FUJITSU

POST OFFICE

Description of Fujitsu's System of IT Infrastructure Services supporting Post Office Limited's POLSAP and HNG-X applications

Throughout the Period 1 April 2014
To 31 December 2014

With the independent service auditor's assurance report including tests performed and results thereof

Table of Contents

POL00399609

1. Management Assertion

Fujitsu Services Limited's Management Assertion

11 February 2015

Fujitsu Services Limited ("Fujitsu", "We", "we", "Company") has prepared the accompanying *Description of Fujitsu's system of IT infrastructure services supporting Post Office Limited's POLSAP and HNG-X applications throughout the period 1 April 2014 to 31 December 2014* ("Description").

This has been prepared for:

1. Post Office Limited ("POL") as users of the system during some or all of the period 1 April 2014 to 31 December 2014; and
2. The independent auditors of POL.

POL and its independent auditors are assumed to have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by POL itself, when assessing the risks of material misstatements of POL's financial statements.

The Company confirms, to the best of its knowledge and belief, that:

a. The Description fairly presents the IT support processes and controls used by and on behalf of Fujitsu to support the POLSAP and HNG-X applications ("System") made available to POL during the period 1 April 2014 to 31 December 2014 for providing IT support to the HNG-X and POL SAP applications. The criteria we used in making this assertion were that the Description:

(1) Presents how the System made available to POL was designed and implemented, including:

- the types of services provided;
- the procedures, within both automated and manual systems, by which those services are provided;
- the related supporting information; this includes the correction of incorrect information and how information is transferred to the reports prepared for POL;
- how the System captures and addresses significant events and conditions;
- the process used to prepare reports or other information provided to POL as the user of the System;
- specified control objectives and controls designed to achieve those objectives;
- controls that, in designing the System, the Company contemplated would be implemented by POL in order to achieve the specified control objectives (Complementary User Entity Controls); and
- Other aspects of the Company's control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to the services provided.

(2) Does not omit or distort information relevant to the scope of the System

b. The Description includes relevant details of changes to the System during the period from 1 April 2014 to 31 December 2014.

c. The controls related to the control objectives stated in the Description which together with the complementary user entity controls referred to above, were suitably designed and operated effectively throughout the period 1 April 2014 to 31 December 2014 to achieve those control objectives stated in the Description. The criteria we used in making this assertion were that:

(1) The risks that threaten the achievement of the control objectives stated in the Description have been identified by Fujitsu;

(2) the controls identified in the Description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved; and

(3) The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Gavin Bell
Service Delivery Director Private Sector BAS

EY
Building a better
working world

Ernst & Young LLP
1 More London Place
London
SE1 2AF

Tel: GRO
Fax
ey.com

2. Report of Independent Service Auditor

Fujitsu Services Limited
Lovelace Road
Bracknell
RG12 8SN

Scope

We have been engaged to report on Fujitsu Services Limited ("Fujitsu")'s accompanying *Description of Fujitsu's system of IT infrastructure services supporting Post Office Limited's POLSAP and HNG-X applications throughout the period 1 April 2014 to 31 December 2014* (Description) and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the Description. The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls contemplated in the design of POL's controls are suitably designed and operating effectively, along with related controls at the service organisation. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Fujitsu uses a range of network providers to provide Wide Area Network (WAN) services to POL. The Description includes only the controls and related control objectives of Fujitsu and excludes the control objectives, and related controls of these network providers. Our examination did not extend to the controls of network providers.

Fujitsu's responsibilities

Fujitsu has provided the accompanying assertion titled, *Management Assertion* (Assertion) about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description. Fujitsu is responsible for preparing the Description and the Assertion, including the completeness, accuracy and method of presentation of the Description and the Assertion and stating the control objectives in the Description. Fujitsu is also responsible for providing the services covered by the Description, specifying the control objectives, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the Assertion and designing, implementing and documenting controls to achieve the related control objectives stated in the Description.

Service Auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description, based on our examination. We conducted our engagement in accordance with International Standard on Assurance Engagements 3402 *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board. That standard requires that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the Description throughout the period 1 April 2014 to 31 December 2014.

An assurance engagement to report on a description of a service organisation's system, and the suitability of the design and operating effectiveness of the service organisation's controls to achieve the related control objectives stated in the description, involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the Description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the Description were achieved. A reasonable assurance engagement of this type also includes evaluating the overall presentation of the Description, the suitability of the control objectives stated therein and the suitability of the criteria specified by the service organisation and described in the Assertion. We believe that the evidence we obtained is sufficient and appropriate to provide a basis for our opinion.

Inherent limitations

The Description is prepared to meet the needs of POL and its auditors and may not, therefore, include every aspect of the system that POL may consider important in its own particular environment. Because of their nature, controls at a service organisation may not prevent or detect and correct all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in the Assertion. In our opinion, in all material respects:

a. the Description fairly presents the IT support processes and controls used by and on behalf of Fujitsu to support the POLSAP and HNG-X applications that were designed and implemented throughout the period 1 April 2014 to 31 December 2014.

b. the controls related to the control objectives stated in the Description were suitably designed throughout the period 1 April 2014 to 31 December 2014 if POL applied the complementary user entity controls contemplated in the design of Fujitsu's controls and subservice organisations.

c. the controls tested, which, together with the complementary user entity controls referred to in the scope paragraph of this report if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period 1 April 2014 to 31 December 2014.

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed in the accompanying ***Description of Control Objectives, Controls, Tests and Results of Tests*** (Description of Tests and Results).

Intended use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Fujitsu, POL as the user of the IT support processes and controls used by and on behalf of Fujitsu to support the POLSAP and HNG-X applications during some or all of the period 1 April 2014 to 31 December 2014 and the independent auditors of POL, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Ernst & Young LLP

13 February 2015
London
United Kingdom

3. Description of Fujitsu's system of IT infrastructure services supporting Post Office Limited's POLSAP and HNG-X applications throughout the period 1 April 2014 to 31 December 2014

3.1 Overview of Fujitsu

3.1.1 History of Fujitsu

Fujitsu has evolved, through a process of acquisition and organic development, to create a broad-based technology and services organisation, with a strong record of innovation and lean service delivery. Fujitsu has a long and successful history which has links going back more than 40 years.

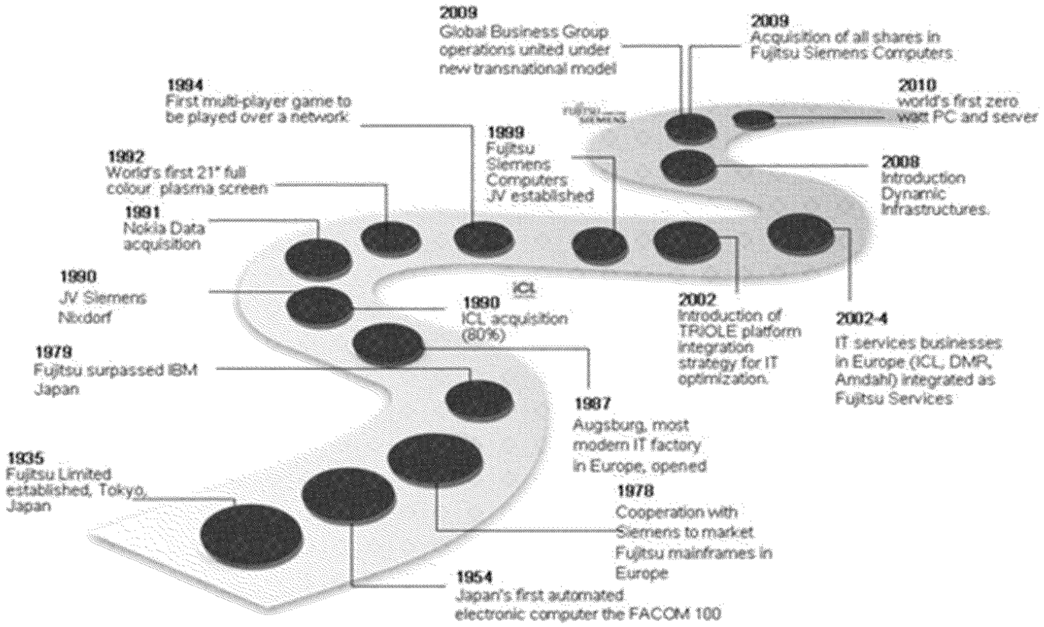

2009
Global Business Group operations united under new transnational model
2009
Acquisition of all shares in Fujitsu Siemens Computers
1994
First multi-player game to be played over a network
2010
world's first zero watt PC and server
1999
Fujitsu Siemens Computers JV established
1992
World's first 21" full colour plasma screen
2008
Introduction Dynamic Infrastructures.
1991
Nokia Data acquisition
1990
JV Siemens Nixdorf
ICL
1990
ICL acquisition (80%)
2002
Introduction of TRIOLE platform integration strategy for IT optimization.
2002-4
IT services businesses in Europe (ICL, DMR, Amdahl) integrated as Fujitsu Services
1979
Fujitsu surpassed IBM Japan
1987
Augsburg, most modern IT factory in Europe, opened
1935
Fujitsu Limited established, Tokyo, Japan
1978
Cooperation with Siemens to market Fujitsu mainframes in Europe
1954
Japan's first automated electronic computer the FACOM 100

Figure 1. Fujitsu's Growth in Services through Acquisition or Organic Development

The recent history of the company in Europe began in 1968 as International Computers Limited (ICL), formed through the merger of English Electric Computers (EEC) and International Computers and Tabulators (ICT), in response to the increasing market dominance of the large American corporations. The company was listed on the stock market until it was acquired by Standard Telephones and Cables (STC plc) in 1984.

In 1990, the Japanese IT Services Company, Fujitsu Ltd, acquired an initial 80% stake for £740million. Further acquisitions were made by Fujitsu in 1993 and 1996 from STC, (then owned by Nortel), with the remaining interest in the company being acquired in 1998.

In April 2002, ICL fully re-branded to Fujitsu Services Limited (FSL), and later as Fujitsu, as it looked to exploit the Fujitsu Group's expertise and technology, including its extensive R&D spend. FSL (Fujitsu) now operates as the UK and Ireland IT Services-based arm of the global Fujitsu Group.

In 2009, we integrated Fujitsu Siemens Computers (FSC) into the organisation, representing an exciting step in Fujitsu's strategy for growth, and forming the new Technology Solutions Division (TSD). This new division has a portfolio that encompasses Infrastructure Products and Solutions, Managed Services and Infrastructure as a Service. Following this integration Fujitsu adopted an operating model based on 8 regions and a number of global support functions.

The UK and Ireland (UK&I) region was formed, merging the expertise previously delivered by Fujitsu Services and the product know-how from Fujitsu Siemens. Operating under the name of Fujitsu (UK and Ireland) the company provides integrated technology offerings and business solutions.

From April 1, 2014 we created a truly global matrix structure to create a single global team, utilizing the best Fujitsu talent from across the world. In line with our globalisation strategy, our new structure is by 5 geographic regions focused on our customers, sales and delivery, with Fujitsu UK&I becoming part of the EMEIA region. The other 4 regions are Americas, Asia (including China), Oceania and Japan.

In April 2014 Fujitsu announced the acquisition of GlobeRanger – a US based technology company that operates in the Radio Frequency Identification (RFID) technology space. The acquisition will see GlobeRanger remain as an autonomous product development and marketing unit, owned by UK and Ireland, but with Fujitsu taking a place on their Board of Directors.

3.1.2 Major Markets and Human Capital

Fujitsu UK and Ireland is a leading IT systems, services and products company employing 11,400 people with an annual revenue of £1.7 billion. Its business is in enabling its customers to realise their objectives by exploiting information technology through its integrated product and service portfolio. This includes consulting, applications, systems integration, managed services and product for customers in the private and public sectors including retail, financial services, telecoms, government, defence and consumer sectors.

3.1.3 Organisational Structure, including Business Units

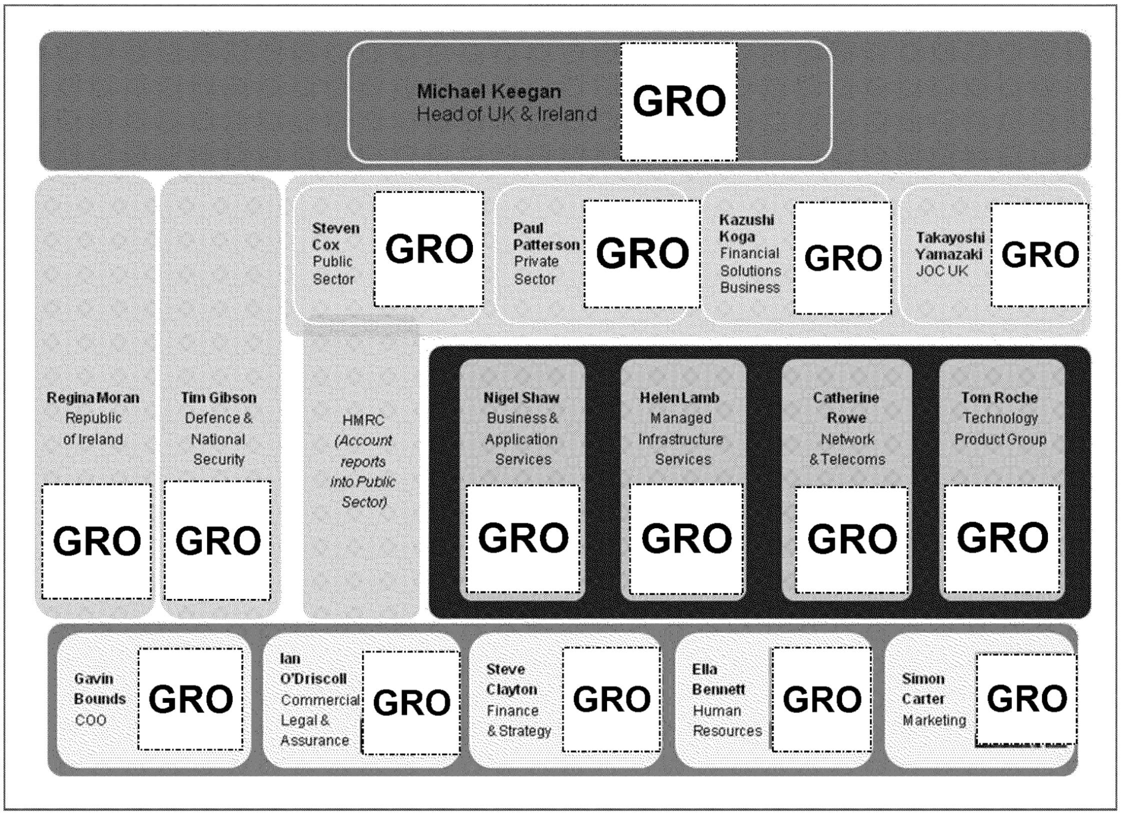


Figure 2. Fujitsu UK and I Organisation

3.1.4 Geographical Spread

Fujitsu operates in the following Regions:

- Africa: Algeria, Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Congo, Democratic Republic of Congo, Djibouti, Egypt, Equatorial Guinea, Eritrea, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea Bissau, Ivory Coast, Kenya, Lesotho, Liberia, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Niger, Nigeria, Reunion, Rwanda, Sao Tome, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, Swaziland, Tanzania, Togo, Tunisia, Uganda, Western Sahara, Zambia, Zimbabwe
- Asia: China, Hong Kong, India, Indonesia, Japan, Korea, Malaysia, Philippines, Singapore, Sri Lanka, Taiwan, Thailand, Vietnam
- Australasia: Australia, New Zealand
- Central America and Caribbean: Anguilla, Aruba, Bahamas, Barbados, Cayman Islands, Dominica, French Guiana, Guadeloupe, Jamaica, Martinique, Mexico, Montserrat, Netherlands Antilles, Saint Vincent and Grenadines, Trinidad-and-Tobago, Virgin Islands British, Virgin Islands U.S.

- Europe: Armenia, Azerbaijan, Austria, Belarus, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Ireland, Italy, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Luxembourg, Macedonia, Moldova, Netherlands, Norway, Poland, Portugal, Romania, Russia, Serbia, Slovenia, Slovakia, Spain, Sweden, Switzerland, Tajikistan, Turkmenistan, Ukraine, United Kingdom, Uzbekistan
- Middle East: Afghanistan, Bahrain, Gaza, Iraq, Israel, Jordan, Kuwait, Lebanon, Malta, Oman, Pakistan, Palestine, Qatar, Saudi Arabia, Turkey, United Arab Emirates, West Bank, Yemen.
- North America: Canada, United States
- South America: Argentina, Brazil, Chile, Colombia.

4. Overall Control Components

This section provides information about the five interrelated components of internal control at Fujitsu:

- **Control Environment** – sets the tone of an organisation, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
- **Control Activities** – are the policies and procedures that help make sure that management's directives are carried out.
- **Information and Communication** – are systems, both automated and manual, that support the identification, capture and exchange of information in a form and time frame that enable people to carry out their responsibilities.
- **Monitoring** – is a process that assesses the quality of internal control performance over time.
- **Risk Assessment** – is the entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks can be managed.

Fujitsu's internal control components include controls that may have a pervasive effect on the organisation, an effect on specific processes, account balances, disclosures, classes of transactions or applications, or both. Some of the components of internal control include controls that have more of an effect at the entity level, while other components include controls that are primarily related to specific processes or applications. When assessing internal control, we consider the interrelationships among the five components.

4.1 Control Environment

Management has established and maintains an internal control structure that monitors compliance with established standards, policies, and procedures. The remainder of this section discusses the tone at the top as set by Leadership and Management, the integrity, ethical values and competence of Fujitsu employees, the standards, policies and procedures, the risk management process and monitoring and the roles of significant control groups. The internal control structure is established and refreshed based on Fujitsu's assessment of risk facing the organisation.

4.2 Integrity and Ethical Values

Fujitsu recognizes its responsibility to foster a strong ethical environment to determine that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct. This responsibility is characterized and reflected in the Fujitsu Way Code of Conduct, which is communicated to all employees of the organisation. All employees are required to maintain ongoing compliance. Compliance checks are undertaken to help ensure that employees understand and comply with the Fujitsu Way Code of Conduct.

4.3 Structure for Serving Post Office Ltd.

4.3.1 Service Lines and Functions

The Service Lines and Functions that provide services, or support the delivery of service to PO Limited (POL) are as follows:

- Business and Applications Services (BAS) (Direct to POL).
- End User Services Group.
- Hosting and Network Services Group.
- Technology Product Group.
- Business Operations & Business Excellence.
- Commercial and Legal Assurance.
- Finance and Strategy.
- Human Resources.
- Sales and Marketing.

The purpose of these Service Lines and Functions is to enable, organise and facilitate the requirements placed on the Fujitsu Post Office Account (POA) by POL.

The management of the above Service Lines and Functions establish their own frameworks within their areas for the continuous formal support of POA and enforce this through their own policies, procedures and standards, and registers, including where applicable internal and external audits. The procedures to support POA are set out in each area's own implementation of the Fujitsu Business Management System (BMS). The controls in place in each of these Services Lines and Functions help ensure that the areas have overall objectives, terms of reference, job descriptions and senior management roles. Each of these functions has its own levels of management, staff, directors and stakeholders all of which impact the service that POA is able to provide to POL. Each of these Service Lines and Functions is also responsible for ensuring that their staff are appropriately trained and follow Fujitsu Corporate processes to achieve this.

