti-virus client will be installed on all server systems. The clients will be configured to perform real-time analysis of files as they are accessed and processed by the system. Alerts raised by the clients will be forwarded to the Secure Event Management Service. The detailed design process will establish precisely the parameters needed for this process.

Anti-virus engine and signature updates will be distributed using the Sophos management console following testing. These updates will be scheduled to avoid peak usage periods. It is not expected that anti-virus signature updates will require significant testing.

The policy for dealing with malware will be based on the prevention, containment, detection and response model. This is intended to reduce the impact of a malware outbreak and to ensure the HNG-X system continues to operate.

Anti-virus will not be installed on Counters as compensating controls will be used to protect the Counter and to contain the spread of any malicious code. These compensating controls are;

1) Hardened operating system
2) For Windows XP - Windows firewall configured to permit only the following traffic
   a) Inbound – Tivoli, SSH from SAS Server, Syslog from Branch Router. Remote printing (on gateway system only).

POL00394877

b) Outbound – Tivoli, Remote printing, SSL from application.

3) For Windows NT - Windows TCP/IP security parameters configured to permit only the following traffic

   a) Inbound – Tivoli, SSH from SAS Server, Syslog from Branch Router. Remote printing (on gateway system only).

   b) Outbound – Tivoli, Remote printing, Windows shares, SSL from application.

4) Branch and Data centre routers configured with access control lists to restrict traffic flow.

5) Data Centre firewall rule-sets configured to only allow application and management related traffic.

6) Intrusion detection/prevention implemented in the Data Centre.

These compensating controls are designed to prevent the spread of malware both within the Branch and from the Branch to the Data Centre.

Intrusion detection is deployed throughout the HNG-X infrastructure using a managed service provided by Fujitsu Core Services, to provide immediate notification of an attempted compromise of the HNG-X infrastructure and systems.

Network intrusion detection sensors will be deployed throughout the network infrastructure to detect and alert of potentially malicious activity.

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

To reduce processing overhead on core HNG-X systems, host based IDS is not being deployed. However, all hosts and network devices will send event logging information to the secure event management service which will process the logs in real-time and raise alerts based on anomalous events in the log files.

6.4.4.3 Patch and Vulnerability Management

Patch and vulnerability management is a key preventive control is ensuring that the exposure level of a system, application or device is reduced to an acceptable level.

This process will be managed by the CS Operational Security Management team and Test.

This service will ensure that an asset database is maintained, notification of relevant patches is obtained, relevant patches are obtained, tested and applied to the live environment in an acceptable timeframe.

A process for evaluation and application of security patches will be established that will differentiate between critical security patches and others.

All other patches will be assessed and those that need to be deployed will be tested and applied on a quarterly or six-monthly basis. The exact timeframes for this will be established during the detailed design process.

For Migration, HNG-X migrated systems will be subject to the new regime. Horizon systems will continue as for current Horizon policy.

POL00394877

6.5 Operational Security Management

6.5.1 Service Description

The operational security management service works with all other services to ensure the security of HNG-X is maintained at the appropriate level. This service supplies the day-to-day support necessary to ensure HNG-X operates securely.

The following facilities are supplied by the service;

- Provides security testing of code, systems and infrastructure.
- Provides Policy, Procedure, Standards and Guidelines.
- Provides Compliance advice on Regulation, Legislation and Standards.
- Provides change management.
- Provides prosecution support.
- Enables migration, implementation and change.
- Controls and enables the operational security management of HNG-X.

6.5.2 Requirements

Ref.	Description
SEC-3062	The logical security perimeter of the HNG-X system shall be defined and agreed with Post Office Information Security.
SEC-3076	Fujitsu Services shall produce and manage development, changes, enhancements and modifications to their systems, architectures and security-related policies in line with the controls and recommendations contained within BS7799-2:2002 / ISO17799 and its successors, as they are embedded in Fujitsu's working practices.
SEC-3092	Fujitsu Services shall update the Horizon Security Policy (RS/POL/002) to reflect the agreed risk profile of HNG-X (see SEC- 3082). In all other respects, the revised Security Policy shall be consistent with the latest version of the Policy. Fujitsu shall previously have updated the Policy to include those aspects of the ISO1779 control framework currently missing from the Policy. Such update shall reflect current Fujitsu and Post Office policies and practice applied to Horizon.
SEC-3095	Fujitsu shall be responsible for reporting to Post Office Limited, investigating and resolving security incidents within their own domain that present an actual or potential threat to the HNG-X environment or to any of the organisations whose data is processed by HNG-X.
SEC-3242	Prosecution support shall continue to be provided as at present.
SEC-3255	Prior to being allowed access to any systems processing Post Office data, all Fujitsu staff shall be subject to an appropriate level of vetting using criteria approved and provided by Fujitsu Services Group Security. This must include checks on their identity, qualifications and financial circumstances. Criminal record checks must be performed where legally permitted. Business and personal references must also be checked

6.5.3 Control Objectives

6.5.4 Implementation

Performs day to day operational security management including vetting of staff, approving access to HNG-X systems, prosecution support, key management and managing security incidents.