Each of the Service Lines and Functions is also controlled through its own service descriptions, organisational controls, vision, mission and value statements, governance and control frameworks, monitoring and review controls and performance measures.

Although POL are in the process of amending the way they work with suppliers to deliver the services to their end users, these changes to the service delivery model, and Fujitsu's role and place in this model, is still being finalized. On this basis, since 1 April 2014 these changes have not had a significant impact on either the scope of the services Fujitsu deliver under the contract with POL, or on the way that these services are delivered.

4.4 Control Activities

4.4.1 Governance and Oversight of Control Activities

Fujitsu has established the Corporate Governance Committee (CGC) and Audit Committee responsible to the Fujitsu UK and Ireland Board to oversee the companies' approach to governance and control.

The directors are committed to maintaining a strong control environment throughout the organisation and recognise that the control environment provides the foundation for all other components of internal control providing discipline and structure.

The Board of Directors (the Board) is responsible for monitoring the performance of the Company on behalf of its shareholders and ensuring that Fujitsu satisfies all regulatory and statutory requirements related to its operations.

Authority for all action and expenditure within Fujitsu Service flows from the Board and the Board has established that the necessary control systems are in place to ensure that business is undertaken in a responsible manner. Fujitsu's policies, operations and strategy are controlled by the Board.

The Board meets as required and its two key sub-committees the CGC and the Audit Committee meet quarterly.

In addition Fujitsu has a systematic approach to policy and process with a set of Master Policies approved by the CGC and sub-policies and processes determined by the relevant regional functions underneath. The framework, known as the Business Management System (BMS) is managed by Fujitsu's Business Assurance teams and comprises of a set of mandatory Master Policies and Business Processes. The key Master Policies cover Ethics, Security, Human Resources, Corporate Responsibility, Finance, Legal, Service Delivery, Quality, Project Management, Risk Management and Business Continuity under each of which is a set of specific business processes owned by Senior Management.

Within POA each Service Line and Function follows the BMS. Where exceptions to the BMS are necessary, local standards, procedures and work instructions are documented with a 'Let' from the Corporate Process Owner where the Corporate Process Owner authorises that local departure from the BMS.

4.4.2 Human Resources

4.4.2.1 Policies and Practices

Human resource policies and practices relate to hiring, orienting, training, evaluating, counselling, promoting and compensating personnel. The competence and integrity of Fujitsu's personnel are essential elements of its control environment.

4.4.2.2 Performance Management

Performance Management is a process for managing and improving performance of teams and individuals through proactive management of objectives / deliverables which are clearly linked to the Mid Term Plan. It includes the identification of development needs and ongoing evaluation of achievement and capability by the reviewer and the individual involved. Fujitsu UK & Ireland is committed to providing the organisation and our employees with a common performance management process that is consistently applied across the organisation and is aligned with organisational goals.

This process also defines how individual employees express their short and long term desires for career development. The process involves the individual in planning career goals by identifying the specific steps to develop skills to fulfil and manage career transitions.

The Fujitsu UK & Ireland's Performance process applies to all employees within Fujitsu UK & Ireland and embodies the principle that strong business performance is most likely when employees feel they are operating at the peak of their potential in roles that match the company's objectives.

Fujitsu's Human Resource policies are held and maintained on its CafeVik web portal and managed by Fujitsu's HR teams. These policies operate employment policies to provide a framework for the employment of people and provide employees with a clear and concise set of rules in which to operate.

Its policies apply to Fujitsu UK & Ireland. This means all employees, contractors and businesses carried out by Fujitsu Services Limited and its subsidiaries and any other company or organisation that is managed by the Chief Executive Officer, Fujitsu United Kingdom and Ireland.

4.5 Information and Communication

Fujitsu UK and Ireland Service Lines and Functions have CaféVik portals to enable sharing of knowledge across the company, and throughout their own business areas.

These portals provide information about each of the Service Lines and Functions and what products and services they offer to the company.

Fujitsu has a robust and reliable communication framework that utilises push and pull strategies to help ensure that all employees have the information they need to perform their roles effectively, efficiently and ethically. Some of the mechanisms used to communicate directly with Fujitsu employees include:

- Road Shows.
- Staff Briefings.
- Team Meetings.
- Leadership and Management Cascades.

In April 2014 invitations were sent to all employees in the Group to participate in a Global wide employee engagement survey.

Fujitsu also seeks the views of employees via representative groups in different parts of the Company. During this year (2014) in the UK it has set up Fujitsu Voice with over 39% of employees voting in an election for its 23 members. Fujitsu management consults regularly with these bodies, providing updates and seeking views on important issues. In addition Fujitsu has agreements with Trade Unions that include regular meetings with local and senior management to discuss issues affecting employees in the unions' area of interest.

4.6 Monitoring

Fujitsu utilises a variety of systems, processes and tools to help ensure that operations are efficient, effective and ethical, including:

- Performance Dashboards.
- Standard Reporting Packs.
- Audits and Health Checks.
- Reviews and Lessons Learned.
- Customer Satisfaction Scores.

Audits by Fujitsu Business Assurance Teams, Fujitsu External ISO Accreditors (the POL account is itself accredited to ISO 27001) and POL or its agents (including PCI DSS and Link Auditors) are used to support the design, implementation and post implementation review of the controls in place and to help ensure that the relevant governance, strategy and needs and requirements of both POL and Fujitsu are met.

Data and information from these sources are used to identify weaknesses, inefficiencies or potential performance issues. Performance issues are remediated and opportunities for improvement are identified, evaluated, prioritised and managed through to appropriate implementation.

The BMS Team interacts periodically with both the internal and external auditors.

4.7 Risk Assessment

4.7.1 Risk Policy and Implementation

All operating companies within Fujitsu's Global Business Group (GBG) are required to have a Risk Management Framework. Each group is also required to have a designated Chief Risk Management Officer (CRMO) whose responsibilities include bi-annual risk reporting and prompt escalation of significant risks to GBG in addition to managing the risk process for the Board. Fujitsu's Risk Management Framework centres on the Risk Management Policy which is a key management policy overseen by the Corporate Governance Committee (CGC) of the Board chaired by the Executive Chairman. Responsibility for implementation of the Risk Management Policy is delegated throughout the business cycle. Fujitsu provides support and guidance to employees through the Customer Solution Lifecycle, a repository of best practice and training. Management oversight at critical points in the business cycle is provided through the Review Framework, a structured set of formal management reviews. Fujitsu's management of risk is exhibited throughout these structures such that potential problems can be planned for and managed appropriately.

4.7.2 Fujitsu's Risk Process

The Fujitsu Risk Process is used to support the evaluation reporting and management of risks within the business and is consistent with recognised Risk Management standards.

Fujitsu's Enterprise Risk Management System (ERM) provides clear and effective monthly risk reporting to the regional leadership teams and forms the basis of the GBG. This helps to ensure a high level of risk management is maintained throughout the organisation.

4.8 Services provided

4.8.1 Physical and Environmental Controls

1. ***Control Objective 1: Controls provide reasonable assurance that access to the data centre and facilities with computer equipment, storage media and program documentation is restricted to properly authorised individuals.***

#	Control
1.1	**Data centre access:** Data centre specific physical access security policies and procedures to control access to the data centre and other sensitive areas, including computer equipment and storage media, are implemented. These are made available to Fujitsu staff via the intranet.
1.2	**Access within the data centre:** Access beyond the security desk is protected by a key-card system that restricts individual access to specific data processing areas. Security management has determined appropriate levels of physical access to the data centre, which is based on the roles and responsibilities of staff. Staff requiring access to the data centre must complete an access form, which must be signed as approved by the line manager responsible for the zones requested.
1.3	**CCTV**: The data centre(s) is controlled and monitored through the use of CCTV video cameras. Video cameras are placed at strategic locations around the perimeter of the building to help ensure that coverage of the data centre is obtained.
1.4	**Security guards:** Security guards are present at the data centre 24 hours per day, seven days per week. The data centre can only be accessed through a central area.
1.5	**Data centre visitors:** Visitors are required to sign in at the reception areas and temporary badges are issued. Visitors must have been pre notified to data centre security by a Fujitsu employee.

#	Control
1.6	**Failed access monitoring:** Attempts to enter restricted areas without using authentication devices are denied and a security alert is triggered and logged. Data centre management proactively follows up on security alerts that are triggered.
1.7	**Review of user access within the data centre:** Periodic reviews are performed of users who have access to the data centre to help ensure that their access rights are appropriate.
1.8	**Deletion of user access:** The managers of the various delivery teams are responsible for notifying the local site facilities team of terminations or transfers of their direct reports. Upon notification of employment changes, access through the security access control system is revoked.

2. Control Objective 2: Controls provide reasonable assurance that computer equipment and facilities are protected from damage by fire, flood and other environmental hazards and maintenance agreements are in place.

#	Control
2.1	**Fire Suppression:** Fire detection and suppression devices, such as hand-held fire extinguishers, are strategically placed throughout the entire data centre.
2.2	**Maintenance Schedule:** Periodic inspection and maintenance is performed on protection devices, sensors and alarm systems.
2.3	**Environmental monitoring:** Smoke detectors and water, humidity and temperature monitoring devices are installed to detect abnormal environmental conditions.
2.4	**UPS Supply**: A UPS system is installed to protect the facilities and computer equipment from electrical power fluctuations and outages.

The Trident House campus comprises of a two storey office block (Phase I) with an adjoining computer room and data / output handling area. There is also a separate single storey building (Phase II) containing offices and another computer room. There is one main entrance to the Trident House Phase I building and a loading bay and one main entrance to the Trident House Phase II building.

The IRE11 data centre component of the Trident House campus is composed of raised floor computer rooms, office space and facility support (Un-interruptible Power Supply [UPS], backup generators and power distribution equipment). The IRE11 data centre is staffed with its own security guards, who are on duty 24 hours a day, seven days a week (**1.4**). Physical access to the data centre can only be obtained through the security officer's desk at the main entrance to the campus. The Trident House campus is also equipped with Closed Circuit Television (CCTV) cameras, monitored by the campus security guards (for all areas) and the Data Centre Operations team for all secure Data Centre computer rooms. These cameras are located along the IRE11 campus perimeter, entry / exit locations, main entrances and numerous additional strategic locations within the secure computer rooms to help ensure complete coverage of the data centre **(1.3)**.

The IRE11 data centre has developed and implemented data centre specific physical access security policies and procedures to control access to the data centre and other sensitive areas, including computer equipment and storage media **(1.1)**.

The POL computing hardware and storage media are located in secure areas of the data centre facility with access restricted to appropriate personnel through the use of an electronic cards access system (SAFE); the computer room employs keypad / PIN code technology as an additional level of access control **(1.2)**. Personnel are required to individually swipe in and where applicable, swipe out of an area. "Piggy backing" off someone else swiping in is prohibited. Attempts to enter restricted areas without using authentication devices are denied and a security alert is triggered and logged. Data centre management proactively follows up on security alerts that are triggered **(1.6 and 1.7)**.

Access to the data centre is secured based on electronic card access systems (**1.2**).

This system controls entry to personnel who need it, while maintaining the security of the building.

When an employee leaves the company, the card is removed from the system database and would no longer provide access to the cardholder. Therefore if cards are not retrieved, the security of a facility can be maintained. Unique cards are issued for each employee, for individual control, accountability and tracking of activity. Flexible control is accomplished by allowing each person access to different areas and only at certain times.

An audit trail is provided for management tracking and reporting of who entered and / or left a particular area at a particular time. Tracking of all access attempts is provided to allow management to determine if employees are attempting to enter areas they are not permitted into, or whether employees are attempting to get into areas at the times when they are not allowed access to those areas (**1.6**).

4.8.1.1 Visitor Access

Visitors (and initially new joiners who have not yet been issued their photo access card) are issued with a visitor's access card (**1.5**). Visits to the IRE11 campus, and the issue of visitor access cards, must be recorded in the local site visitors' log. The details must include: Date and time of entry, Name, Company (where applicable), Person visiting, Unique number of the visitor access card and Time of exit.

Visitors should normally be escorted around Fujitsu sites, but they can be issued with an 'unescorted' access card, depending on the provisions in the Local Site Building Security Procedures.

The 'escorted' and 'unescorted' badges (and lanyards) clearly distinguish visually which is which.

All access to the computer rooms is strictly controlled. To access the computer rooms an individual must first complete a request in the data centre on-line access request system to obtain approval; if a valid reason has not been provided for multiple accesses, the access will only allow the individual to access the data centre once. No access is granted unless a valid reason has been provided and the on-line access ticket has been authorized **(1.5)**.

All visitor access cards (common areas) are handed into the issuer (normally reception or site security) at the end of each day. All visitor access cards (computer rooms) must be handed into the issuer (IRE11 Operations team) at the end of each day.

Persons issuing visitor access cards (reception / site security / DC Operations team) must check the records to help ensure that all visitor access cards are recovered at the end of each day. If cards are outstanding at the end of the day they must be electronically disabled and enquiries made to the person issued with the access card, or the person they were visiting, as to the return of the access card.

4.8.1.2 Monitoring of Individuals with Access to the Data Centre

Listings are maintained showing individuals with IRE11 data centre access. The IRE11 Data Centre management and Fujitsu Group Security personnel periodically review reports that list user access levels to restricted areas of the data centre to determine whether user access rights are appropriate **(1.7)**. The managers of the various delivery teams are responsible for notifying the local site facilities team of terminations or transfers of their direct reports. Upon notification of employment changes, access through the security access control system is revoked and the card key and other physical access devices are collected **(1.8)**.

4.8.1.3 Environmental systems

The IRE11 data centre is equipped with environmental systems to safeguard POL's hardware and information assets located within the facilities. The computer room is equipped with leak detection systems, smoke detectors, fire suppression systems, hand held fire extinguishers and temperature monitoring systems **(2.1, 2.3).** Condensing units, pumps, and chillers provide cooling for the data centre.

This equipment supports multiple computer room air conditioning units distributed throughout the raised floors. The POL client's servers and hardware equipment are mounted in locked racks or free standing cabinets on the raised floors.

Each computer room is supplied by separate commercial power feeds, each from a single power generation substation. Separate diesel generators support each computer room and provide backup power in the event that commercial power is temporarily unavailable. These generators are supplied by additional fuel tanks that provide an operating window at full load. The power distribution equipment consists of two uninterruptible power supply (UPS) systems providing conditioned power to a UPS Static Switch. The UPS Static Switch provides power as the primary and alternate source of power to the associated Static Switch Power Distribution Units (PDUs). The PDUs have dual feeds designed to provide a seamless transfer in the event of a power loss **(2.4).**

The IRE11 data centre is monitored by a Building Management System (BMS) located in the Site facilities office (monitored by 3rd party GS Hall engineers) in the Phase I buildings within the data centre location, with repeater heads located in the Security office and the data centre Operations Bridge. The BMS automatically alerts all three stations if abnormal environmental conditions occur.

The GS Hall engineers, Security and Operations teams monitor the system 24 hours a day, seven days a week to provide rapid evaluation and response to facility problems **(2.3).** Scheduled inspection and maintenance are performed on environmental protection devices, sensors, and alarm systems **(2.2).** Checks are performed at varying intervals dependent on the devices being maintained; however, devices are checked at least annually.

4.8.2 Backup

3. Control Objective 3: Controls provide reasonable assurance that programs, files and datasets that have been identified as requiring periodic backup are backed up and retained.

#	Control
3.1	**Backup Definition**: The Backup High Level Design documents define Backup and recovery requirements and policy for the platform.
3.2	**Backup Toolset:** Backups are performed using Net Backup or RMAN (automated tools).
3.3	**Backups are written to a secondary location:** Backups performed are written to a separate disk array and are simultaneously written to a disk array at the disaster recovery site.
3.4	**Failed backups are tracked and monitored**: Failed backups are signalled to the Master Batch Scheduling system which raises events in a generic manner to the SMC.

The Solution Owner is responsible for ensuring that in the event of accidental deletion or corruption of data that the data can be recovered. The Platform Physical Design document will define whether a NetBackup client is required and the Application High Level Design will define the backup and recovery policy and method (**3.1**). The Solution Owner is also responsible for defining the archive and deletion policy and data that needs to be retained for audit purposes.

At the discretion of the Solution Owner, backups may be performed using Oracle RMAN or the NetBackup based Backup System according to patterns defined in the Backup & Recovery High Level Design (**3.2**).

In the case of Oracle RMAN backups the backup data is written to disk in a separate disk array. Simultaneously it is also written to a disk array at the disaster recovery site (**3.3**). Those systems which have been identified as requiring backups via the NetBackup solution will have their backups scheduled via the TWS scheduler; this provides automatic monitoring of the status of the backups, and will have backups written to each data centre to provide resilience in the event of a requirement to perform Disaster Recovery.

Depending on the size of the dataset to be backed up either a direct client backup via the network may be performed or a split mirror backup using standard features (clones and snapshots) of the storage arrays which are presented to the backup media server. Data is written to a virtual tape library at both the primary and the disaster recovery sites. No tapes are exported from the system unless specifically requested and authorised.

Note that in some circumstances, the recovery may by design be effected by replaying the data from an upstream system rather than by performing a traditional "backup recovery" as many systems need to keep a consistent view of each other and going backwards in time is not always appropriate.

The Backup Development team delivers appropriate NetBackup policies according to these definitions. The Live System Test team reviews the delivered policies against the design requirement. If an RMAN backup has been specified, the Live System Test application instance will perform those same RMAN backups or, in the case of POLSAP application service, the Operational Acceptance Test (OAT) system will be used to confirm the operation of the RMAN backup before deploying to Production.

The backup jobs are automated as defined by the Solution Owner in the Batch Scheduling High Level Design and implemented by the Schedule Development team. If a backup does not complete or does not backup all files it will exit with a failure status. Detection of failed backups is through job failure being signalled to the Master Batch Scheduling system which raises events in a generic manner to the System Management Centre (SMC). SMC uses the Known Error Log (KEL) system to identify the appropriate team to respond to the backup failure and pass a Triole for Service (TFS) call to their call stack with a voice prompt. Corrective action that is required beyond a simple rerun via the batch scheduler is planned and a Managed Service Change (MSC) ticket is raised for approval. A mechanism exists to provide emergency approval by escalating to the Duty Service Manager out of hours (**3.4**).

The backup and recovery methods are based on well-known industry standard solutions, and the general operation was extensively tested during non-functional testing prior to HNG-X go-live. The responsibility of the operational teams only extends to recovering data from tape or clone images and performing database recovery, such as archivelog replay. There may subsequently be application support activity required to return the service to an operational state. Recovery is tracked through the incident number of the call raised for the original fault report, and is only performed when a MSC has been approved by Service Management. This same process is followed for all systems that may perform backup recoveries.

Recoveries for RMAN backups are performed by the DBA team that supports those databases.

Recoveries for NetBackup backups are performed by the Unix team.

Recoveries from clones are performed by the Unix or NT team depending upon the OS type of the target system.

There is no formal periodic testing of backup recovery as the account has not provided any servers or disk space to perform such recoveries and recovery to the live server is not permissible unless a failure has occurred. There have in the past been operational recoveries of each type.

Audit retrievals are happening on a fairly constant basis driven by formal customer requests from POL. Audit retrieval is tested as part of an upgrade or change to the audit infrastructure such as firmware upgrades of the EMC Centera.