POL00394877

#	Item	Description
1	Maintain Security Policy	Maintaining the HNG-X security policy document set. Responsible for updating, distributing, educating and auditing compliance with the policies and standards in the document set. Maintaining the HNG-X policies, standards, procedures and guidelines document management process.
2	Legislation	Review and analysis of existing legislation, in conjunction with Commercial and Legal, as it relates to HNG-X including Data Protection Act, Police & Criminal Evidence Act, Regulation of Investigatory Powers Act and FSA Regulation.
3	Penetration Testing	Regular penetration and vulnerability testing of infrastructure, applications and systems.
4	Security Audits	Regular assessment of compliance with security standards for processes and system builds.
5	Security Awareness	Education programmes for POA and for POL
6	Change Control	Impact and management of security related change.
7	Problem Management	Investigation and resolution of security related problems.
8	Security Operations	Event Management, Incident Reporting
9	Automatic Key Management	Horizon KMA and HNG-X KMNg management and event management during Migration. HNG-X KMNG management post-migration.
10	Manual Key Production	AP Clients, AZMK, BDK, IE, Rambutan, (Migration)
11	Audit Data Retrieval	ARQ, Witness Statements, Adhoc Requests, Call Log Analysis. Training Record Analysis, Investigation and Support
12	Mal-ware and Vulnerability management	Managing vulnerability alerts, distributing for analysis and impact, scheduling testing and arranging implementation. Managing the implementation, update and maintenance of anti-malware controls such as anti-virus.
13	Horizon Pass Management	Managing applications, vetting applicants, issuing passes and recording details of engineers that need to go counter side to work.
15	POA Vetting Process	Vetting staff for security clearance.
15	Live System Access Management	Managing the process for adding and removing users to the live system through the Identity and Access Management Service.
16	OOH process management	Managing the process for providing out-of-hours and remote access to the Horizon and HNG-X infrastructure and systems.

The security management team will be responsible for reviewing change controls relating to firewall configuration and rule changes. This will be to ensure that an overall view of the change is taken and therefore reduce the number of firewall rules implemented on any single firewall.

A risk management method will be chosen for the security management team to use to evaluate the impact of security related changes and projects.

POL00394877

The security management team will also be responsible for creating and managing an incident management policy to ensure that the response part of the prevention – containment – detection – response strategy is in place.

POL00394877

A Appendix A – Mapping of NFRs to ISO27001 Control Objectives

ID	Requirement	Mapping to ISO27001 Control Objectives
	Overarching	
SEC-3058	By provision of an appropriate architecture for HNG-X and associated service operation, Fujitsu Services shall protect Post Office from liability for information security threats to a similar extent that Post Office is protected by Baseline Horizon unless otherwise required by PO Ltd	All BS7799:2/ISO270001 Controls
	Architectural Deltas	
SEC-3062	The logical security perimeter of the HNG-X system shall be defined and agreed with Post Office Information Security.	A10.8.5 Business information systems
SEC-3068	Fujitsu will inform PO Information Security of any changes to the solution that are likely to have an impact upon security.	A10.1.2 Changes to information processing facilities and systems shall be controlled.
SEC-3069	Individual digital signing of individual transactions shall be replaced with user session based authentication, initially using user name and password.	A10.9.2 Information involved in on-line transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. A11.5.1 Access to operating systems shall be controlled by a secure log-on procedure. A11.5.2 All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.
SEC-3073	The security constraints for each HNG-X transaction shall be specified by means of business rules expressed in Reference Data/Code. This Data/Code shall be managed in a way that ensures the security of the Reference Data / Code.	A10.9.2 Information involved in on-line transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. A12.1.1 Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.