POLSAP retrievals also happen on a fairly constant basis as generating a report in SAP that spans a time period which is in the archive causes an automatic retrieval which is seamless to the user. There is no change control process, retrievals are automatic as part of the normal user reporting process. Report retrieval is tested as part of an upgrade or change to the audit infrastructure such as firmware upgrades of the EMC Centera.

4.8.3 Job Scheduling

4. ***Control Objective 4: Controls provide reasonable assurance that processing is appropriately authorised and scheduled and that deviations from scheduled processing are identified and resolved.***

#	Control
4.1	**Maintenance of Job Schedules:** Access to amend job schedules is restricted to appropriate Fujitsu personnel required to have this level of access by their role.
4.2	**SAP Schedules are continuously monitored**: The SAP Basis Team uses the SAP GUI and SAP transaction code SM37 to monitor the success / failure of SAP batch jobs. The SAP Basis team will also check and monitor the batch job start and end times and send the daily monitoring statistics to agreed parties.
4.3	**Failed job schedules are monitored and alerted**: Automated alerts are configured and sent to relevant parties upon the occurrence of a batch job failure. These are investigated in line with the incident management process.

4.8.3.1 HNG-X Job Scheduling

Scheduling of jobs within the data centre environment is an automated process using Tivoli. The Tivoli Workflow Scheduler (TWS) is used to orchestrate the execution of jobs within the environment. Each vertical application has its own set of tasks which are defined and TWS is used to schedule those and maintain the dependencies within that application.

The platform architect will outline the required jobs needed for that platform as part of the High Level Design (HLD) document. It is then the responsibility of Services Management Group (SMG) to help ensure that these jobs are appropriately configured within TWS through creation of the TWS schedule. SMG also performs day to day monitoring and management of the Tivoli toolsets.

If there are failures in the daily processing, alerts are raised to the Tivoli Business Service Manager TBSM module and TWS co-ordinates the reporting of the abnormal end of those jobs that are in error. These alerts are then identified as part of the SMC proactive monitoring of the TBSM module, further detailed in Control Objective 6. They will then raise a TFS ticket to the Unix Team based in IRE11 and ask them to investigate the failed schedule (**4.3**).

Access to maintain and amend schedules is restricted to the Systems Management Group based in IRE11 (**4.1**). If changes are required to the initial schedule that has been implemented, this will follow the standard MSC process. Please refer to Control Objective 8 for further details of this process.

4.8.3.2 SAP Job Scheduling

The POLSAP Basis team manages and maintains the batch scheduling (**4.1**). The details of the POLSAP batch is held in Dimensions, documented in POLSAP/DES/APP/SCH/TBC.

Dimensions has several roles in supporting services to POL including:

- Acting as a document management system.
- Acting as a software configuration repository.

The SAP Basis team performs the daily proactive monitoring of POLSAP–PLP system (**4.2**) which includes:

- General health check of all systems.
- The SAP Basis team will maintain the Batch Jobs scheduling document “POLSAP BATCH CATALOG” so if there are changes to the batch jobs then the document will be updated. This document is available on the project repository on the intranet.

- SAP batch jobs are maintained in the POLSAP R3 system.
- SAP batch jobs are monitored from SAP GUI through SAP transaction code SM37. This screen is monitored on a daily basis by the SAP Basis team.
- The SAP Basis team will also check and monitor all the batch job start and end times and send the daily monitoring statistics to agreed parties.
- The SAP Basis team will check and send the transaction response time to the agreed parties.
- The SAP Basis Team is responsible for the investigation and resolution of issues found with the batch jobs.

If the monitoring identifies an issue with a critical job (a critical job being defined as a job that is part of the team's daily monitoring list) the team will ask the SMC team to raise an incident on the Post Office-owned and managed Triole incident logging tool. The SMC team will then assign this incident to the appropriate resolving team. These tickets would then be managed through the standard incident management procedure that is described in Control Objective 6 (**4.3**).

If there is a batch job failure in POLSAP, the Solution Manager system is configured to trigger an automated alert to the SMC team. Based on that alert the SMC team will raise an incident in the Triole tool. This will then be handled using the Incident Management procedures described below.

If a change in the Schedule of the Batch jobs is required or a new Batch Job is required, an MSC is raised and once the MSC is approved the change implemented in the system by the Basis team.

4.8.4 Availability and Capacity Management

5. ***Control Objective 5: Controls provide reasonable assurance that system availability, performance and capacity are routinely monitored to help ensure that potential issues are captured and investigated.***

#	Control
5.1	**SAP Performance Monitoring**: The SAP Basis team regularly monitors table space and databases to help ensure there is sufficient system availability and capacity and that potential issues are captured and investigated.
5.2	**SAP Capacity Alerting**: An automated alert will be generated in the Solution Manager System (PLM) if the table space is more than 95% filled and the SAP Basis team will monitor and review these alerts.
5.3	**SAP Availability Alerting:** Automated alerts are configured in Solution Manager to advise if a part of the system is shutdown / not available for users. These alerts go to SMC team and they will create an incident.
5.4	**HNG-X Performance Monitoring**: The SYSMAN3 tool (Tivoli ITM) proactively monitors CPU, Memory, Disk utilisation and capacity of internal services on these platforms, raising alerts for investigation by the SMC as appropriate.
5.5	**HNG-X Capacity and Availability Monitoring:** The Tivoli ITM tool proactively monitors the availability of Wintel and Unix platforms, feeding platform availability data to Tivoli Business Service Manager (via Netcool Omnibus) about the availability of platforms. Tivoli Business Service Manager presents this data in a business context to the SMC, highlighting service affecting issues.
5.6	**Monitoring of Service Delivery:** A monthly Service Review Book is provided to POL to review its agreed Service Levels. Within this book are details of capacity, availability and incident management performance.

4.8.4.1 SAP Availability and Capacity Management

Details of the system availability and agreed SLAs are detailed in the OLA document held on Dimensions database. The document reference is *POLSAP/SVM/SDM/OLA/874.*

The SAP Basis team regularly monitors the Table space within the production databases; an automated alert will be generated in the Solution Manager System (PLM) if the table space is more than 95% filled (**5.1** and **5.2)**.

The SAP Basis Team also monitor the weekly and monthly database growth for the POLSAP system and based on that can plan the future growth of the database.

Automated alerts are configured in Solution Manager to advise if a part of the system is shutdown / not available for users (**5.3**). These alerts go to SMC team and it will create an incident and assign to the appropriate team (which again will be handled as per Incident Management process described in Control Objective 6).

The Athene product is used to manage the Component capacity of UNIX and Wintel Hardware on POA. This tool is located within the IRE11 data centre and its results are managed by the Capacity Manager in the SSC. The tool looks at the CPU, Memory, Disk utilisation and capacity of internal services on these platforms.

4.8.4.2 HNG-X Capacity and Availability Management

SYSMAN3 (Latest version of SYSYMAN3 is the Tivoli ITM Tool) is a generic name for the set of Platforms and software that provides System and Estate Management support to all HNG-X Platforms. This management includes the capture of availability information for the platforms via the IBM Tivoli Monitoring system and SYSMAN3 (**5.3**).

SYSMAN3 comprises the following applications:

Application	**Scope**
IBM Tivoli Monitoring (ITM)	Proactive monitoring of Data centre Platforms.
Netcool Omnibus	Event collection from: • Data Centre. • Branch Estate. • Networks (NNM). • EMC Storage. • Applications.
Tivoli Business Service Manager (TBSM)	Presentation of alerts and events in a business context.
Tivoli Provisioning Manager (TPM)	• Data Centre software provisioning. • Branch Router and Switch management.
Tivoli Endpoint Manager (TEM)	• Software distribution to the Branch Estate. • Reference data delivery to Branch Estate and Data Centre.
Tivoli Workload Scheduler (TWS)	Monitors and controls workflow throughout the POL infrastructure.
Netcool Reporter	Reporting Product for SYSMAN reports.
Oracle Enterprise Manager (Oracle Grid) (OEM)	Monitoring of Oracle Databases.

SYSMAN3 collects events using Tivoli Omnibus Technology and presents this to the SMC using Tivoli Business Service Manager (TBSM) views and alerts in a business' context, correlated to the application or system that is impacted.

WebTop, an Omnibus Graphical User Interface (GUI), is used to provide a filtered view of events that are not presented to the SMC within TBSM – particularly for Counter and Security Alerts.

One month's historical reporting from both TBSM and WebTop is available from Tivoli Reporter.

Events collected by a SYSMAN version are sent to the Audit Server.

The SYSMAN system, an earlier version of SYSMAN3, collects events from the counter estate including:

- Quality of Service.
- Operating System.
- Application and Branch Router.

Systems within the Data Centre are proactively monitored through the use of ITM, the Tivoli Monitoring tool. ITM agents gather the event data at regular intervals and measure the data against thresholds and alerts are raised if the thresholds are breached (**5.4**). ITM includes operating system agents that alert on CPU and Disk space events. Databases are also monitored using the ITM database agent. Custom Agents are used within HNG-X to capture:

- Radius Authentication Events.
- Netcool Event Statistics.
- BNS Statistics.
- HNG-X Application Statistics.

SYSMAN gathers alerts into Tivoli Omnibus using Omnibus event probes. Probes used within the HNG-X solution include:

- SNMP Traps.
- IRRELEVANT
-
- Windows Event logs.
- Text file (Application logs).
- IRRELEVANT

IRRELEVANT et

The Athene product is used to manage the Component capacity of UNIX and Wintel Hardware on POA. This tool is located within the IRE11 data centre and its results are managed by the Capacity Manager in the SSC. The tool looks at the CPU, Memory, Disk utilisation and capacity of internal services on these platforms.

The SSC receives reports from Athene detailing capacity on a regular basis.

Applications report their availability and capacity issues to the Business Systems Database and reports are reviewed from this on a monthly basis by the SSC (**5.5**).

4.8.5 Incident Management

6. Control Objective 6: Controls provide reasonable assurance that significant operations incidents are adequately reported, tracked, monitored through resolution and resolved timely.

#	Control
6.1	**Incident policies and procedures are in place:** Fujitsu has documented policies and procedures for managing incidents impacting the in scope applications which are available via CafeVik to Fujitsu teams.
6.2	**Incident prioritisation:** Incidents are assigned a priority in accordance with the severity levels agreed with POL.
6.3	**Incident resolution:** Incidents are handled in a timely manner, as per priority.
6.4	**Major & Security Incident review:** Once a Major or Security Incident is resolved there is a formal closure of the incident and a review including, if applicable a Root Cause Analysis.
6.5	**Incident reporting:** On a daily basis, the Fujitsu HSD / IMT reviews the number and severity of outstanding incidents in TFS.
6.6	**Alert handling:** The Tivoli ITM and Netcool Omnibus automate the collection of events and using Tivoli Business Service Manager highlight areas of concern to the SMC.

4.8.5.1 Incident Management Process

Fujitsu Post Office Account (POA) follows its own implementation of Fujitsu's Corporate Incident management process (**6.1**).

The process applies to all Incidents raised by Fujitsu's Help Service Desk (POA HSD) or by the System Management Centre (SMC) (out of hours or from systems monitoring tools), where they are related to the Fujitsu outsourcing contract. POL staff raise calls at POL's Network Business Support Centre (NBSC) and, where relevant, they are passed to the POA HSD or SMC. Calls presented to POA HSD / SMC that should be placed with Post Office Ltd.'s Network Business Support Centre (NBSC) are transferred/ referred from POA HSD / SMC to NBSC. Incidents are logged and managed using TFS which also produces status reporting on incidents. On a daily basis, the Fujitsu HSD / IMT reviews the number and severity of outstanding incidents in TFS (**6.5**).

The scope of the process is from the receipt of an incident by the HSD / SMC, through to the successful workaround or resolution of the incident.

The key objectives of the process are:

- Log, track and close all types of incident requests.
- Respond to all types of incident requests.
- Restore agreed service to the business as soon as possible.
- Resolve incidents within the target timescales set for each priority level within the Service Level Agreement(s).
- Resolve a high number of requests at first contact.
- Ensuring incident priorities are linked to business priorities.
- Keeping the user informed of progress.
- Reduced unplanned downtime.
- Improved customer satisfaction.

Fujitsu has defined an incident as "Any event which is not part of the standard operation of a service and which causes an interruption to, or a reduction in, the quality of that service".

Incidents are triggered by the following methods:

- All Incidents reported by Contact with the HSD / SMC. Contact is defined as voice or a Tivoli Alert generated by the Tivoli Event Monitoring tool as the methods of communication with the HSD / SMC and fall into the following categories:
    - Business process error.
    - Hardware or software error.
    - Request for information e.g., progress of a previously reported Incident.
    - User complaint.
    - Network Error.
    - Logging via HNG-X web interface.
- Severity and Service Level Target (SLT) information.
- Evidence of an Error.
- System Alerts received automatically from transaction monitoring tools (**6.6**). Due to the urgent nature of some of these alerts, they may be dealt with directly by the Fujitsu Software Support Centre (SSC), with an update of workaround or resolution supplied to HSD / SMC.

The initial detection stage is the responsibility of the HSD and SMC who receive calls from Users:

- Fujitsu Service Lines or Functions.
- POA IT Service Management.
- Third Parties.
- Fujitsu Service Delivery Management.
- Post Office Ltd, including Post Office Information Security.

These calls are recorded in TFS and are classified in one of the following ways:

- Advice and Guidance.
- Out of Scope.
- Quality Issue.
- Incident.

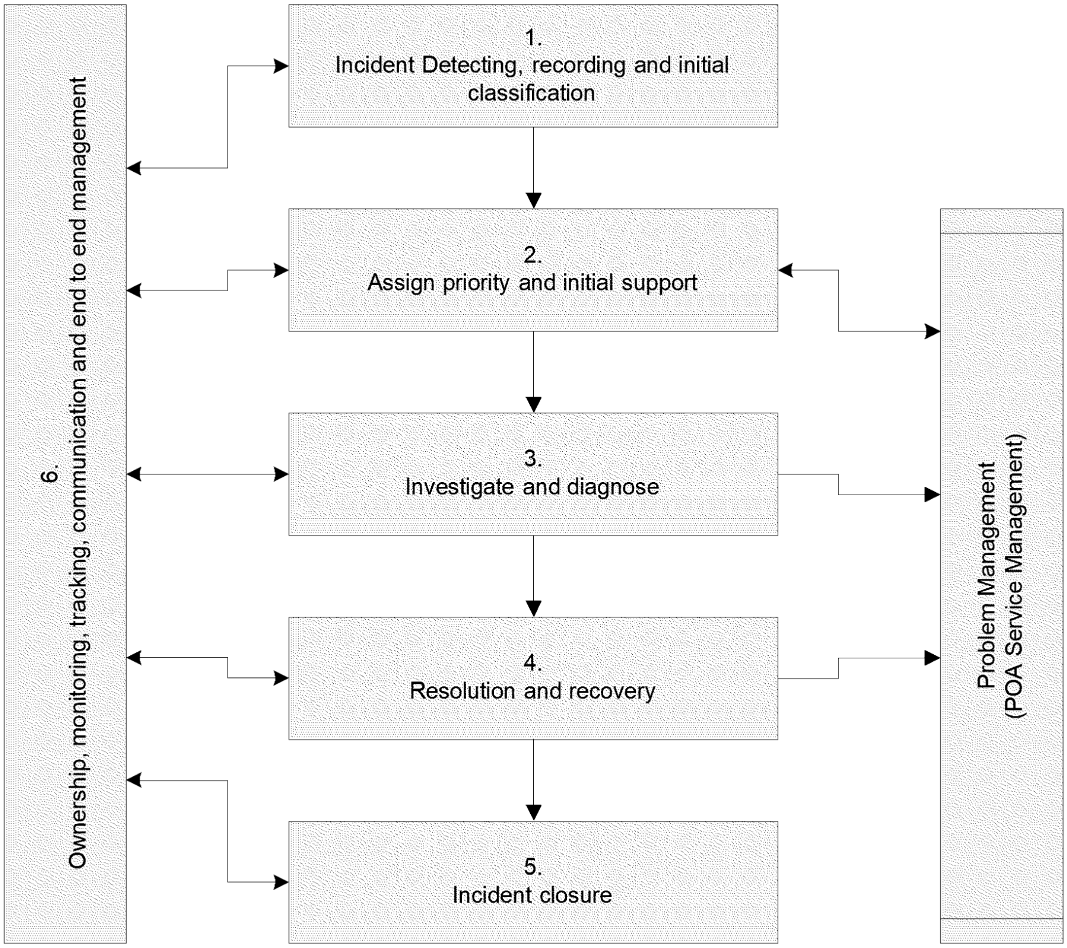
The first three above are referred back to Post Office NBSC and the last follows Fujitsu's incident management steps.

Once the details of the incident are recorded in TFS the HSD / SMC team assigns a severity level to the call (**6.2**). If the call is classed as a Security Incident or Major Incident it follows a different route detailed below. Call Priority for Hardware and Network calls is assigned in accordance with the Priority matrix as detailed in the agreed contractual Engineering Service Description.

The table overleaf does not indicate resolution times as Fujitsu is required to work to POL Service Level Agreements and availability targets and not incident resolution times (**6.3**). Major Incidents are therefore resolved in as short a time as possible dependent on the nature of the incident. The high priority placed on a Major Incident by Fujitsu's POA management team helps to ensure that the full resources required to resolve it are forthcoming.

Severity	Importance	Definition
A	Critical	• BUSINESS STOPPED, a Post Office unable to trade (where engineering cover available), unable to process any business, or central system failure which will result in a number of Post Offices being unable to process work. • Causes significant financial loss (as agreed between POL and POA Operations). • Results in data corruption or unrecoverable data loss.
B	Major	• BUSINESS RESTRICTED, a Post Office restricted in its ability to transact business e.g., 50% of counters unable to trade or trading with restricted business capability. • Has an adverse impact on the delivery of service to a number of end users. • Causes a financial loss that impacts POL and / or POA reputation (as agreed between POL and POA Customer Services). • If a PCI Major Incident process is invoked.
C	Medium	• NON-CRITICAL, a Post Office working normally but with a known disability, e.g., an interim solution (workaround) has been provided. • If a PCI Minor Incident process is invoked. • Has a minor adverse impact upon the delivery of service to a small number of end users.
D	Low	• Non-urgent. • Insignificant and usually cosmetic error, either a trivial documentation error or spelling error on the system.

The Incident Management process contains 5 stages as detailed in the diagram below and ownership passes between the various service lines and towers delivering the service.


1.
Incident Detecting, recording and initial classification
2.
Assign priority and initial support
3.
Investigate and diagnose
4.
Resolution and recovery
5.
Incident closure
6.
Ownership, monitoring, tracking, communication and end to end management
Problem Management
(POA Service Management)

If an incident is not a Security Incident or Major Incident then a check is made against the SSC KEL to establish whether the problem has been seen before and if there are known actions that need to be taken. If the KEL has information about the problem then the resolution or work around is applied and details are linked to the Master Incident / error log for this known problem.

If it is a new issue the TFS call is passed to first line support who will attempt to resolve the incident with the help of Product Support Engineers (PSE). If the call is resolved this is agreed with the Incident owner and the TFS call record is closed.

If the incident is not resolved, the TFS call is passed to the appropriate Service Delivery Unit (SDU) using the HSD / SMC Support Matrix and the Incident Management Team (IMT) are apprised of the position. For Hardware calls, the caller is given an indication of engineer arrival time, based on the Service Level Agreement (SLA) associated with the priority of the call.