POL00394877

ID	Requirement	Mapping to ISO27001 Control Objectives
SEC-3076	Fujitsu Services shall produce and manage development, changes, enhancements and modifications to their systems, architectures and security-related policies in line with the controls and recommendations contained within BS7799-2:2002 / ISO17799 and its successors, as they are embedded in Fujitsu's working practices.	A10.1.2 Changes to information processing facilities and systems shall be controlled.
SEC-3078	Fujitsu Services shall allow all system security functionality to be audited against Post Office Security policies and Standards, including the current support for preparation of the annual LiNK security statement.	A10.10.1 Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring. A10.10.2 Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly. A10.10.3 Logging facilities and log information shall be protected against tampering and unauthorized access. A10.10.4 System administrator and system operator activities shall be logged. A10.10.5 Faults shall be logged, analyzed, and appropriate action taken. A15.2.2 Information systems shall be regularly checked for compliance with security implementation standards. A15.3.1 Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.
SEC-3080	Fujitsu Services shall allow all subsequent additions, deletions, modifications and updates to be re-audited and the security requirements and concomitant measures shall be re-visited if necessary. Any costs or changes to HNG-X will be agreed between the parties.	As SEC-3078
SEC-3082	The security measures appropriate for HNG-X, including those appropriate during the migration from Baseline Horizon, shall be determined by Fujitsu Services by means of a HNG-X System Risk Assessment which covers the HNG-X Service Domain. It is recognised this may increase costs if the scope of the contract is extended.	A7.1.1 All assets shall be clearly identified and an inventory of all important assets drawn up and maintained. A14.1.2 Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.

POL00394877

ID	Requirement	Mapping to ISO27001 Control Objectives
SEC-3084	The preparation of the HNG-X System Risk Assessment shall be the responsibility of Fujitsu Services and approved by the Post Office Information Security.	As SEC-3082
SEC-3086	Based on the System and Business Risk Assessments, Post Office and Fujitsu Services shall work together to agree appropriate countermeasures commensurate with the value and nature of the business risk. It is recognised this may increase costs if the scope of the contract is extended.	As SEC-3082 A12.1.1 Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls. A14.1.2 Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.
SEC-3087	When determining any changes to security measures for HNG-X compared with those in Baseline Horizon, Fujitsu Services shall take account of the System Risk Assessment.	A10.1.2 Changes to information processing facilities and systems shall be controlled.
	Liability	
SEC-3092	Fujitsu Services shall update the Horizon Security Policy (RS/POL/002) to reflect the agreed risk profile of HNG-X (see SEC-3082). In all other respects, the revised Security Policy shall be consistent with the latest version of the Policy. Fujitsu shall previously have updated the Policy to include those aspects of the ISO1779 control framework currently missing from the Policy. Such update shall reflect current Fujitsu and Post Office policies and practice applied to Horizon.	A5.1.1 An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties. A5.1.2 The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
SEC-3095	Fujitsu shall be responsible for reporting to Post Office Limited, investigating and resolving security incidents within their own domain that present an actual or potential threat to the HNG-X environment or to any of the organisations whose data is processed by HNG-X.	A10.10.1 Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring. A10.10.2 Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly. A10.10.5 Faults shall be logged, analyzed, and appropriate action taken. A13.1.1 Information security events shall be reported through appropriate management channels as quickly as possible.

POL00394877

ID	Requirement	Mapping to ISO27001 Control Objectives
	Security Organisation	
SEC-3100	Third Party access requirements shall not apply to access by Fujitsu Post Office Account Support Staff that access the system from the operational support centres, or via a network with remote access secured using encryption and 2 factor authentication.	A10.6.1 Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. A10.6.2 Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced. A11.1.1 An access control policy shall be established, documented, and reviewed based on business and security requirements for access. A11.7.1 A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.
SEC-3102	Fujitsu shall apply all reasonable endeavours to ensure all third parties suppliers for HNG-X allow all system security functionality to be audited against good practice as exemplified by BS7799-2, ISO17799 and its successors.	A10.2.1 It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party. A10.2.2 The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.
	Outsourcing	

POL00394877

ID	Requirement	Mapping to ISO27001 Control Objectives
SEC-3107	Fujitsu Services shall, at their own cost, perform a 'Due Diligence assessment' on any potential offshore developer to be used on HNG-X. The outcome of this 'DD assessment' will be used by FS to assure POL that acceptable standards of physical, logical and management security are followed by the proposed developer or resource. Before any work is placed with the proposed developer or resource, FS shall secure notification that the results of this 'DD assessment' are acceptable to both Post Office and Royal Mail Group Information Security functions. Commercially sensitive information that cannot be shared shall be in a separate document or annex.	A6.1.5 Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed. A6.2.3 Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements. A8.1.1 Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy. A8.1.2 Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. A10.2.1 It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party. A10.7.3 Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse. A10.7.4 System documentation shall be protected against unauthorized access. A12.4.3 Access to program source code shall be restricted.A12.5.5 Outsourced software development shall be supervised and monitored by the organization
	Equipment Security	
SEC-3110	Fujitsu Services shall provide a list of measures that will be taken to mitigate the risk of unauthorised devices being connected to any component of the HNG-X system, with the exception of passive devices within the Branch.	A10.6.1 Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

POL00394877

ID	Requirement	Mapping to ISO27001 Control Objectives
SEC-3114	Branch Terminals shall be bootable only from their primary mass storage device on the terminal.	A11.6.2 Sensitive systems shall have a dedicated (isolated) computing environment.
SEC-3117	FS shall define the content and security status of all data that will be stored locally on terminals (e.g. on HDD) to enable the determination of appropriate security measures.	A7.2.1 Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization. A7.2.2 An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.
SEC-3118	The secure filestore in configured Horizon terminals shall be deleted on migration to HNG-X. Any terminal which is not migrated (e.g. it is taken out of service instead) shall have its filestore deleted in accordance with current procedures.	A9.2.6 All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. A10.7.2 Media shall be disposed of securely and safely when no longer required, using formal procedures. A10.7.3 Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.
	Clear Desk and Clear Screen	
SEC-3124	Any Branch Terminal shall include a single user action that clears the screen, prevents further data entry and maintains the current session states, until such time as the operator re-authenticates himself or until the Branch Terminal sessions are closed by Horizon system following an inactivity timeout; whichever is the sooner.	A11.1.1 An access control policy shall be established, documented, and reviewed based on business and security requirements for access. A11.3.3 A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

POL00394877

ID	Requirement	Mapping to ISO27001 Control Objectives
SEC-3127	Fujitsu Services shall specify what enforced disconnection facilities they consider necessary. These disconnection facilities shall be agreed with Post Office and documented in an Operational Level Agreement (OLA). Such agreement shall not unreasonably be withheld .	A11.1.1 An access control policy shall be established, documented, and reviewed based on business and security requirements for access. A11.3.3 A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted. A11.5.5 Inactive sessions shall shut down after a defined period of inactivity. A11.5.6 Restrictions on connection times shall be used to provide additional security for high-risk applications.
	Protection Against Malicious Software	
SEC-3129	All hosts and terminals carrying Operational Business data shall be protected on an ongoing basis against malware attacks. Such protection shall be demonstrated in the design to be commensurate with the risk as anticipated by Fujitsu.	A10.4.1 Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented. A12.6.1 Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.
SEC-3133	All new developments will protect databases from SQL injection attacks mounted through data centre perimeter controls such as firewalls.	A10.4.1 Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented. A12.2.1 Data input to applications shall be validated to ensure that this data is correct and appropriate. A12.2.2 Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts. A12.2.3 Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented. A12.2.4 Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
SEC-3137	A risk assessment will be undertaken for retained functionality in the area of SQL injection attacks under HNG-X.	As SEC-3129

POL00394877

ID	Requirement	Mapping to ISO27001 Control Objectives
SEC-3138	Risks identified in the area of SQL injection attacks will be managed under Change Control	A10.1.2 Changes to information processing facilities and systems shall be controlled. A10.4.1 Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.
	Network Management	
SEC-3140	No password shall be transmitted in clear text across any network, whether internal or external.	A10.6.1 Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
SEC-3142	The HNG-X system shall not retrieve data from any external web service unless additional security features are agreed with Post Office Information Security. For the avoidance of doubt, no security change is required to the connection to the DVLA web service.	A10.6.1 Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
	Network Controls	
SEC-3150	{CISP 8.5.1a} The Horizon network configuration shall permit traffic to flow between HNG-X and external systems or services only as agreed by PO Ltd.	A10.6.1 Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. A10.6.2 Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced. A11.1.1 An access control policy shall be established, documented, and reviewed based on business and security requirements for access. A11.7.1 A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.

POL00394877

ID	Requirement	Mapping to ISO27001 Control Objectives
SEC-3152	{CISP 8.5.1b} Unauthorised logical access from non-Horizon systems and networks shall be prevented. This shall include but shall not be limited to, unauthorised access from any of the following: Any public networks used. Networks connecting to Third Parties. Networks connecting Horizon to PO Ltd and/or Royal Mail Group. Other systems operated by the domain supplier on behalf of itself or other clients.	As SEC-3150
SEC-3156	{CISP 8.5.1c} Controls shall protect against denial-of-service attacks originating from non-Horizon systems including those listed in Requirement SEC-3152.	As SEC-3150
SEC-3160	All HNG-X systems shall use private IP addresses which shall not be exposed across the system boundary.	As SEC-3150
SEC-3162	{CISP 8.5.1e} Network management staff within each domain shall be alerted to any attempt to reach the HNG-X systems in their domain from unauthorised network addresses.	A10.6.1 Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. A10.6.2 Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.
SEC-3165	Individual attempts to breach network security controls shall be treated as a minor security breach. A concerted attempt or a successful breach of network security controls shall be treated as a major security breach.	As SEC-3162