If the incident is a known current issue then the caller is advised of the status of the problem and the TFS Master call updated with this occurrence and the SDU(s) managing the call's resolution are advised of another occurrence of the issue and the IMT are apprised of the position. The SDU investigates and diagnoses the Incident, based on the information in TFS, together with new information. The SDU also coordinates where sub-contract third parties are involved.

If the Incident has no associated KEL or it is complex and involves multiple SDUs, or if it has been unresolved for an extended period, the IMT will alert the POA Service Delivery Manager (SDM) to the existence of a pattern likely to produce a Problem.

The SDU will produce a workaround or resolution for the problem. The SDU then either applies the workaround or resolution or passes it to the HSD / SMC to implement. The Master Incident Record is the first call for an issue in TFS and is used as a tracking call for a major incident.

Where this Incident has a number of Calls referenced to it, or where there is a probability that proactive action is required to prevent further occurrences of this Incident the IMT will alert the POA SDM to the existence of a pattern likely to produce a Problem.

The Incident is then passed to the HSD / SMC to manage and if the call is resolved this is agreed with the Incident owner and the TFS call record is closed.

Throughout the Incident, the HSD / SMC retains ownership for monitoring and keeping the call raiser informed of progress, unless the incident is specifically software related, in which case SSC holds the responsibility for confirming details of closure.

The HSD / SMC manage the complete end-to-end Incident process. Their activities include:

- Regularly monitoring the status and progress towards resolution of all open Incidents.
- Keeping affected users informed of progress without waiting for them to call, thus creating a pro-active profile.
- Monitoring Service Level target (SLT) information and escalating accordingly if an incident looks likely to breach SLA thresholds.
- Updating HSD /SMC knowledge database from information supplied by SSC KEL. This may be applied as a direct copy or amended for use by the agents, dependent upon the technical complexity of the update.

4.8.5.2 Major Incidents Definition

As a general rule a Major Incident will always be an incident rated as severity level A (critical) in the POA BU Operations Incident Management Procedure document (SVM/SDM/PRO/0018), or a series of connected lower severity rated Incidents, which combine to have a significant business impact. However not all incidents rated at severity level A qualify as Major Incidents (**6.4**). This is because the severity levels do not necessarily translate to the global business impact on POL's business. For example a single counter post office which is unable to transact, regardless of its business volumes is rated as a Severity A.

For simplicity, Incidents are classified into three impact levels: High, Medium and Low.

High – An Incident that has occurred with a significant and potentially prolonged adverse impact on POL business. Typically these Incidents will initially require a significant amount of reactive management before they can be controlled and resolved.

Medium – An Incident that has the potential to cause significant impact to POL business but can be controlled and mitigated against through effective management.

Low – An Incident that requires business attention but if managed effectively will not have significant impact on POL business.

A Major Incident can be triggered by a range of causes including network triggers, application / service outages, hardware / infrastructure failures or security issues.

In the event of a Security Major Incident (which may also include PCI Incidents), the Security SDM MUST be alerted and they will then follow the Security Incident Management procedure as detailed in both:

- SVM/SDM/PRO/0018 Appendix A.
- SVM/SDM/PLA/0031 HNG-X Security Business Continuity Plan defines the actions to be taken if security violations are identified.

4.8.6 Major Incident Process

An initial impact assessment of an incident is undertaken by members of the IMT to determine if it should be classified as a Major Incident, taking into account as described above.

The Major Incident Manager will consult with the Business Continuity Plans to identify if potential Major Business Continuity Incident (MBCI) or MBCI triggers have been met and inform POA Business Continuity Manager if appropriate.

POL Service Delivery (SD) will be informed by the Major Incident Manager of the incident, and the incident will also be escalated to Fujitsu Service Delivery / Service Support team managers, if this has not already occurred.

With agreement from POA Service Delivery Manager/s, or Duty Manager out of hours, a Short Message (Phone text) will be sent to POA and POL Management alerting to the potential existence of a Major Incident.

Once a Major Incident is opened the relevant internal SDUs / Third Parties are contacted to initiate investigation and diagnosis and the Major Incident Manager opens a Major Incident Report which is held on SharePoint.

A Technical Bridge is scheduled, with a standard agenda, with all the relevant Service Delivery Units, IMT and Service Delivery Managers (SDM) and an agenda distributed. The Technical Bridge is technically focused.

The Technical Bridge aims:

- To discuss & agree the recovery investigation & resolution of Major Incidents.
- To provide a forum for up-to-date progress reports.
- To aid communication and, if necessary, support the Technical Recovery Manager (TRM) in producing a short term technical recovery plan and if appropriate longer term corrective actions. These will be included in the Major Incident (MI) report. This ensures that Major Incident progress is known by all, whilst also ensuring that all actions whether short term or long term is clearly stated.
- To collate information for inclusion on the Service Portal.

Attendees at the Technical Bridge include, but are not limited to, POA Service Management, SDU, Third Parties, POL, and POA Security & POL Security Managers.

If the outcome of the Technical Bridge is that the Incident is determined Business As Usual (low) then an SMS communication will be sent stating that the Incident is not a Major Incident, and the incident is then resolved using the standard incident management process.

The Major Incident Manager will also distribute actions (provided by the Technical Recovery Manager (TRM)), following the conference call.

If during the Technical Bridge a clear recovery path is identified, this is discussed and agreed on the call. Following agreement the recovery is implemented.

Following the Technical Bridge the Technical Recovery Manager will liaise with the SDUs and / or third parties during the investigation / recovery. If no clear recovery path is identified, the decision is then taken on whether to escalate for Service Bridge direction.

The nature of the Major Incident determines which POA BU Service Team members and POL Managers are involved in the Service Bridge.

The purpose of the Service Bridge is to:

- Provide appropriate direction on Incident resolution.
- Provide added impetus to restoration of service ASAP.
- Define communication intervals to Key Stakeholders.
- Provide focused Incident Management in line with the impact and severity of the Incident.

Once the Incident is deemed to be resolved, a final Technical Bridge is held to agree and confirm the resolution of the Incident. The Major Incident Review date is set at the final Technical Bridge. SMS communication is sent confirming resolution of the Incident.

A Draft Major Incident Report is distributed within 24hrs of resolution of Major Incident.

Once a Major Incident is resolved there is a Formal Closure of the Major Incident and a review of the Incident including consideration of:

- Lessons learnt.
- Incident definition.
- What went well?
- Timeline.
- Changes required to infrastructure.
- A review of the Major Incident Communication Procedure.
- Root Cause Analysis.
- Business impact.
- Action plan, including any changes requiring MSC's.
- Service Improvement Plan update.
- Review service risk(s) and update Risk Register as appropriate.

4.8.7 Security Incident Process

An information security Incident is: "an adverse event or series of events that compromises the confidentiality, integrity or availability of Fujitsu Services Post Office Account information or information technology assets, having an adverse impact on Fujitsu Services and/or POL reputation, brand, performance or ability to meet its regulatory or legal obligations." This will also extend to include assets entrusted to Fujitsu including data belonging to Post Office Ltd, its clients and its customers.

Fujitsu classifies Security incidents using one of two levels of severity:

- A MINOR incident will normally have limited and localised impact and be confined to one domain.
- A MAJOR incident will have a significant impact on the Network Banking Automation Community.

NB. For a Major Incident the POA Major Incident Process (SVM/SDM/PRO/0001) is followed.

Whenever a security incident is identified which presents a serious threat to conducting normal business it is contained and isolated as quickly as possible.

A security Incident is first notified to a person's Line Manager. The Line Manager gathers as much detail of the incident as possible, following Fujitsu BMS procedures. He or she will undertake an initial local investigation into the incident, seeking to ensure that in the case of missing equipment or materials that they have not just been misplaced. Information gathered will be entered into the initial Fujitsu case report template (ICR).

If the severity of the Incident is considered as Minor but warrants further investigation, the Line Manager would immediately log a call with the Horizon Service Desk (HSD), stating that they are reporting a security incident, giving brief details. Having logged the call and obtained a call reference number, the Line Manager may then continue with the investigation if they believe the incident warrants this, and act as a liaison between the person reporting and all concerned parties. All Incidents reported to the HSD with a call reference and even when classified as Minor are still forwarded to POA Security Management to determine if there is a Security Impact.

If the severity of the Security Incident is considered as Major, the Incident details are reported directly to the POA Security Manager immediately. Depending on the type of Incident and the severity of the incident, POA Security makes the decision to escalate details to the POL Security team. In the case of Data Centre incidents specifically, POA Security also informs the Data Centre Manager if this has not already been done. Regardless of the severity of the incident, when a compromise in card data occurs, the incident is reported to POL Security so that POL can comply with its contractual obligations with its card acquirer.

Once a call is raised with the SSC the call is then placed on the call stack of the POA Security Team, which monitors the incident, assists or advises the Line Manager if required, and is available to take over the investigation should the need arise, but always be able to respond, within 2 hours of the initial call being made.

In most cases, the initial investigation of a reported incident is carried out by a nominated investigator normally the POA Security Manager or his nominated deputy. POA and POL Security Teams will be on hand to provide backup and assistance if required. The investigator will endeavour to obtain as much original evidence as possible. In the event of a court appearance the court prefers the original evidence rather than a copy but will accept a duplicate if the original is lost or destroyed or is in the possession of a third party who cannot be subpoenaed.

Following the initial investigation and where considered appropriate, the investigator reports to / liaises with the local Police and / or other external Agencies; this will only be done following consultation with the POL Head of Security and POL Head of Information Security or substitute.

Copies of the initial and follow up reports are submitted to relevant authorities and details of investigations are held on file by POA Security to aid subsequent trend analysis.

When the final report of an investigation has been completed, it is passed to the relevant authority for follow up action, the results of which are referred back to the POA Security Manager.

When an investigation is closed the POA Security Manager seeks to ensure that details of the investigation have been recorded and can be made available for subsequent future analysis.

On call closure, the POA Security Team completes and notifies CPNI where required. Thereafter the incident is reviewed to identify the lessons learnt and the processes and relevant documentation is updated as appropriate.

4.8.7.1 Security Incident Trends and Checks

POA Security Team carries out a monthly check of investigations and creates a summary report highlighting incidents to the POL Head of Information Security.

The report highlights trends or weaknesses which may need to be raised at future Information Security Management Forums (ISMF).

Details from the monthly reports may also be considered suitable for Line Managers.

4.8.8 Network Incident Management

Incidents relating to network problems are managed using the standard incident management processes and controls described above.

4.8.9 Networks

7. ***Control Objective 7: Controls provide reasonable assurance that networks are managed to contractual and site requirements, monitored for availability and response times and issues are identified, tracked and resolved.***

#	Control
5.6	**Monitoring of Service Delivery:** A monthly Service Review Book is provided to POL to review its agreed Service Levels. Within this book are details of capacity, availability and incident management performance.
7.1	**Network performance criteria:** Network availability and performance requirements are clearly defined between Fujitsu and POL in the Network Service descriptions and network service is measured and monitored using these agreed service levels.
7.2	**Network change management:** Network changes are managed using the standard Fujitsu MSC process including authorisation, testing (where deemed appropriate) and approval of changes before they are implemented.
7.3	**Network availability monitoring:** Network availability is monitored using several tools which send automated alerts to the Network Operating Support Service Team (NOSS) if key components are unavailable, or if traffic levels breach predefined thresholds.
7.4	**Network incident management:** Incidents relating to network availability are managed using standard incident management procedures used on the POA, and are included in the standard incident management reporting to POL.

4.8.9.1 Network Service Description

POL defines the network services it requires from Fujitsu in two contract controlled documents - the Branch Services Network Service Description (SVM/SDM/SD/0011) and the Central Network Service description (SVM/SDM/SD/0012) (**7.1** and **7.2**).

4.8.9.2 Provision of the Network Service

Fujitsu provides a network service to POL using its Hosting and Network Services (HNS) teams. These teams provide technical support and implementation for the following products and platforms:

- The HNS Post Office Account Network team based in Warrington supports Cisco Routers, Switches, Load balancers and Firewalls.
- A separate team also based in Warrington supports the Intrusion Detection System (IDS) and proxy servers (McAfee Web Washer & Bluecoat Proxy SG).
- A centralised Network Operations Support Service (NOSS) overviews and monitors the systems.

Wide Area Network Services are provided through a number of third parties depending on the circuit or communications requirement.

Controls operated by these third parties are outside the scope of this report.

4.8.9.3 Network Change Management

Fujitsu follows the MSC change management structure for all changes to Network equipment as described below in section 5.9.9 which describes Control Objective 8 (**7.3**).

4.8.9.4 Network Availability Monitoring

Fujitsu has its own dedicated Network Operating Support Service to monitor the availability of Network Services to POL using TFS to raise problems or incidents to the Network, Firewall or IDS teams and where applicable the Incident management process (described under Control Objective 6) is used to resolve these (**7.4**).

4.8.9.5 Network Service Monitoring

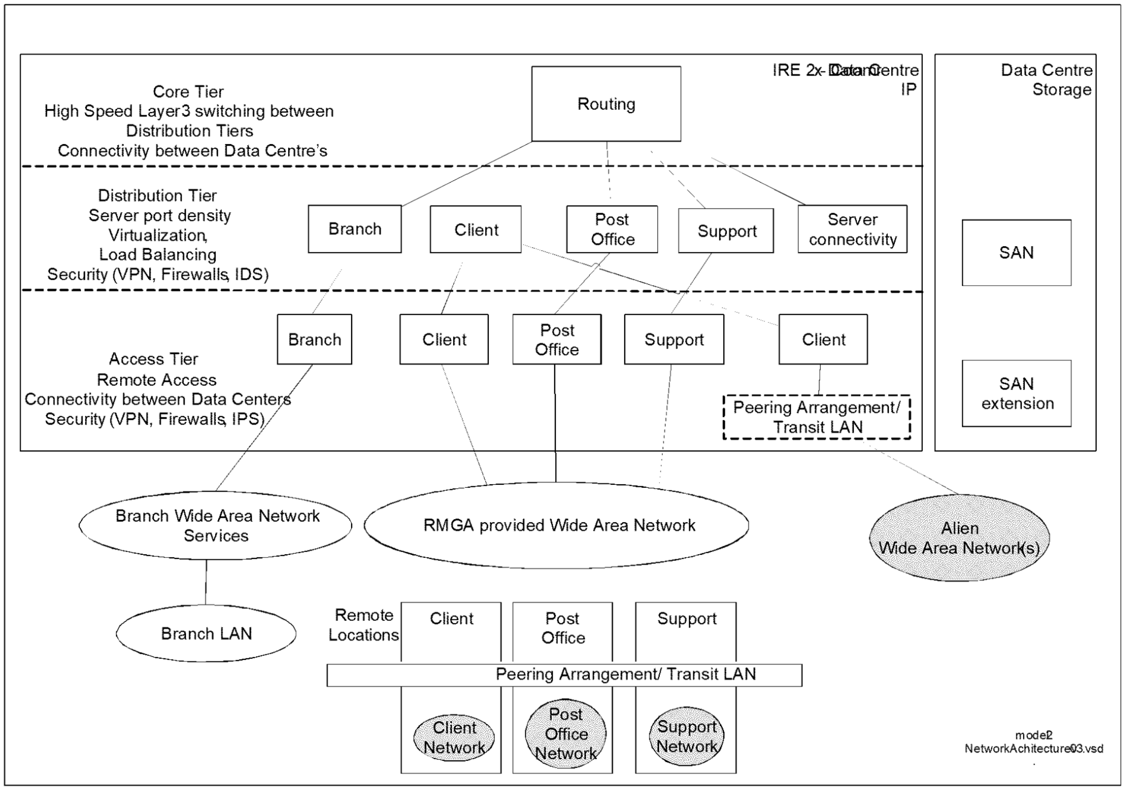
A monthly Service Review Book is provided to POL to review its agreed Service Levels and within this book are details of Network performance. This book is jointly reviewed monthly at a Service Review Board and network performance is included (**7.1**).

4.8.9.6 Overview of Network Technical Design

The Network that Fujitsu provides to support its services and applications to POL is divided into the following at the top level:

- IP Network Space Data Centre Networks.
- Branch Networks.
- Transit Networks.
- Wide Area Networks.

As shown in the diagram on the next page:

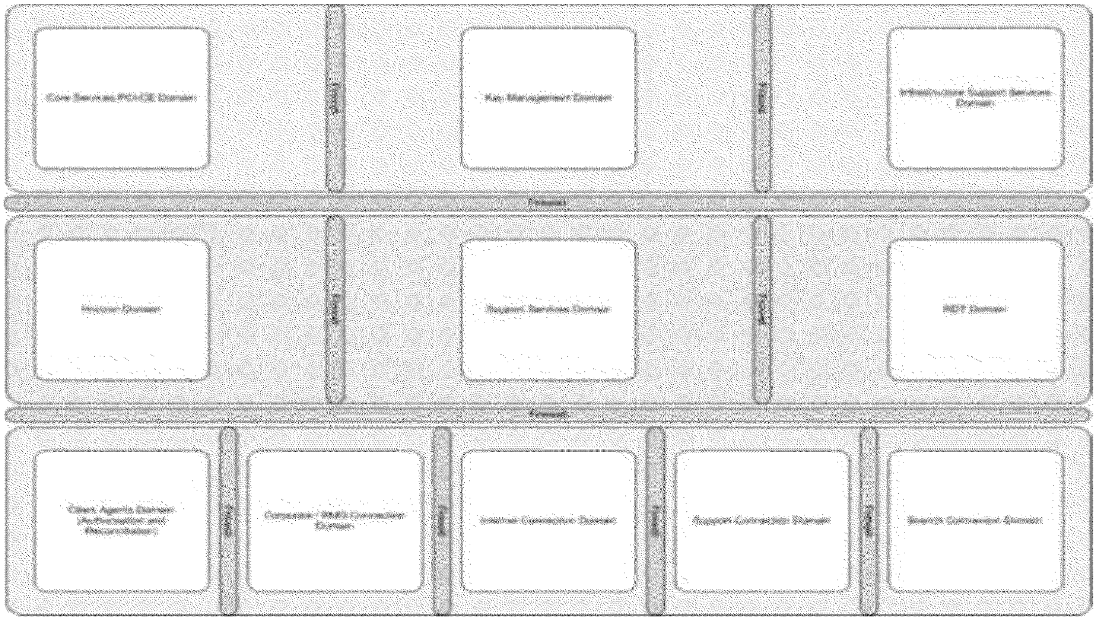


Testing is provided through the standby data centre for Live System Test and System and Volume Integration during normal operations. This test support would disappear if the standby data centre was required to act as the primary. Under normal business as usual conditions the traffic is segregated with access between production and test environments prevented by means of various physical and logical means of separation as appropriate. Change Management is strictly controlled through a variety of internal change & release processes and procedures – see below for more information on change management for network components [Control Objective 8).

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

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

The following diagram illustrates how Network Domains fit within the Network tier model.


Core Services PCI-CE Domain
Firewall
Key Management Domain
Firewall
Infrastructure Support Services Domain
Firewall
Horizon Domain
Firewall
Support Services Domain
Firewall
RDT Domain
Firewall
Client Agents Domain (Authorisation and Reconciliation)
Firewall
Corporate / RMG Connection Domain
Firewall
Internet Connection Domain
Firewall
Support Connection Domain
Firewall
Branch Connection Domain

Network Domains are the basic building blocks for enforcing security in the Network.