POL00394877

ID	Requirement	Mapping to ISO27001 Control Objectives
SEC-3167	{CISP 8.5.1g} Data over Wide Area Networks shall be encrypted unless specifically agreed in the relevant Technical Interface Specification or where otherwise specifically agreed by Post Office Limited Information Security. The Fibre Optic link between Data Centres is not considered to be a Wide Area Network. The requirement applies to transaction data between branches and the data centre(s).	As SEC-3162 A10.9.1 Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification. A10.9.2 Information involved in on-line transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. A12.3.1 A policy on the use of cryptographic controls for protection of information shall be developed and implemented. A12.3.2 Key management shall be in place to support the organization's use of cryptographic techniques. A15.1.6 Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
SEC-3168	WAN Encryption key management shall be independent of network configuration such that the confidentiality of Post Office traffic is not compromised by a single configuration error of either the WAN or the encryption system.	A12.3.1 A policy on the use of cryptographic controls for protection of information shall be developed and implemented. A12.3.2 Key management shall be in place to support the organization's use of cryptographic techniques. A15.1.6 Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.

POL00394877

ID	Requirement	Mapping to ISO27001 Control Objectives
SEC-3169	{CISP 8.5.1h} The system design shall require that no encrypted data is to pass through any HNG-X firewall layer other than certain defined fields in the application level protocol (e.g. encrypted PINs) except where data is subsequently decrypted and passes through another firewall layer. Other cases may be authorised by Post Office Information Security where a risk assessment has identified that the requirement for confidentiality outweighs the requirement for system availability and integrity.	A10.4.1 Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented. A10.6.1 Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. A10.6.2 Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced. A10.9.1 Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification. A10.9.2 Information involved in on-line transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. A12.3.1 A policy on the use of cryptographic controls for protection of information shall be developed and implemented. A12.3.2 Key management shall be in place to support the organization's use of cryptographic techniques. A12.5.1 The implementation of changes shall be controlled by the use of formal change control procedures. A15.1.6 Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
SEC-3170	All proposals for encrypted data to pass through any HNG-X firewall layer shall be subject to risk assessment to determine if the requirement for confidentiality outweighs the requirement for system availability and integrity.	As SEC-3169

POL00394877

ID	Requirement	Mapping to ISO27001 Control Objectives
SEC-3172	Cases requiring encrypted data to pass through any HNG-X firewall layer shall only be authorised by Post Office where a risk assessment has identified that the requirement for confidentiality outweighs the requirement for system availability and integrity.	As SEC-3169
SEC-3174	{CISP 8.5.1j} Test systems shall only share logical network connection with operational systems in carefully controlled circumstances. Test systems shall be configured to connect in this manner for the minimum duration necessary to support testing. The logical connection shall only be permitted after an assessment has confirmed that live operation will not be adversely impacted or as otherwise agreed by Post Office Limited.	As SEC-3162 A11.4.5 Groups of information services, users, and information systems shall be segregated on networks. A11.4.6 For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications. A11.4.7 Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications. A12.5.1 The implementation of changes shall be controlled by the use of formal change control procedures.
SEC-3176	All RADIUS servers that authenticate network access shall be secured and segregated into logical network segments by carrier access method and be externally visible to authorised domain users only.	As SEC-3174
SEC-3178	Any end-user messaging components or services, and their dependent systems or services shall be usable by authorised users from within the HNG-X environment only. "End-user messaging" shall be interpreted as the Branch Message Broadcast Service and any other end-user messaging system subsequently introduced into HNG-X.	As SEC-3174 A11.4.1 Users shall only be provided with access to the services that they have been specifically authorized to use. A11.5.2 All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.
SEC-3180	In the event that e-mail facilities are added to HNG-X, additional security features shall be agreed with Post Office Information Security prior to implementation.	A12.5.1 The implementation of changes shall be controlled by the use of formal change control procedures.

POL00394877

ID	Requirement	Mapping to ISO27001 Control Objectives
SEC-3185	The provision of messaging capability shall not permit active or scripted code to be carried within the message body that may be executed upon Branch Terminals or intermediate systems.	A10.4.1 Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented. A12.6.1 Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.
SEC-3187	The HNG-X messaging system shall not permit messages to carry any attachments except where such attachments have been specifically validated by Post Office Information Security.	As SEC-3185
SEC-3189	{CISP 8.5.1k} The use of wireless technologies within or associated with HNG-X systems or services shall be excluded with the sole exception of mobile public telecommunications services provided by UK licensed public telecommunications operators or as otherwise agreed by Post Office.	A11.4.1 Users shall only be provided with access to the services that they have been specifically authorized to use.
SEC-3192	Any mobile backup or secondary network produced within the {CISP 8.5.1k} specification of the requirement shall be secured to the same level as the primary network.	As SEC-3167
	Access Control	
SEC-3199	Logon to Counter Terminals must provide equivalent security to that provided by logon via native operating systems.	A11.1.1 An access control policy shall be established, documented, and reviewed based on business and security requirements for access. A11.2.1 There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. A11.2.2 The allocation and use of privileges shall be restricted and controlled.

POL00394877

ID	Requirement	Mapping to ISO27001 Control Objectives
SEC-3203	The Horizon Access Control Policy RS/POL/003 shall apply but shall be updated to reflect the change in policy due to HNG-X or other agreed security requirements.	A11.1.1 An access control policy shall be established, documented, and reviewed based on business and security requirements for access. A11.2.1 There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. A11.2.2 The allocation and use of privileges shall be restricted and controlled. A11.2.3 The allocation of passwords shall be controlled through a formal management process. A11.2.4 Management shall review users' access rights at regular intervals using a formal process. A11.3.1 Users shall be required to follow good security practices in the selection and use of passwords. A11.5.1 Access to operating systems shall be controlled by a secure log-on procedure. A11.5.2 All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user. A11.6.1 Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.
SEC-3204	Such update shall include at least the following password requirements: Minimum password length of 7, Minimum password history length of 4	A11.1.1 An access control policy shall be established, documented, and reviewed based on business and security requirements for access. A11.2.3 The allocation of passwords shall be controlled through a formal management process. A11.3.1 Users shall be required to follow good security practices in the selection and use of passwords.

POL00394877

ID	Requirement	Mapping to ISO27001 Control Objectives
SEC-3207	Branch Terminals shall include a single user action that, in between customer sessions, cleanly terminates the clerk session and presents a new clerk login screen. During a customer session, the clerk must first complete or cancel the session in accordance with business rules.	A11.1.1 An access control policy shall be established, documented, and reviewed based on business and security requirements for access. A11.3.2 Users shall ensure that unattended equipment has appropriate protection. A11.5.1 Access to operating systems shall be controlled by a secure log-on procedure. A11.5.2 All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.
SEC-3209	HNG-X shall have controls in place to prevent user bypass of the standard application.	A11.5.1 Access to operating systems shall be controlled by a secure log-on procedure.
SEC-3211	It shall not be possible to install any application or operating system extension except under the control of properly authorised and authenticated systems administrators carrying out authorised and audited changes.	As SEC-3203 A12.4.1 There shall be procedures in place to control the installation of software on operational systems.
	Security in Application Systems	
SEC-3213	The HNG-X system shall provide protection against replay of application messages.	A12.1.1 Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls. A12.2.3 Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.
SEC-3216	Once entered by a cardholder, plain text PINs shall be processed only in a physically secure device as defined in ISO 9564. At all other times, PINs shall be encrypted as defined in ISO 9564.	A12.3.1 A policy on the use of cryptographic controls for protection of information shall be developed and implemented. A12.3.2 Key management shall be in place to support the organization's use of cryptographic techniques.
SEC-3217	Any new PIN processing devices at Data Centres must also comply with FIPS 140-2 Level 3 [DN: This is a LINK requirement - we have a concession for the present Atalla modules but Post Office Limited cannot guarantee it will be renewed if the modules are replaced as part of HNG-X].	As SEC-3216 A11.6.2 Sensitive systems shall have a dedicated (isolated) computing environment.

POL00394877

ID	Requirement	Mapping to ISO27001 Control Objectives
SEC-3218	Any cryptographic key knowledge of which could directly or indirectly reveal plain text PINs must be managed in accordance with ISO 11568	As SEC-3216
SEC-3219	PIN encipherment keys must not be used for any other cryptographic purpose.	As SEC-3216
SEC-3220	Replay of encrypted PIN values shall be prevented.	As SEC-3213 As SEC-3216
SEC-3223	It shall 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. This represents no change to the current Horizon system.	As SEC-3216
SEC-3226	Fujitsu Services shall define a provide high-level description (including any security implications) of use of any Java technology for the Branch Terminal for approval of Post Office Information Security.	A12.1.1 Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.
SEC-3228	HNG-X users shall not have any access to add, modify, delete or execute any operating system or application files without first being properly authorised, authenticated and audited. Controls shall be in place to prevent this requirement being bypassed by any new or upgraded application or system build.	As SEC-3203 A12.4.1 There shall be procedures in place to control the installation of software on operational systems.
SEC-3229	Applications requiring passwords shall continue to comply with the conditions stated in the updated Horizon (HNG-X) Access Control Policy CCD (ref. RS/POL/003). See also Requirement SEC0056.	As SEC-3203
	Cryptographic Controls	
SEC-3235	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 HNG-X Business Data, Reference Data or Application Software unless otherwise agreed with Post Office Information Security. Note: Post Office is highly unlikely to agree to any shorter keys lengths (even for COTS products). For the avoidance of doubt, access to the TES Query service is not covered by this requirement but by requirement SEC-3236.	As SEC-3216 A15.1.6 Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
	Business Continuity Planning	