The Domain structure places a logical ring around the logical Security Perimeter of the HNG-X Network in the data centre, but this perimeter extends beyond the data centre in some cases and is protected by means of IPSEC VPN technology using access lists to allow specific classes of traffic to enter HNG-X. More specifically, this perimeter can be best described as the collection of devices managed (or monitored) by Fujitsu Services. At the boundary of these managed devices a firewall (hardware or software-based) will be located, and the perimeter will be secured according to firewall guidelines laid out in ARC/NET/ARC/0001.

4.8.9.7 Network Asset Management

Network Assets are managed through Cisco Works Inventory along with an offline hardware inventory register. Hardware and Software maintenance is on a business case basis and is based on business availability targets.

4.8.10 Change Management

8. Control Objective 8: Controls provide reasonable assurance that modifications to system software and networks are authorised, tested, approved, properly implemented and documented.

#	Control
8.1	**Change management:** The MSC toolset is used to manage all changes with a joint decision between Fujitsu and POL as to which parts of the tool are relevant for a change.
8.2	**Change approval:** All changes must be authorised by the Fujitsu Duty Manager or technical bridge, with approval being documented in the MSC system. Changes that cause major service interruption must also be authorised by the Change Advisory Board (CAB), with approval being documented in the meeting minutes and within the MSC system.
8.3	**Emergency Changes:** A change deemed necessary in order to resume live service will be agreed and authorised and documented during the incident along with updates to POL at an agreed timeframe dependent on the severity of the incident.

4.8.10.1 Business as Usual Change

All change is subject to the Managed System Change (MSC) change process whether it requires changes to existing services or the managing of new services or functionality (**8.1**). Key change types that fall into scope for this process are listed below:

- Changes that require physical access to or are making changes to POL services being hosted in the Data Centre.
- Changes that are requested to be shared by POL data centre or Branch Counter estate by either:
    - A supplier i.e., BT, C&W, the Data Centre utility suppliers etc.
    - Shared networks.
    - Shared infrastructure.
    - Account specific infrastructure.
    - Account specific networks.
- Changes that require the release of an application software change or support patching / security patching changes.
- POLSAP service offering change.
- Credence service server support changes (note these relate only to hosting of the service).
- On-line services changes.
- Changes as the result of an Incident.
- Changes to resolve a Problem.

These changes include POL authorised project work with Fujitsu or POL 3rd Party or POL Network Partners. These types of changes are supplied by POL and are then recorded in MSC and assessed / reviewed by Fujitsu staff with issues or concerns fed back to POL.

The Manage Service Change (MSC) operational change process uses the Fujitsu MSC toolset to progress the change through control gates which are described overleaf.

The MSC toolset is secure and auditable (at both system and user levels with time stamping being employed). As changes are made to a change record and it progresses through the control gates listed below with permissions and ownership of the change recorded at the various stages.

Both POL and Fujitsu change control teams participate in tailoring the questions in the MSC toolset to enable the relevant information to be obtained for POL's internal change process. This helps their network partners and third party suppliers assess a Fujitsu-controlled change for risks and impacts. These controls, along with the KPIs established by POL to monitor the MSC toolset information standards for quality, timings of the notice of the change etc., help to ensure the efficient and effective control and management of operational change.

Once a change is ready to be tested it becomes subject to the Manage Service Change (MSC) process. Change Advisory Board (CAB) approvals are obtained before deployment can begin, with approvals documented both in CAB meeting minutes and within the MSC system (although these are not formal signoffs, for example, they can be copied in from POL e-mails).

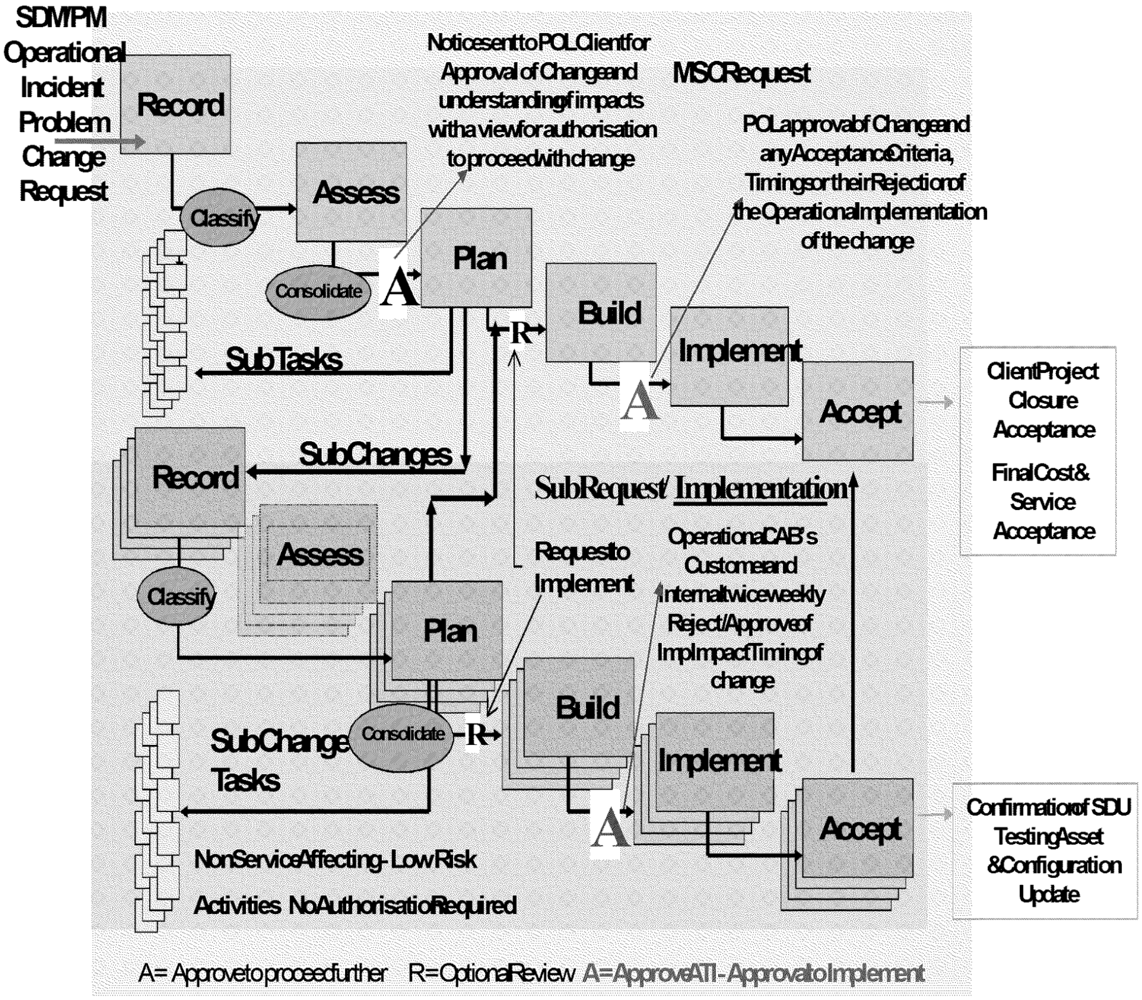
The control gates to be established around change are:

- The request for the change from POL (projects).
- The establishment of a Design Proposal by POL (projects).
- The acceptance of the Design Proposal by Fujitsu (projects).
- POL raises a Change Request (CR) or a Contract Technical Change (CT) or Contract Change Notice (projects).
- Fujitsu raises a Change Proposal (CP) to impact change (projects).
- Costs and Impacts are sent to POL and approved or rejected (projects).
- If accepted, then a set of Requirements is jointly agreed with POL (projects).
- A project is initiated and project plans drawn up (projects).
- Architecture, High Level Designs and Low Level Designs and interface documents are written and where appropriate discussed with POL.
- Development of Code is undertaken (projects).
- Code is tested by development (projects).
- Code is packaged by integration into Dimensions ready for delivery to System Volume and Integration Test or Live Systems Test (projects).
- Code is tested by Solution Validation & Integration (SV&I) and Live Systems Test (LST) based on project plans from requirements (projects).
- Tickets are raised in the PEAK system (these are known as PEAKS) for defects identified by SV&I and / or LST (projects).
- Defects are fixed and follow Test cycle until approved (projects).
- Consecutively to Code Development platforms are built where appropriate using current standards (projects).
- Platforms are tested in conjunction with the code in SV&I and LST (projects).
- PEAKS are raised for defects (projects).
- Defects are fixed and follow Test cycle until approved (projects).
- To deliver integration packages to SV&I & test the recording of the change takes place in MSC and contains appropriate release notes and details (Projects).
- MSC is used to Record and authorise BAU changes also (Operational changes).
- The MSC systems records assessment by other potentially impacted teams to determine risks associated with the change in their area (Operational Changes).
- The MSC systems contain a plan of the change (Operational Changes).

- The MSC team agrees the change internally and with the customer where relevant at CABs, (Operational Changes).
- The CAB review helps to ensure (Operational Changes):
  - the change meets the governance requirements;
  - the change does not overlap with other changes;
  - that the change has considered any group or associated further risks and impacts by doing the change; and
  - the CAB follows the standard CAB Terms of Reference (TOR) which defines:
    - Attendees.
    - Sign off or rejection or associated actions.
    - Recording and issuing of minutes from the CAB.
    - Updating the MSC toolset with the CAB decision.
- The Change Manager satisfies themselves that the change has (Operational Changes):
  - Met all areas of governance.
  - Considered impacts / risks.
  - CAB agreement for the change to proceed is in place.
- If the above are in place, the Change Manager authorises the change within the MSC system to proceed and implement the change (Operational Changes) (**8.2**).
- Post implementation outcomes of change are recorded in post implementation review and records are updated and success criteria examined and lessons learnt are documented (Operational Changes).
- Change close down (Operational Changes).

In summary, MSC is a Fujitsu toolset that allows a securely accessed, time stamped auditable system to record change, provides Service Delivery Units and Service owners with audit trails and gives reasonable assurance that modifications to software and infrastructure are assessed for risks & impacts. The changes are authorised by the Service owner and Change Manager, are tested by appropriate methods and teams, and are approved to be deployed to a live environment subject to testing results, they are implemented by the authorised and approved teams and the changes are documented into new or existing documentation.

MSC Process Steps - Overview



SDM/PM Operational Incident Problem Change Request

Record

Classify

Assess

Consolidate

A

Plan

R

Build

Implement

A

Accept

Sub Tasks

Notice sent to POL Client for Approval of Change and understanding of impacts with a view for authorisation to proceed with change

MSC Request

POL approval of Change and any Acceptance Criteria, Timings or their Rejection of the Operational Implementation of the change

Client Project Closure Acceptance

Final Cost & Service Acceptance

Record

Sub Changes

Assess

Classify

Sub Request / Implementation

Request to Implement

Operational CAB's Customer and Internal twice weekly Reject/Approve of Impl Impact Timing of change

Plan

Build

Implement

Sub Change Tasks

Consolidate

R

A

Accept

Confirmation of SDU Testing Asset & Configuration Update

Non Service Affecting - Low Risk Activities No Authorisation Required

A= Approve to proceed further R=Optional Review A=Approve ATI - Approval to Implement

18 ©Fujitsu Services 2006 Alan Flack Manage Service Change

4.8.10.2 *Emergency Changes*

Emergency changes are progressed through one of two methods:

- a service incident; or
- the emergency CAB (E-CAB) process.

Both processes will document changes required in the MSC toolset.

A service-affecting incident sees a Technical Bridge convened (see the Incident Management section of this document above – Control Objective 6) to analyse the cause and impacts of the incident. This team will include service managers, an incident manager and technical staff and the Operational change manager. Any change deemed necessary in order to resume live service will be agreed and authorised and documented during the incident along with updates to POL at an agreed timeframe dependent on the severity of the incident.

If the level of the emergency is at lower level such as a disk failure the resolver (often an incident manager) will request that an E-CAB is called. The Change manager will call the E-CAB meeting together following the process as documented in the CAB Terms of Reference (TOR) via a conference call to discuss the change with both technical staff and service managers. The MSC record will be E-mailed around the mandatory assessment teams with a timeframe turn round of assessments within an hour and documented with the Incident Management documentation. The incident or change manager will contact POL Change Control to discuss the emergency and ask for verbal permission to proceed during which time the Fujitsu change Administration staff will send the change to POL Change Control for their records (**8.3**).

9. *Control Objective 9: Controls provide reasonable assurance that new or modified application software development efforts are authorised, tested, approved, properly implemented and documented.*

#	Control
9.1	**System Development and Maintenance policies and procedures:** Fujitsu has a formal Systems Development Life cycle (SDLC) which incorporates phases including initiation, Requirements, Definition, Design, Development, Deployment and Maintenance.
9.2	**Change Control Board:** Depending on the nature, changes must either be approved by the Change Control Board (CCB) before progressing into development or by the PEAK Targeting Forum (PTF).
9.3	**Design Proposal:** Projects are outlined in a Design Proposal (DPR) that is held in DOORS or Sharepoint and is reviewed and approved by POL as well as Fujitsu management.
9.4	**Change Testing:** Changes are tested in line with the defined procedure.
9.5	**Ability to implement changes:** Only appropriate individuals have access needed to move code builds between environments or promote transports to live. Segregation of duties is enforced between users able to develop and implement changes.
9.6	**Approval to implement changes:** POL approval is required to promote software changes to the live environment. Approval is captured within the relevant MSC.

Fujitsu's change management process consists of two components - Project Changes and Business as Usual (BAU) changes. Project Changes relate to the delivery of new or changed services and BAU Changes to Operational changes to the live service provided to POL (**9.1**).

4.8.10.3 Project Changes for HNG-X and SAP

External requests for changes will be raised on a Change Request (CR) and sent electronically to Commercial Change Management (ChM) and allocated to a Change Owner and converted into a Change Proposal (CP).

All CPs are initially reviewed and impacted by Programme teams and impacts are returned to ChM where they are collated and shared with the Change Owners. Where appropriate the CPs indicate that they have the Design Authority Board (DAB) approval.

Once reviewed, CPs will be submitted to the Programme Change Control Board (PCCB) for agreement to progress the CP. The PCCB typically meets weekly. The PCCB is chaired by ChM and brings together representatives from a wide range of functions potentially affected by proposed changes.

Once the PCCB has assessed and agreed the progression of a CP, it will be submitted to the Change Control Board (CCB), which includes the Account management team, with a recommendation from the PCCB as to whether the CCB should approve or reject it (**9.2**).

The CCB typically meets weekly. Change Owners are required to attend to sponsor the change detailed in their CP. The CCB consists of members who represent the key functions within the Account to help ensure that if the CP is accepted for implementation it will:

- **Commercial / Finance**
  - Have no adverse financial or commercial implications.
  - Not increase the overall risk to the Account / Customer contract and Service commitments.
- **Customer Service**
  - Be operationally supportable and will meet the Account's service obligations.
- **Development**
  - Be developed within the agreed timescales to the required quality level.
- **Architects**
  - Be constrained within the overall architectural solution and is technically viable.
- **Testing**
  - Be tested and integrated to the required quality level within the agreed timescales.
- **Business Management**
  - Not inhibit the Account in exploiting future business opportunities for the Account and its Customers.

A minimum of three Directors are required to be in attendance for a CCB to be able to reach a decision on CPs.

Minutes from both of these meetings showing approval of the CP are held in PVCS (Project Change database).

Once the CCB has approved a change the following occurs:

- If the change is internal the Programme team is advised, time codes and plan activities are set-up and work can start.
- If it is external, the change will be submitted to the customer (electronically and hard-copy) and POL reviews the change until formal agreement which then allows the CP to be progressed.

Work on a project will not begin unless approval is in place.

Project Changes are allocated unique numbers and lodged within a database (PVCS) and related accordingly. These can be viewed by all members of the team working on that project but can only be updated, edited and actioned by members of ChM.

All Minutes from the Change Boards (PCCB and CCB) and actions from the same are recorded in the change history of the change vehicles in the database.

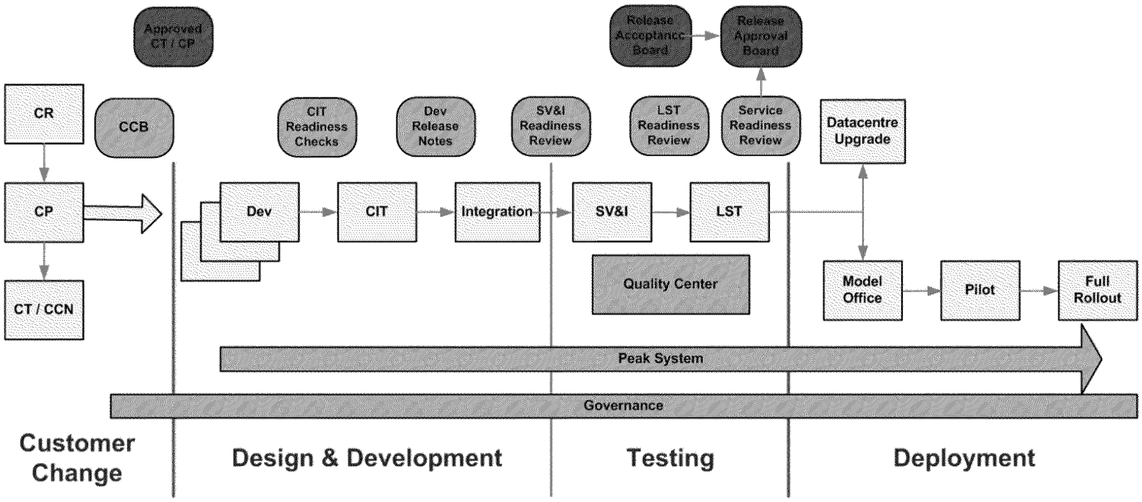
Comments and decisions around the changes are also lodged in the change history.

CP Impacts are collated into CP specific files and stored on a back-up server.

Approvals from the CCB and POL are documented in the relevant change history.