POL00394877

ID	Requirement	Mapping to ISO27001 Control Objectives
SEC-3237	Fujitsu Services shall ensure that any data processing components within the HNG-X system are provided with data backup facilities in line with BS7799-2:2002 / ISO17799 and its successors as those requirements are embedded in Fujitsu Services. This shall apply both for Business As Usual and any maintenance or migration purposes.	A10.5.1 Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy. A10.7.1 There shall be procedures in place for the management of removable media. A10.7.2 Media shall be disposed of securely and safely when no longer required, using formal procedures. A10.7.3 Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse. A10.8.3 Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.
	Compliance	

POL00394877

ID	Requirement	Mapping to ISO27001 Control Objectives
SEC-3241	With respect to Security, in addition to requirements already listed, all suppliers and Fujitsu Services sub-contractors, and all systems and services supplied specifically for HNG-X shall comply with relevant legal requirements at all stages in the lifecycle. Should either party become aware that a change to systems or procedures is required in order to meet this requirement, it shall inform the other party.	A15.1.1 All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization. A15.1.2 Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products. A15.1.3 Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements. A15.1.4 Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. A15.1.6 Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations. A15.2.1 Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
	Audit	

POL00394877

ID	Requirement	Mapping to ISO27001 Control Objectives
SEC-3242	Prosecution support shall continue to be provided as at present	A8.2.3 There shall be a formal disciplinary process for employees who have committed a security breach. A13.2.3 Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s) A15.1.1 All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization. A15.1.5 Users shall be deterred from using information processing facilities for unauthorized purposes.
SEC-3243	It shall be possible to operate terminals in a branch where there are fewer terminals than configured on the Fujitsu configuration management system. If there are more terminals than expected, the extra ones shall be prevented from performing business transactions. Any variances to the expected number of counter positions must be reported with any update to the number subject to formal change management.	A10.6.1 Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. A11.1.1 An access control policy shall be established, documented, and reviewed based on business and security requirements for access.
	Fallback and Recovery	
SEC-3255	Prior to being allowed access to any systems processing Post Office data, all Fujitsu staff shall be subject to an appropriate level of vetting using criteria approved and provided by Fujitsu Services Group Security. This must include checks on their identity, qualifications and financial circumstances. Criminal record checks must be performed where legally permitted. Business and personal references must also be checked	A8.1.2 Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

POL00394877

B Appendix B – Oracle Database Security Checklist

Adobe Acrobat 7.0 Document

POL00394877

C Appendix C – Counter and Branch Risk Assessment

C.1 Main Risks

The main risks identified in this section are;

#	Risk	Owner	Examples
1	Risk of fraudulent transactions from a valid Counter	Post Office	• Fraudulent mobile phone top-ups. • Fraudulent banking transactions. • Fraudulent sales of products.
2	Risk of SQL injection and other hacking attacks from LAN connected device	Fujitsu	• SQL Injection attacks. • Buffer overflows,

C.2 Threat Scenarios

#	Threat Scenario	Likelihood	Impact	Risk	Vulnerabilities	Potential Mitigation
1	A rogue valid Counter is deployed on the Branch LAN.	Low	Medium	Low	• Fraudulent transactions	• Physical access to the Branch is controlled by the sub-postmaster. • Engineers require one-shot passwords to provision a new Counter onto the Branch LAN. • Counters will always be provisioned with the same Counter IP address in the same Counter position. • Branch Router will be configured to only allow valid IP

POL00394877

#	Threat Scenario	Likelihood	Impact	Risk	Vulnerabilities	Potential Mitigation
						addresses to pass to the Data Centre • Each Counter has a unique identifier, used by the application server in conjunction with the username and password, to control access to the application. • Profiling of Branch transactions – Volumes, types, amounts and times. • Reconciliation of Branch accounts would detect transactions where cash should have changed hands but didn't.
2	A rogue device is deployed on the Branch LAN.	Low	High	Low	• SQL injection attacks • Denial of service attacks • Replayed transaction attacks.	• Physical access to the Branch is controlled by the sub-postmaster. • Counters will always be provisioned with the same Counter IP address in the same Counter position. • Branch Router will be configured to only allow valid IP addresses to pass to the Data Centre • A valid Counter has a unique identifier, used by the application server in conjunction with the username and password, to control access to the application. • Counter application uses session asymmetric and symmetric cryptography based on the username/password combination to setup validate a connection between the Counter and the Data Centre and provide session based anti-replay protection. • Branch Router is configured as a switch which then requires