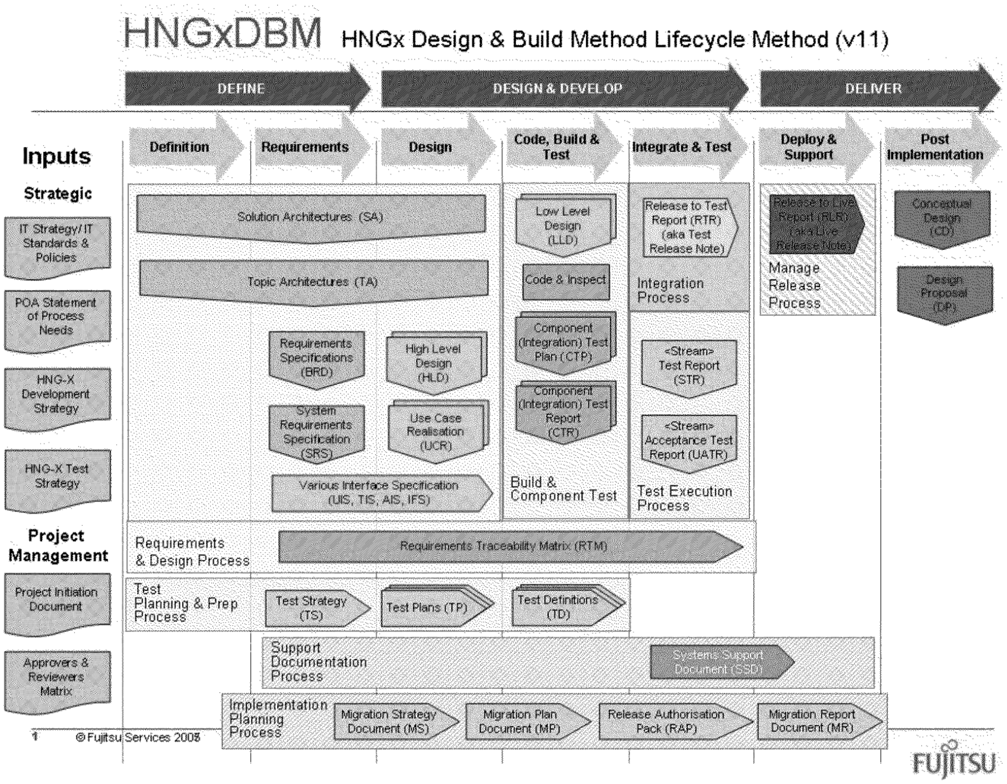
4.8.10.4 Projects for HNG-X

Fujitsu follows its Corporate Methodology outlined in the diagram below to deliver a project to POL. Each project has clear requirements, is designed, tested and deployed prior to its acceptance into the Live Production Estate. All projects are assigned a Project Manager to deliver the specific project with oversight of all projects by the Programme Director.



The diagram below shows an overview of the design and builds methodology used by Fujitsu to define, design, develop and deliver a project into the POL production environment.

This Methodology is used for HNG-X projects and projects that integrate HNG-X and SAP.


HNGxDBM HNGx Design & Build Method Lifecycle Method (v11)
DEFINE
DESIGN & DEVELOP
DELIVER
Inputs
Definition
Requirements
Design
Code, Build & Test
Integrate & Test
Deploy & Support
Post Implementation
Strategic
IT Strategy/IT Standards & Policies
POA Statement of Process Needs
HNG-X Development Strategy
HNG-X Test Strategy
Project Management
Project Initiation Document
Approvers & Reviewers Matrix
Solution Architectures (SA)
Topic Architectures (TA)
Requirements Specifications (BRD)
High Level Design (HLD)
System Requirements Specification (SRS)
Use Case Realisation (UCR)
Various Interface Specification (UIS, TIS, AIS, IFS)
Low Level Design (LLD)
Code & Inspect
Component (Integration) Test Plan (CTP)
Component (Integration) Test Report (CTR)
Build & Component Test
Release to Test Report (RTR) (aka Test Release Note)
Integration Process
<Stream> Test Report (STR)
<Stream> Acceptance Test Report (UATR)
Test Execution Process
Release to Live Report (RLR) (aka Live Release Note)
Manage Release Process
Conceptual Design (CD)
Design Proposal (DP)
Requirements & Design Process
Requirements Traceability Matrix (RTM)
Test Planning & Prep Process
Test Strategy (TS)
Test Plans (TP)
Test Definitions (TD)
Support Documentation Process
Systems Support Document (SSD)
Implementation Planning Process
Migration Strategy Document (MS)
Migration Plan Document (MP)
Release Authorisation Pack (RAP)
Migration Report Document (MR)
1
© Fujitsu Services 2008
FUJITSU

4.8.10.5 Definition

POL defines projects according to their defined business needs and provides these to Fujitsu as documented requirements and acceptance criteria.

4.8.10.6 Requirements

Requirements are managed within Fujitsu by the Requirements manager.

POL defines a requirements baseline and where applicable a baseline design proposal (DPR) and Fujitsu may be requested to assist POL in the preparation of these (**9.3**). These requirements are stored within the POL DOORS system and replicated within Fujitsu and exceptions, non-compliances etc. are recorded in the Design Proposal and in the Commercial Terms response to POL. The DOORS system is jointly managed by Fujitsu and POL and is used to contain the documentation of the requirements for changes.

The Design Proposal contains 3 key elements:

- The Acceptance Criteria.
- The Work Packages that are built to deliver the project.
- The Monitoring Criteria for the project after go live.

There is no formal POL sign off of the DPR however they are involved throughout the process and through the use of DOORS have visibility of the detailed requirements that the project must deliver. Once POL has approved the detailed requirements in DOORS this is taken as approval of the overall DPR by POL.

4.8.10.7 Design

Application Development for the in scope applications will be performed by a range of Fujitsu teams depending on the nature of the project.

4.8.10.8 SDLC Methodology

POA Design and Build Methodology (DBM) engineering lifecycle was derived from the Fujitsu corporate Applications Design and Build Methodology (ADBM), Infrastructure Design and Build Methodology (IDBM) and Test & Validation lifecycles (**9.1**). This is the SDLC currently used by Post Office Account (POA) team to modify existing or develop new applications for Post Office Limited (POL). It is defined in the standard document sets that are specific to the in scope applications.

High level designs (HLD) and Low-level designs (LLD) are the way Fujitsu meets the relevant Design Proposal requirements and these are stored in Dimensions or SharePoint. The HLD's and LLD's for HNG-X projects are approved by one of the approvers defined in PGM/DCM/ION/0001 & PGM/DCM/PRO/0001. SAP HLD's and LLD's are approved more informally within the SAP teams (**9.3**).

4.8.10.9 Code Build and Test

The Development Manager is responsible for the building and testing of code. Code is built in a segregated environment using appropriate repositories. These repositories use standard code management tools including locking, the booking of code in and out and the management of changes. Each project will have a Development manager who will take the relevant HLDs and LLDs and allocate these to developers. The Development manager will also develop their own project plan to track progress of the code development and testing. Code will be booked out by developers and worked on within the context of this project plan.

A generic code review template is used to review the code and it is approved by the Team Leader or Senior Designer once outstanding issues are resolved. The resulting review document is stored in SharePoint.

Individual Developers are responsible for producing Unit Test plans and reviewed by a separate developer. The initial developer will then develop the Unit Test plan which will be signed off by the reviewer, a developer will then execute the unit test plan and the results are recorded by the Developer in the Unit Test plan – usually as an appendix and the combined Test plan and report is stored in SharePoint / Dimensions. This evidence of results of testing is then signed off by a separate developer.

Component Integration Testing (CIT) is an independent testing phase that carries out initial integration of developed components it is performed to a CIT test schedule produced by the CIT tester and the schedule is updated with test results and stored in SharePoint / Dimensions. A formalised defect management (JIRA / Quality Centre) is used to record and track issues to resolution. The CIT testing is undertaken in a segregated environment under the supervision of the CIT manager.

Approval to move from the Code build and Test phase is an informal process agreed by the Development Manager and CIT manager. Once the Development is assessed as passing CIT the Development team will use one of the standard tools to create a deployable build of the updated / new software, they will then place this build into Dimensions for integration to then load into the next test environment. Development only have access to place the build into Dimensions, they cannot then move it into the next test environment.

4.8.10.10 Integration and Test

HNG-X has 2 test streams responsible for testing software changes to the live estate:

- Solution Validation and Integration (SV&I):

- Testing against Requirements - Functional and Non Functional covering business and infrastructure and based on testing the complete integrated solution.
- Has End-to-End capability for testing with 3rd parties e.g., Merchant Acquirer.

- Live Support Test (LST):
  - Final pre-production proving and release deployment validation.

The development-written test automation framework (documented in TST/SOT/HTP/0976) has been deployed into the SV&I environment to support testing. This automation framework offers the benefits of unattended execution, and allows the expansion of the automation suite to encompass a larger share of the regression test overhead.

Testing uses Quality Centre as the test management and defect management tool for defect management. Quality Centre interfaces with Peak which is the POA Development Defect Management System:

- Adherence to gateway criteria such as test stage entry criteria.

Entry into each test stream (or test cycle within test stream) will be subject to review against a pre-defined and agreed set of entry criteria. These criteria are set by the Test stream manager. Similarly testing within each stream will not be considered complete until the testing is adequately reported and a resolution path for all outstanding issues is understood (**9.4**):

- Progressive, incremental development, testing and acceptance.

Each test cycle is subject to entry criteria acceptance. Quality Centre is used to store and measure progress against project requirements. An assessment of requirements coverage is produced towards the end of test completion. This feeds into the Acceptance Process which is a joint board (with POL) with agreed criteria for acceptance.

4.8.10.11 SV&I Testing Process

Test Analysis is based on Requirements and high level designs. Test cases are documented in Quality Centre (QC) and details are extracted into a High Level Test Plan for each release. This document is reviewed via POA document management.

Entry into Test Cycles is controlled by Test Readiness Reviews.

Test Execution is recorded in QC and defects are recorded within QC.

Daily and Weekly reports are produced using QC to produce statistics e.g., test coverage.

After the last cycle of testing (pre LST) a report is produced covering the full release.

4.8.10.12 LST Testing Process

Testing is controlled via the Release Management team.

Release Planning sessions identify maintenance test slots and Peak targeting Forums assign defects into appropriate maintenance releases.

Release Management engage with test via Release Notes and Deployment plans.

LST put test plans together which are held in SharePoint and once testing is complete these are updated with results. LST assess test results and determine a release sign-off or release rejection position. The final document is attached to the release peak which is returned to Release Management.

4.8.10.13 Acceptance

The Acceptance phase is managed by the Acceptance manager. The Acceptance manager will review the progress of the testing teams in completing the testing specified for each acceptance criterion in the design proposal (**9.6**). The results of testing are summarised in the Acceptance Report. This is then discussed by the Acceptance Assessment Board which reviews the Acceptance Report including Acceptance Incidents. An acceptance incident is where the acceptance criteria have been tested and either not met or are partially met.

A joint Release Acceptance Board is then held with POL to agree how to progress the Acceptance Incidents and overall whether the project as stand-alone entity is ready to be implemented. The decision is documented in the minutes of the Release Acceptance Board which are held in Dimensions.

The POL and Fujitsu Project Managers will then produce a slide pack for presentation to the Release Authorisation Board; this board will then consider whether to approve implementation based on:

- The Release has passed the Release Acceptance Board.
- That Fujitsu Service teams are ready to support the new services / functionality.
- That Post Office Service teams are ready to support the new services / functionality.
- That communications to interested parties e.g., Post Masters are ready.

Approval to implement the project is documented in the meeting minutes that are held in Dimensions.

Once these approvals are in place the project can be implemented into production.

4.8.10.14 Deploy and Support

Release management is based around the use of two documentation tools, PEAK and Managed System Change (MSC), and two delivery tools, Dimensions and Tivoli Provisioning Manager (TPM) (**9.5**). A ticket will be created in PEAK for each change or element of a project. The PEAK Targeting Forum (PTF) which meets weekly reviews the open PEAK tickets and groups these into deployment groups each of which contains typically no more than 20 PEAK tickets.

Development will then create a PEAK Product Version Baseline (PVB) for the deployment group and this is effectively what is placed into production on the successful completion of the relevant testing. Development will then perform unit and component and integration testing as outlined above, once this is successfully completed, they will use one of the standard tools to create a build package which is placed in Dimensions.

Integration will test that the baseline package is capable of being deployed into the existing software/hardware environments and can be regressed off of the Integration testing rig as well as doing some basic functional testing. Once this has taken place and the baseline package is deemed fit to further progress into the testing environments then a PEAK Deployable Product Version Baseline (DPVB) is created to enable further progression into the Release process.

The package created by Development (PVB) & then Integration (DPVB) is then made available to Release management for preparation to be tested in either SV&I for project functional testing with POL and other third parties ready to be implemented (identified by a INT suffix) or if it is for current system maintenance for existing software security or minor bug fixes it will be implemented identified by a LT suffix in the LST (Live Support Test) via a RM Release note (RN) will be passed to Software Configuration Management (SCM). SCM will then place this package onto the TPM server based on receiving authority from Release Management in the Release Note. SCM are the only team with access rights to move software onto the TPM server (**9.5**). SCM advise RM that the output is ready to be shipped to the test environment by updating PEAK.RM will via Peak and the MSC process authorise the relevant operating teams via a sub task MSC to pick up the package and place it into the relevant test environments for further testing as outlined above, this task has a reference to the Release Note. Once testing is complete Release Management will update the release note to reflect this. They will also create a new release note with the same number but a PR suffix to manage the movement into production.

At the same time as Release Management release the RN to the LST team, the ticket will be created in MSC. MSC is used by Release Management to manage the process steps that need to be completed to move a change into production. The approvals to move the change through the various stages (both Fujitsu and POL approvals) are logged in the MSC ticket, and are typically copies of emails pasted into the ticket- MSC does not use formal workflow-based sign offs (**9.6**).

When Release Management believes the package is ready to be implemented the PR suffix Release note will be passed to Software Configuration Management (SCM). SCM will then place this package onto the TPM server, based on receiving authority from Release Management, in the Release Note. SCM are the only team with access rights to move software onto the TPM server.

The final move into production is then made by the relevant deployment team, depending on the platform the change is being made to (**9.5**). The authority and ability to move the change into production is given to the deployment team when Release Management assigns the MSC and the release note ticket to the deployment team.

Once the deployment is complete the PEAK ticket will be closed by the Change Owner who opened it.

4.8.10.15 Post Implementation

4.8.10.15.1 Monitoring and Review

Fujitsu Project Managers monitor and control projects throughout their lifecycle through the following:

Weekly Releases report to Post Office Project Managers

A collated reporting pack issued to the Post Office Project Managers showing the RAG (Red, Amber, and Green) status, Executive summary, key milestones, dependencies risks and issues for each of the Releases that are currently in Delivery.

Monthly Joint Programme Board (with Post Office)

Presentation of a collated reporting pack to the Post Office Programme Manager and the Fujitsu Programme Director showing the RAG status, Executive summary, key milestones, dependencies risks and issues for each of the Releases that are currently in Delivery.

Monthly Demand Planning Forum (with Post Office)

A monthly meeting held with Post Office to look at the forward expected work load from Post Office against the committed resources currently allocated to the Account to see if demand equals resource supply or if any whitespace (not enough work for the committed resources).

Internal Fortnightly Releases Board

Presentation of a collated reporting pack to the Fujitsu Programme Manager showing the RAG status, Executive summary, key milestones, dependencies risks and issues for each of the Releases that are currently in Delivery.

Internal Monthly Programme Board

Presentation of a collated reporting pack to the senior Fujitsu Post Office Management and Fujitsu capability units showing the RAG status and Executive summary, plus any matters relevant at that time, for each of the Releases that are currently in Delivery.

4.8.10.16 POLSAP Application Changes

4.8.10.16.1 POL SAP Application Changes Overview

POLSAP follows the account processes for change control.

The customer will draft a change request (CR) which will be sent from POL's change management team to the change management team in Fujitsu. It will send that CR to the relevant assessing team which will assess:

- The level of resource needed for the change.
- How long it might take.
- How much it might cost.
- Whether it would impact anything else already being done for POL.

This assessment process is known as "impacting the change", based on the information supplied. A Change Proposal (CP) is drafted and sent to potentially affected teams to provide their impacts. This will give an overview of what will be changed, what is not included, assumptions and a breakdown of effort in man days.

Once impacts are collated, the CP is discussed at the Pre Change Control Board (PCCB), which meets weekly. The PCCB is made up of various technical and functional team leaders.

Changes are allocated unique numbers and lodged within a database (PVCS) and related accordingly. These can be viewed by all members of the team working on that project but can only be updated, edited and actioned by members of ChM.

All Minutes from the Change Boards (PCCB and Change Control Board (CCB)) and any actions from the same are recorded in the change history of the change vehicles in the database.

All comments and decision around the changes are also lodged in the change history.

All CP Impacts are collated into CP specific files and stored on a back-up server.

Approvals from the CCB and POL are documented in the relevant change history (**9.2**).

Once agreed at the PCCB and minuted as such (added to CP history in PVCS) a Commercial Terms (CT) document is created and discussed at the Change Control Board (CCB), which meets weekly. Assuming this is approved by the CCB and minuted as such (added to CP history in PVCS) the CT is then sent to POL. This whole process has to be completed in 21 days from Change request received to CT sent to POL.

POL then has a further 21 days to agree the CT and sign it. Once a signed CT is received by the Fujitsu change management team (initially by e-mail, fax and then signed hard-copy – stored locally at first then transferred to a secure Fire-safe), this is announced to the Programme and relevant timesheet codes can be created (aligned to the impacts included for the change) and work can begin on the change.

The change will be developed in the development client (PLD) and the relevant transports created. It will be unit tested in this client before the request is raised to migrate the transports simultaneously to the PLQ and PLE quality assurance clients. The transport requests are authorised by the POLSAP support manager via emailed response to the Basis team and the actual migration is performed by the SAP Basis Team.

The change will now be system tested by the relevant POLSAP Fujitsu team, and then integration, and end to end tested by the dedicated Post Office testing team. The Post Office test team place their test plans and any defects on their Quality Centre application (**9.4**).

Once all testing is completed and an emailed sign off has been received from the Post Office testing manager, or change manager, Fujitsu will raise an MSC for onward migration to the Production client.

This MSC is usually given seven working days' notice period unless deemed an emergency change by the customer. The MSC will be discussed at the weekly CCB meeting and will not proceed unless all sign offs both internally and from the customer have been received and updated on the MSC. In the case of minor application changes, they may not be discussed at the CCB, however they will appear on the CCB agenda and identified as a minor change. The (Fujitsu) Post Office Account Operational Change team determine which internal teams need to review each MSC, however as far as approvals go, it is the customer – The Post Office Change Manager approval that is required to be on the MSC. This is reflected in the notes section on the MSC itself and no change should go to Production without this approval (**9.6**).

The development resource will then request the migration of the transport/s to the Production system in line with the agreed timelines detailed on the MSC. Again this transport will need emailed authorisation from the POLSAP support manager to the SAP Basis team and is carried out by the SAP Basis team (**9.5**). The MSC process is described above under Control Objective 8.

4.8.10.17 Network Change Management

All Network changes are considered in accordance with established Fujitsu operational practices. All changes require an approved design, all changes must be impact assessed by all business and technical stakeholders, an implementation plan is provided, and a change window is agreed and acted on. The system used by Fujitsu for change management is the MSC system. Full details of the change management are in the section above.

All documents concerning the architecture, design, service delivery, monitoring and review of POL networks are held in the appropriate Fujitsu's document repositories Dimensions or SharePoint.

4.8.10.18 Exceptions to Fujitsu Change Management Process

The exception to this process is Reference Data which is supplied by POL for onwards transmission to the POL Branch Counter estate via the Fujitsu network and is subject to a POL authorisation / POA to release and having followed the POL / POA reference data testing process.

4.8.11 Security

10. Control Objective 10: Controls provide reasonable assurance that access to system resources, including computing platforms and operating systems, is restricted to properly authorised individuals.

#	Control
10.1	**Client Security Policies:** Security requirements for infrastructure and software are designed, documented and agreed by both POL and Fujitsu.
10.2	**Baseline Operating System Standards:** Platforms in operational use have defined baseline standards that document their set up and configurations, as agreed by Post Office Limited.
10.3	**Baseline Operating System Standards Implementation:** Platforms in operational use are set up and configured in line with documented and agreed baseline standards. Variances from the baseline standard are fully documented and appropriately approved.
10.4	**User (Fujitsu) Set-up and Amendment:** Fujitsu users requiring new or modified access to Post Office Limited systems are set up appropriately and approved by an appropriate Fujitsu line manager.
10.5	**User (Fujitsu) Deletion:** Access to Post Office Limited systems for Fujitsu users is removed in a timely manner once no longer required.
10.6	**Periodic User Reviews:** Fujitsu and POL meet regularly in the ISMF to review whether user access to systems remains appropriate, with changes then processed as necessary by POL.
10.7	**Two-Factor Authentication:** Access to Post Office Limited systems for Fujitsu users is controlled using two-factor authentication.