POL00394877

#	Threat Scenario	Likelihood	Impact	Risk	Vulnerabilities	Potential Mitigation
						additional hardware or administrative access to the router to 'sniff' the network traffic on more than one LAN connection. • Admin access to the Branch Router is only possible over an IPSEC tunnel from the WAN, (not the LAN), interfaces on the Router. • Application traffic is encrypted between the Counter and the Data Centre using SSL with TDES or AES • Application middleware written to validate input to prevent application based DOS attacks. • Firewalls prevent network based DOS attacks • Platforms patched and hardened to prevent network and application based DOS attacks.
2	Stolen Counter	Medium	Medium	Low	•	• Closed networks mean Counter can only access system via GPRS when outside the Branch. • Requires GPRS CHAP secret, (unknown and inaccessible to Engineers), or the Branch Router as the HNG-X network is restricted to specific SIM cards and the SIM card is in the Router. • Branch Router can only be used in the geographical area surrounding its base GPRS relay. (Also applies to Mobile POs but will be a wider area). • Branch Staff will notice the theft!

POL00394877

#	Threat Scenario	Likelihood	Impact	Risk	Vulnerabilities	Potential Mitigation
						• Valid username and password is required to access the system. • Anti-fraud measures protect against fraudulent transactions
3	Stolen Branch Router	Medium	Medium	Low	•	• Branch Router is monitored from the Data Centre periodically. • Only GPRS connection will work from outside a Branch. • Branch Router can only be connected to, for management, from the WAN side and then only over IPSEC. • Branch Router can only be used in the geographical area surrounding its base GPRS relay. (Also applies to Mobile POs but will be a wider area). • Branch Staff will notice the theft! • Application middleware written to validate input to prevent application based DOS attacks. • Firewalls prevent network based DOS attacks • Platforms patched and hardened to prevent network and application based DOS attacks. • A valid Counter has a unique identifier, used by the application server in conjunction with the username and password, to control access to the application. • Counter application uses session asymmetric and symmetric

POL00394877

#	Threat Scenario	Likelihood	Impact	Risk	Vulnerabilities	Potential Mitigation
						cryptography based on the username/password combination to setup validate a connection between the Counter and the Data Centre and provide session based anti-replay protection.
4	Stolen GPRS SIM	Medium	Low	Low	•	• Branch Router can only be used in the geographical area surrounding its base GPRS relay. (Also applies to Mobile POs but will be a wider area). • Application middleware written to validate input to prevent application based DOS attacks. • Firewalls prevent network based DOS attacks • Platforms patched and hardened to prevent network and application based DOS attacks. • A valid Counter has a unique identifier, used by the application server in conjunction with the username and password, to control access to the application. • Counter application uses session asymmetric and symmetric cryptography based on the username/password combination to setup validate a connection between the Counter and the Data Centre and provide session based anti-replay protection.
	SSL traffic is intercepted using a 'man in the middle attack'	Low	High	Low	•	• Would require a copy of the Data Centre SSL private key, access to which is controlled through a combination of policy, process, logical and physical access controls.

POL00394877

#	Threat Scenario	Likelihood	Impact	Risk	Vulnerabilities	Potential Mitigation
						• Data Centre certificate will be set to expire every 12 months. • Counters will be configured with the Data Centre issuing CA as the only one they will accept valid certificates from. • Counter will be configured to check for CRL prior to every SSL connection. • Sensitive authentication and authorisation data, (PAN, PIN, PIN offset and PIN Blocks, personally identifiable information as defined by the Data Protection Act 1998), will be protected further by encryption and obfuscation using TDES or AES or SHA1 hashing using a randomised seed value.

	Fraudulent use of a valid counter bt branch staff				•	• Branch User authentication providing no repudiation of transactions within the Branch User Session.
						• Application level auditing providing a secure and consistent audit trail with no gaps.
						• Anti-fraud measures protect against fraudulent transactions built into business applications, for example:
						  • Recovery records lodged centrally for transactions which can cause a change of value in an external system, e.g. Banking.
						  • Recovery records lodged prior to printing a Postage Label.
						  • APOP Database updated when value assigned to Postal

POL00394877

#	Threat Scenario	Likelihood	Impact	Risk	Vulnerabilities	Potential Mitigation
						Order, and prior to voucher printing..