4.8.11.1 Policies and Procedures

The Community Information Security Policy (CISP) provides governance and direction in information security for those responsible for initiating, implementing or maintaining security for POL infrastructure. The document describes end-to-end security management process and physical and technical requirements for the in scope systems. This document is authored by POL and shared with relevant third parties. Fujitsu is required, where appropriate, to adhere to the requirements outlined within the document.

The SVM/SEC/POL/0003 document is Fujitsu's interpretation of the CISP document. This policy complies with POL's CISP, the Fujitsu Manage Information Security Policy and the Fujitsu Security Master Policy. SVM/SEC/POL/0003 is reviewed annually and / or by request of POL as a result of a major change. Immediate issues will be dealt with through addendums. The policy is reviewed against POL's CISP, regulatory standards and methodologies (**10.1**).

The ARC/SEC/ARC/0003 document provides a technical standard to the architects and designers to assist them in implementing and maintaining the solutions they provide to POL. The ARC/SEC/ARC0003 is reviewed in line with the above SVM/SEC/POL/003; changes in the latter would result in changes required in the former.

4.8.11.2 General System Security Settings

Each Operating System and Database in use by Fujitsu to support both **IRRELEVANT** **IRRELEVANT** has its own High Level Design (HLD) documentation in place. This sets out the required settings and configuration specific to that Operating System (OS) or Database (DB) at a high 'requirement driven' level. For example, the document might specify that **IRRELEVANT** servers are required to disallow remote shell access attempts (**10.2**).

A corresponding Low Level Design (LLD) document details the OS or DB specific configuration settings needed to meet the requirements set out within the HLD document. These configuration settings are fully documented at a granular level, for example including extracts of OS / DB configuration code and initialisation files (**10.3**).

Both the Operating System / Database HLD and LLD are subject to mandatory review and must be approved by relevant approval authorities documented within Dimensions. All new device builds must conform to specifications set out within the HLD and LLD. Deviations again must be reviewed, risk assessed and approved by POL prior to configurations being implemented or updated.

New devices must be set up in line with the HLD for the required OS / DB. If an HLD does not exist (for example if a new server type is being implemented), an HLD document must first be created, reviewed and approved by the individuals defined in the Reviewers and Approvers Role Matrix. This document is owned and managed by the Fujitsu Document Manager. This document is reviewed upon changes to in key members of staff, i.e., major document owners, as well as on an annual basis.

4.8.11.3 Platform Physical Design (PPD) Document

Each infrastructure element is initially set up from an agreed baseline configuration. Elements of the infrastructure (for example servers) are grouped by type – based on the role they perform within the IT environment – this is defined within Platform Hardware Instance List which is managed and maintained by Infrastructure Lead on the Post Office Account. An example of this is 'ACD', a server type for servers providing directory services for support staff. Each server type has its own technical requirement, and a PPD document is created by the Solution Architects detailing these requirements. The PPD sets out exact hardware specifications, software requirements and configuration requirements for that particular device type.

In short, the PPD sets out the exact requirements that a server must cater for prior to it being set up. Before a server is set up, the PPD must be reviewed and approved by the individuals defined in the Reviewers and Approvers Role Matrix.

There is entry for each server instance within Platform Hardware Instance List stored within Dimensions and this also includes a link to the PPD that was used to initially set up that server. Note that this is a historic document, and remains a record of the initial server configuration rather than necessarily reflecting its current state.

4.8.11.4 Technical Interface Specification Document

As part of a project where a POL third party is involved, both POL and the third party agree a technical interface specification that defines the connectivity between the third party and Fujitsu managed infrastructure. This document is held within Dimensions, once formally agreed by Fujitsu, POL and relevant third parties. This is a historical document that is updated upon changes in requirements of the discussed interface. Changes will have to be agreed by Fujitsu, POL and relevant third parties.

4.8.11.5 Baseline Implementation

A combination of the aforementioned documents dictates the initial configuration of a server added to the Fujitsu POL account infrastructure - this initial configuration is scoped out by the solution architects. It is then the responsibility of the network architects to register application software and products to the identified hardware. A baseline is then sourced and configured using the aforementioned documentation. This configuration is uploaded into Dimensions. This step in turns creates a Package Virtual Baseline (PVB) for the platform. The discussed platform is then set for "Ready for Build" within Dimensions.

The task is then handed over to the Integration Team. It is the responsibility of this team to convert the discussed PVB into a Deployment Package Virtual Baseline (DPVB). This includes a number of packaging exercises, as well as rigorous unit testing. Once a DPVB is established, server definitions are outlined by the Integration team – essentially deciding which DVPB is applied to the differing technologies within the platform.

In order to deliver the DPVB into the Fujitsu managed POL estate, the DPVB is handed to Release Management who are responsible for ensuring the outlined configuration is applied to the appropriate technologies. They will formulate the release note(s) for application of the DPVB to both the test and production environments - the team manages the overall release process from receipt of request for delivery of PSPID / DPVB to authorising deployment for all test rigs and live. The Release Management team act as an escalation point area for the Test team for issues falling within the Release Mechanism.

Once the relevant MSCs have been raised to issue the platform, the release note will be delivered to the relevant Core Service Delivery Unit (Core SDU) – in this case either the Windows NT or UNIX teams. It is the responsibility of the Core SDU to action the release note. They will apply the DPVB to the appropriate technologies, initially to a test rig which will be handed over to the test team.

The test team will accept rig handover from Core SDU and begin their testing procedures – comprising of composition of High Level Test Plans which will act as the base for any Error Logging and Test Reports that are produced once testing is complete. The final sign off from the test team results in liaising with Release Management and the Core SDU to agree deployment of fixes, top-ups or to schedule a rig rebuild. They will also liaise with Customer Services and POL to agree deferments, if applicable.

Once testing sign off is received, the release note will then be passed back to the Core SDU will deliver the baseline via TPM to the relevant technologies.

4.8.11.6 Changes of Configuration to Existing Infrastructure

Once a device is set up, configured, and added to the Fujitsu infrastructure following the process detailed above, its configuration remains static until the need for a configuration change is identified. The server configuration is not by default updated when (for example) the relating OS HLD or LLD documents are modified. Configuration changes made to in-service devices must follow change / incident management processes described elsewhere in this report (include obtaining approval from POL).

The exception to this rule is for the application of standard OS / DB patches and security fixes, which Fujitsu are (in many cases) contractually obliged to apply. Such patches do not bypass approval, as they are reviewed by a Patch Approval Board (PAB) (attended by POL) prior to their application.

Changes to in-service infrastructure configurations can be identified in a number of ways, for example:

- Change Projects.
- New Application Development.
- Patch Application.
- Infrastructure Refresh.
- Fixes identified through the Incident Management process.

Note that these changes follow the formal change and incident management processes.

4.8.11.7 Password Settings

Password configuration requirements are defined in the relevant baselines for infrastructure components. If a component cannot implement the relevant baseline this exception is notified to POL who must authorise it. Passwords are stored in a one-way encrypted form and are protected against substitution or dictionary attack.

Passwords shall conform to the following criteria (unless POL has approved a deviation from these criteria):

- Where passwords are used for authentication, the user must be forced to change the initial password before any other access to the system is permitted.
- Passwords must expire in 30 days.

- Re-use of the same password must not be permitted for either a specified time or until at least 4 other passwords have been used.
- Passwords must be a minimum of 7 characters long and must be alphanumeric (i.e., a mix of letters and numbers). There must not be more than two consecutive identical characters. The password must not be the same as the username.
- After 3 consecutive unsuccessful attempts to log-on, the user must be locked out for at least 30 minutes or until reset by an administrator.
- In general, system users must be subject to the controls specified above. The following exceptions are permitted.
- The username and password used to automate application login may be held in 'clear' i.e., readable format or unencrypted, if it is only accessible to authorised operational management staff for that system and the potential damage from misuse of that username is minimised.
- The password may expire less frequently than the 30 days for human users where suitably obscure passwords are used, e.g., strong passwords consisting of upper case, lower case characters, numbers and symbols and the risk of external access to such accounts is very low however this concession must be documented and approved by the POL CISO.

4.8.11.8 User Administration

The principle of "least privilege" is used to restrict the access rights of users whether human or non-human. The User Access Process details how access is gained to both physical and technical assets within the PO Account and Fujitsu supporting functions and is managed by a POA Security Operations Team (SOT).

4.8.11.9 New Joiners / Transfers

Detailed below are the steps that must be followed for an individual who is new to Fujitsu Services and joining the POA and these are shown in the Figure 1.0 below. Users who have transferred internally onto the Post Office Account from another part of the Fujitsu business will follow a similar process, illustrated in Figure 1.1 (**10.4**).

Figure 1.0 Diagram of User System Access Process Flow for New Joiners

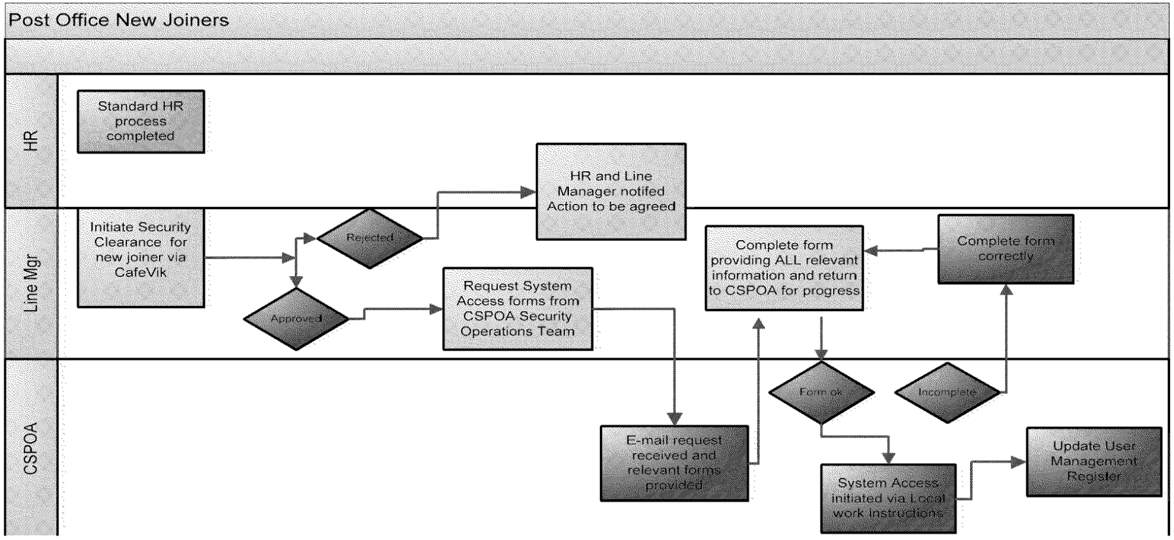
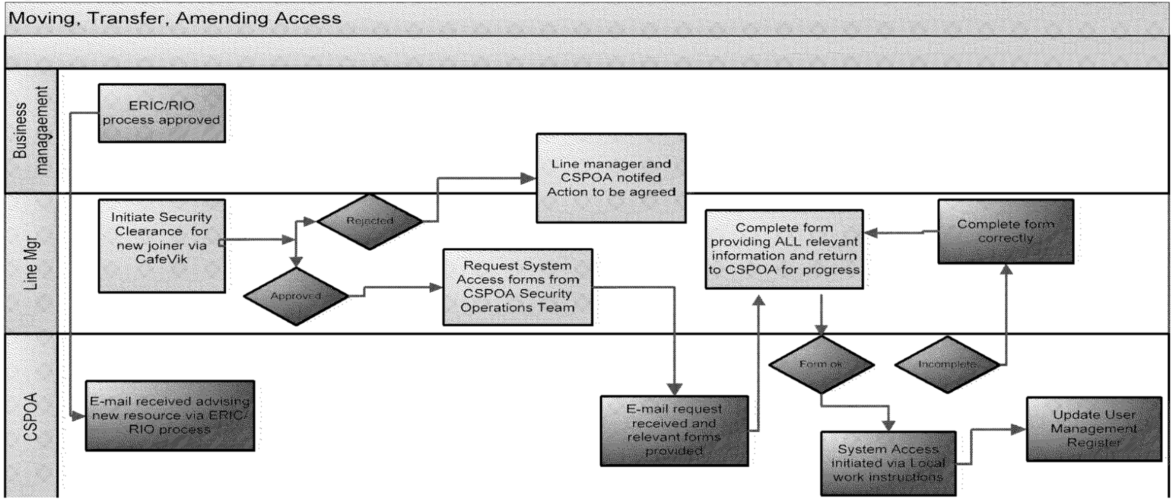

Post Office New Joiners
HR
Line Mgr
CSPOA
Standard HR process completed
HR and Line Manager notifed Action to be agreed
Initiate Security Clearance for new joiner via CafeVik
Rejected
Approved
Request System Access forms from CSPOA Security Operations Team
Complete form providing ALL relevant information and return to CSPOA for progress
Complete form correctly
Form ok
Incomplete
E-mail request received and relevant forms provided
System Access initiated via Local work instructions
Update User Management Register

Figure 1.1 Diagram of User system access flow for Moving, Transferring, and Amending access


Moving, Transfer, Amending Access
Business manageament
Line Mgr
CSPOA
ERIC/RIO process approved
Initiate Security Clearance for new joiner via CafeVik
Rejected
Approved
Line manager and CSPOA notifed Action to be agreed
Request System Access forms from CSPOA Security Operations Team
E-mail received advising new resource via ERIC/RIO process
E-mail request received and relevant forms provided
Complete form providing ALL relevant information and return to CSPOA for progress
Complete form correctly
Form ok
Incomplete
System Access initiated via Local work instructions
Update User Management Register

The Line Manager contacts POA Security Operational Team (SOT) and requests that system access forms are provided. The POA SOT provides the New User Access Forms to the Line Manager and requests they are completed and returned to the POA SOT both as a soft and hard copy. These forms are filed and stored in the security operations secure room and kept for audit purposes.

POA SOT check the form is completed correctly, and in line with PO Account Security Policy. POA SOT then notifies the relevant system owners (Windows NT Team, Unix Team, POLSAP Team) via an e-mail containing the completed request form and a TFS call is raised and suspended whilst access is granted.

Once System Owners configure the user they will update the TFS call on completion of this configuration. POA SOT shall then close the TFS call and update the register.

4.8.11.10 Leavers

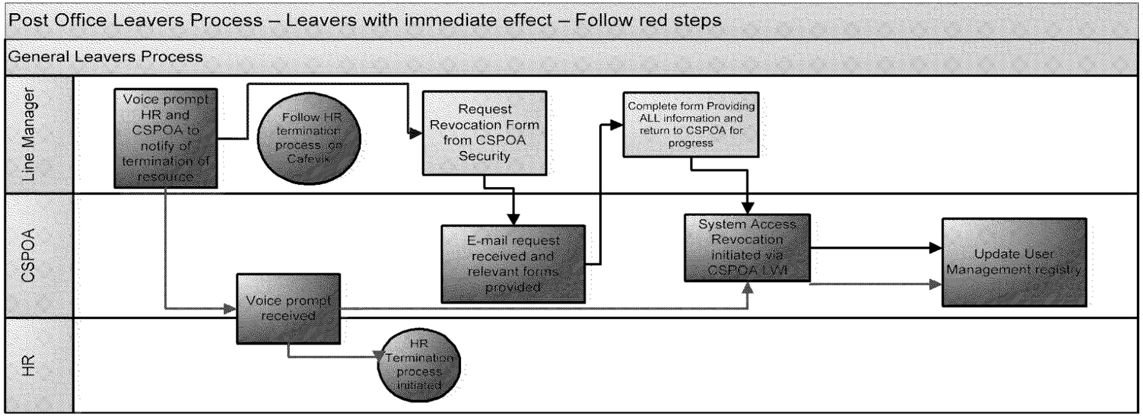
The steps that are followed for an individual leaving Fujitsu Services and the PO Account are shown in the Figure 1.2 Diagram of User system access flow for Leavers (**10.5**).

The Line Manager contacts POA SOT by voice prompt and e-mail, providing the leaver's details and requesting a revocation form. The POA SOT provides the revocation form and asks that it is completed and returned to the POA SOT both as a soft and hard copy. These forms are filed and stored in the security operations secure room and kept for audit purposes.

POA SOT check the form is completed correctly, and in line with PO Account Security Policy. POA SOT notify the relevant system owners (Windows NT Team, Unix Team, POLSAP Team) via an e-mail containing the completed removal form and a TFS call is raised and suspended whilst access is removed.

Once System Owners remove the user they will update the TFS call on completion of this configuration. POA SOT shall then close the TFS call and update the register.

Figure 1.2 Diagram of User system access flow for Leavers


Post Office Leavers Process – Leavers with immediate effect – Follow red steps
General Leavers Process
Line Manager
CSPOA
HR
Voice prompt HR and CSPOA to notify of termination of resource
Follow HR termination process on Cafevik
Request Revocation Form from CSPOA Security
Complete form Providing ALL information and return to CSPOA for progress
E-mail request received and relevant forms provided
System Access Revocation initiated via CSPOA LWI
Update User Management registry
Voice prompt received
HR Termination process initiated

4.8.11.11 Information Security Monthly Forum

The Information Security Monthly Forum (ISMF) is a formalised monthly forum where Post Office and Fujitsu Security production risk and control concerns / issues are raised and progressed with the necessary stakeholders. The purpose of the meeting is to:

- To help ensure the early identification of issues together with timely & effective resolution by those attendees with functional responsibility.
- Review Security Operations monthly reporting on common security control objectives e.g., Patch & Vulnerability Management; Anti-virus / Malware; Configuration Management of Security Infrastructure etc. as agreed between Fujitsu and Post Office.

The Security Operations monthly reporting pack will be compiled and circulated one week in advance of the forum by Fujitsu. This pack will include:

- Agenda for current forum.
- Minutes from previous forum and progress against previous actions.
- Open or new Security Risks and Issues.
- Changes to Information Security Architecture relating to joint venture products.
- Upcoming developments.
- Active Directory User Access Review (**10.6**).

4.8.11.12 User Authentication Technologies

User authentication is two-factor, including dynamic password authentication (known as an iKey) against an external database - TACACS+, RADIUS or similar technology for access (**10.7**). Once authenticated, remote access connections are established via a VPN using an encrypted session. Authorised users should not provide their login token (iKey token) or associated information to anyone at any time for any reason, other than to surrender it when no longer required or when their relationship with Fujitsu has ceased as an employee.

The exception to this would be if they needed to have their account or token reset or a temporary passcode allocated. If this was the case then this information could be given to an authorised person (i.e., member of the Security Operations team) to validate the user.

iKey access is granted to those users who support the HNG-X platform / application. Users must connect to SSN Terminal Servers in order to access to HNG-X platforms within the data centre. As such, all HNG-

X SSN Servers must be a member of the Windows AD (MSAD Domain). Remote users must be granted the Allow log on through Terminal Services right, or be a member of Remote Desktop Users group.

4.8.12 Access to databases, data files and programs

11. Control Objective 11: Controls provide reasonable assurance that access to databases, data files and programs is restricted to properly authorised individuals.

#	Control
11.1	**Patch Management:** In-scope platforms are maintained with vendor released security updates and patches in line with agreed procedures and timescales.
11.2	**System Administrators:** Access to perform system administrator functions restricted to appropriate Fujitsu personnel required to have this level of access by their role.
11.3	**Database Administrators:** Access to administer POL databases is restricted to appropriate Fujitsu personnel required to have this level of access by their role.
11.4	**Administration Tools and System Utilities:** Access to administration tools and system utilities on Post Office Limited infrastructure is restricted to appropriate Fujitsu personnel required to have this level of access by their role.
11.5	**Unauthorized changes are monitored:** The TripWire system is configured to monitor and alert on changes made to in-scope applications and underlying data.
11.6	**Access to Data Files / Programs** Access is restricted to production program and data files through the use of user groups to restrict and allow access.

4.8.12.1 Patch management

Fujitsu's POA SOT and the Service Delivery teams subscribe to relevant vendor information feeds to receive details of patches from vendors that provide critical operating systems, applications, databases and network equipment to POL.

Details of patches are reviewed and documented in the Patch Deployment Spreadsheet. This spreadsheet will be held within Sharepoint.

The Deployment Spreadsheet is reviewed by the SDUs and Application Support teams on a regular basis; they assess whether the patch applies to equipment they manage. They will then update the spreadsheet with the reasoning behind their decision to apply or not to apply a patch in readiness for submission to the Path Approval Board (PAB (**11.1**)).

The PAB consists of members of the Infrastructure Services division, Applications Solutions Team, Operational Security Team and a POL Security representative. The PAB is held on a monthly basis. The PAB will review the Patch Deployment Spreadsheet and seek agreement on the patch set to be deployed and in what timescale (e.g., deploys patches as an emergency fix or include at next release).

4.8.12.2 System Administrators & Database Administrators

The user management database utilised by the POA SOT holds details of all the support teams and the system access the team resources have (**11.2** and **11.3**). This document is monitored on a regular basis to provide assurances against contractual requirements and obligations against the Unit's Roles Responsibilities and Access Requirements.

Access and resources in the teams are reviewed and confirmed as appropriate on a monthly basis by the line managers (**11.4** and **11.6**). The POA SOT then completes the monthly access report for privileged users and presents at the monthly ISMF with POL.

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

1) Reduce the number of passwords required for support purposes.
2) Help 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 method of authentication and authorisation throughout the estate.

Database access control also requires individual role-based accounts for each class of user, both for controlling the actions a user can perform and for helping to ensure administrative and other actions are traceable to an individual to provide a valid and informative audit trail.

The main classes of database users will be:

1) Application – Accounts used by applications for database access to either Oracle or SQL Server Databases.
2) System Administrators – Operational support users with responsibility for managing the database systems.
3) Database Administrators – Operational support users with responsibility for specific databases.
4) Non-administrative Database support users - Operational support users with responsibility for specific databases.

4.8.12.3 Unauthorised changes are monitored & reviewed

Tripwire compares files and directories against a baseline database of file locations, dates modified, and other data. It generates the baseline by taking a snapshot of specified files and directories in a known secure state. After creating the baseline database, Tripwire compares the current system to the baseline and reports modifications, additions or deletions (**11.5**). Tripwire helps to ensure the integrity of critical system files POA SOT who monitor the console.

On a monthly basis, the POA SOT reviews alerts that have been raised from Tripwire. Monthly reports are produced detailing alert statuses and a root cause analysis for each alert. The reviews are available for POL management, in order to monitor unauthorised attempts to modify datasets. The Tripwire alert report is included in the ISMF Security Operational Reports. In cases where no alerts are raised within the month, a report may not be produced and this will be noted within the next month's report.

4.8.13 External threats and access violation management

12. Control Objective 12: Controls provide reasonable assurance that networks and system resources are protected from external threats and access violations are detected, reported and investigated.

#	Control
6.4	**Major & Security Incident review:** Once a Major or Security Incident is resolved there is a formal closure of the incident and a review including, if applicable a Root Cause Analysis.
12.1	**Configuration Access:** Access to set-up and configure firewalls is restricted to appropriate Fujitsu personnel required to have this level of access by their role.
12.2	**Configuration Changes**: Changes to firewall configuration are managed using the standard Fujitsu MSC process including authorisation, testing (where deemed appropriate) and approval of changes before they are implemented.

#	Control
12.3	**Anti-virus software**: Anti-virus software is installed on critical networked Windows and Red Hat Linux platforms as agreed with POL. Installed anti-virus software is up to date in line with agreed contractual requirements.

4.8.13.1 Overall network security design

Within each Data Centre, the POL network is segmented following the Security Domain model. The Security Domain model provides a framework for the network architecture and designs, such that the flow of data around the network is controlled following the principle of least privilege. The applied segmentation is furthered developed within the Network Architecture document and Network High Level and Low Level Design documents – stating the specific details that have been configured on the network.

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

IRRELEVANT

Network segmentation will also be used to provide separation between environments. Each test environment will be separated from other test environments, as well as from the live environment. This will be enforced through the use of Firewall and Router access control lists, VLAN restrictions and user and network access control. These controls will be monitored using the event management system to verify that access control lists and configuration settings are not changed in a way that may allow a network path from one environment to another except under strictly controlled conditions.

4.8.13.2 Firewalls

Direct access between the internet and systems or system components in areas of the network that have been classified as “sensitive” is prohibited and all traffic is routed through a DMZ - a logical sub network that contains and exposes a Fujitsu’s external-facing services to the internet. Firewalls are configured to perform stateful inspection in that only established connections are permitted to connect to the network.

Perimeter firewalls and router components are configured to masquerade internal addresses to the internet using NAT technologies.

Access to set-up and configure firewalls is restricted to appropriate Fujitsu personnel required to have this level of access by their role (**12.1**). MSC is used to raise rule set changes for the firewall configurations (**12.2**). Upon operational change process invocation an appropriate deployment plan is uploaded to the file store within the MSC system which is subjected to peer review prior to deployment, this plan is also used to facilitate change regression if appropriate.

Should any protocols that have been deemed as insecure be required to be included in the configuration then additional information must be supplied that details the security features that have been implemented.

4.8.13.3 Rule Set Review Process

In order to verify the current configuration of network security enforcement devices that manage the POL estate, all configurations are manually inspected at least every 6 months.

Authorised firewall configuration elements in relation to network security enforcement are in document reference SVM/SEC/STD/1985 stored securely in Dimensions. This document is compared against the appropriate device’s active configuration helping to ensure these are in line with the standards in the document. SVM/SEC/STD/1985 is updated when operational configurations are changed through the completion of MSCs. As such SVM/SEC/STD/1985 reflects the secure elements of appropriate operational devices at all times.

If discrepancies are found between SVM/SEC/STD/1985 and the operational configuration these are investigated to help ensure the environment has not been compromised and ascertain why correct process was not followed in relation to inconsistencies.

The review page of SVM/SEC/STD/1985 is updated every 6 months with the new version and contains the date carried out, name and reason for review. This document is stored in a secure area in Dimensions.

4.8.13.4 Anti-Virus Software

The ESET Anti-virus product is a real-time and performs automatic, scheduled and manual scans on all managed clients, in order to identify and contain and eliminate the spread of malicious code (**12.3**).

For the in-scope Wintel systems, real-time file system protection is implemented. All files are scanned for malicious code at the moment they are opened, created or run on the computer.

For the in-scope Linux systems **IRRELEVANT** an on demand daemon has been created using the ESET SDK that can scan files as they are transferred through the respective platforms. ESET is not installed on all Linux systems, by agreement with POL.

In cases where a specific vulnerability or virus stream constitutes a high risk threat to the systems, a scheduled scan is set up from the management console and the client configuration updated accordingly.

ESET provides regular updates of both signatures and engines. For engine updates, these are distributed to clients using the existing Tivoli software distribution management system after having been verified and tested in the test environment to help ensure that no system functionality is compromised by the updated.

The ESET AV System is based on a central Management Server (ERAS) where all the updates (signatures) are stored and managed. ERAS receives the updates from ESET, via an Internet connection, and makes them available for clients to install.

Whenever a virus, vulnerability or suspicious event is detected, the ESET Antivirus system will react according to a configuration that will be enabled using ESET antivirus policies. The workflow describing the process followed is as follows:

1. Windows
   a. On access (read, copy, execute, etc) every item will be scanned by the AV system.

2. Linux
   a. On Demand scanning is performed by the ESET Scanner Daemon.

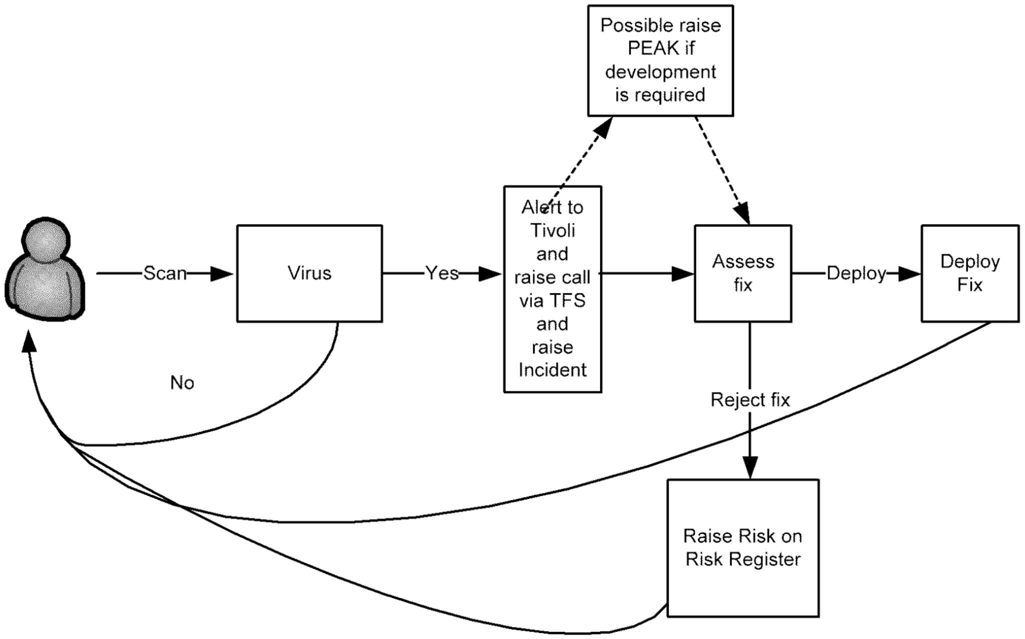
3. If a threat is identified, the AV system will try to automatically clean the item. If the cleaning is successful, an alert event is logged in the ESET Notification manager - which has the ability to take actions when configurable alerts are identified within the ESET environment. This functionality provides an integration point between ESET and the Tivoli Netcool event system. The ESET Notification Manager is monitored proactively by the POA SOT.

4. If the cleaning is not successful, an alert event is logged and an incident is raised in TBSM, with alerts going through to SMC start a remediation action (refer to Control 6 for further information around the incident process):

   a. If development is needed to solve the issue, a PEAK is raised.

b. A fix is produced and assessed according to normal procedure:
   i. If the fix is rejected, a risk is raised on the Risk register.
   ii. If the fix is approved, the fix is deployed on Test and Live environment.

The following is a diagram of the workflow to be applied. Tivoli and KELS are integrated with ESET in order to automate the alerting process in the event of a High/Critical virus being identified by ESET, and start the appropriate remediation activities.


Possible raise PEAK if development is required
Scan
Virus
Yes
Alert to Tivoli and raise call via TFS and raise Incident
Assess fix
Deploy
Deploy Fix
No
Reject fix
Raise Risk on Risk Register

4.8.14 Remote Access

Control Objective 13: Controls exist to provide reasonable assurance that remote access is appropriately restricted to authorised personnel.

#	Control
10.4	**User (Fujitsu) Set-up and Amendment:** Fujitsu users requiring new or modified access to Post Office Limited systems are set up appropriately, and approved by an appropriate Fujitsu line manager.
10.7	**Two-Factor Authentication:** Access to Post Office Limited systems for Fujitsu users is controlled using two-factor authentication.
13.1	**Remote Access Authorisation:** The use of Radius Authentication and CHAP (Challenge Handshake Authentication Protocol) for Counters accessing the data centre ensures that access is restricted to approved devices.

As noted above, remote access for individual users is managed through issuing iKey tokens.

CHAP is used to authenticate the Post Office counters at the outlets when they connect to the data centre. Each counter is authenticated using a dedicated RADIUS server instance for network device access, with different CHAP credentials per Branch Router (**13.1**).

Counters and external devices accessing the data centre can only do so via an ADSL connection utilising the CHAP (Challenge Handshake Authentication) Protocol. CHAP requires that both connecting parties (the data centre and the counter) know the plaintext of a secret string of text (the CHAP secret). During the 'handshaking' phase, (which must take place prior to any other data being communicated), the data centre 'challenges' the counter with a unique calculated value, and expects a particular response.

This expected response must be generated by the counter using both the CHAP secret, and the data centre challenge value, helping to ensure that:

- The counter is the same device that sent the initial connection request.
- The counter is an authorised device, as only authorised devices have knowledge of the CHAP secret.

Note that the CHAP secret is:

- Never shared across the network as part of the handshaking process.
- Securely stored, always in obfuscated or encrypted form.
- 11 characters long and complex.
- Changed at least every two years.

If the counter returns an unexpected value, the connection is immediately terminated. For added security, the handshaking process is repeated at set time intervals, requiring the counter to re-authenticate with the data centre regularly. The CHAP secret is not known by or accessible to users, as it is automatically and randomly generated offline, and encrypted prior to being supplied to specific servers that act as 'distributors' of the secret.

RADIUS (remote authentication dial in user service) provides an additional layer of security, through a centralised Authentication, Authorisation, and Accounting management system. A RADIUS server within the network keeps track of devices approved to connect to the data centre, along with their credentials. These are stored in a secure embedded database. Connection attempt credentials are compared to the RADIUS server, which allows or denies access to the data centre based on whether the connecting device is listed as approved within the database.

POL00399609

5. Not used

6. Complementary User Entity Controls

In designing its system, Fujitsu has contemplated that certain complementary user entity controls would be implemented by POL to achieve certain control objectives included in this report. The complementary user entity controls are as follows:

- **Organisation and Administration**

  Controls should be established to:

  - Evaluate that contracted processes and controls have been implemented.
  - Evaluate and monitor Fujitsu's delivery of services for conformance with contractual obligations.
  - Designate their own internal client representative to determine adequate maintenance of controls over Fujitsu services.
  - Implement and monitor proper segregation of duties exist at POL owned / managed facilities.

- **Physical Access**

  Controls should be established to:

  - Appropriately restrict access to terminals, workstations, and other computing equipment at POL sites, which can also allow access to infrastructure located in the Fujitsu data centre.
  - Request and approve employee access to computer rooms in a fashion that limits access to only those employees requiring it based on job function.

- **Computer Operations**

  Controls should be established to:

  - Approve additions, modifications or deletions to scheduled jobs if necessary.
  - Inform Fujitsu of critical scheduled jobs and the appropriate escalation procedures are associated to those jobs.
  - Define SLAs for availability, capacity and performance management in the agreement with Fujitsu.
  - Review and take action on reports on availability, capacity and performance management, supplied by Fujitsu, where required.
  - Data Retention requirements are documented and agreed with Fujitsu.
  - Periodically, request restores from backup to validate that programs, files and data are recoverable.

- **Networks**

  Controls should be established to:

  - Review network performance statistics (e.g., response time, availability) periodically and that the service levels received are in compliance with the service levels specified in their contracts.
  - Compare metrics in network availability and performance reports to user experience to determine whether availability and performance statistics are accurate.

- **Change Control**

  Controls should be established to:

  - Ensure that application changes follow a formal change process and are approved.
  - Ensure that requests for Fujitsu to implement changes to systems come from authorised individuals.
  - Ensure that a POL representative participates in, or has input to, the system development activities that are relevant to POL, including participation in testing activities, if applicable.

  - Ensure that POL individuals who are permitted to authorise firewall changes have an understanding of the impact the change could have and carry out a risk assessment prior to authorising a change.

- **Logical Access**

  Controls should be established to:

  - Establish and implement procedures and documentation for authorising user access to terminals and application functions.
  - Periodically, review access granted to users at the application layer, to confirm that such access remains appropriate based on users' job functions.
  - Establish and implement procedures to ensure additions, changes, and deletions in client organisations' personnel and their associated job responsibilities are authorised and communicated to Fujitsu in a timely manner (if applicable). Where it is the responsibility of POL to remove users, POL should implement procedures to review that all leavers are removed in a timely manner.
  - Where Fujitsu is asked to implement compensating controls to address situations where infrastructure cannot be configured to meet agreed baselines (e.g. additional monitoring controls), ensure they are comfortable that such controls are being operated whether it be by Fujitsu or POL's employees or contractors.
  - Establish and implement procedures to prohibit the use of shared user IDs or user IDs whose passwords are not changed on a regular basis.
  - Advise POL employees regularly of the importance of security and to report suspicious personnel, transactions or activity to management.
  - Establish and implement procedures to review operating system configurations to ensure settings are providing adequate security, particularly where security parameters are maintained at the original client settings when transferred to Fujitsu.

- **Applications Development**

  Controls should be established to:

  - Document, review and sign off user requirements by the business, prior to commencing a change.
  - Ensure that requests for Fujitsu to implement changes to POL systems come from authorised individuals.
  - Ensure that where POL or its other suppliers administer POL infrastructure, the application's developers have appropriate access.
  - Review reporting received from Steria about the use of the SCC4 transaction to unlock the SAP production environment and to check that these are part of changes that POL has authorised.

The list of client control considerations presented above is not a comprehensive list of all internal controls that should be applied by POL. Other internal controls may be needed at POL.

POL00399609

7. Description of Control Objectives, Controls, Tests and Results of Tests

7.1 Testing Performed and Results of Tests of Entity-Level Control

In planning the nature, timing and extent of our testing of the controls specified by Fujitsu, we considered the aspects of Fujitsu's control environment, risk assessment processes, information and communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

7.2 Control Objectives, Control Activities, Testing Procedures and Results of Testing

On the pages that follow, the description of control objectives and the controls to achieve the objectives have been specified by, and are the responsibility of, Fujitsu. The description of the testing performed by Ernst & Young and the results of tests are the responsibility of the service auditor.

The service auditor's examination was limited to the IT general controls relevant to Fujitsu's operations supporting IT services provided to POL to support the POLSAP and HNG-X applications. Accordingly, the service auditor expresses no opinion on the operating effectiveness of any aspects of application processing and application controls, individually or in the aggregate. POL may need to gain information about application processing and application controls through other means.

7.2.1 Control Objective 1

Controls Specified by Fujitsu	*Testing Performed by Ernst & Young LLP*	*Results of Tests*
Control Objective 1: Controls provide reasonable assurance that access to the data centre and facilities with computer equipment, storage media and program documentation is restricted to properly authorised individuals.		
1.1 Data Centre Access Data centre specific physical access security policies and procedures to control access to the data centre and other sensitive areas, including computer equipment and storage media, are implemented. These are made available to Fujitsu staff via the intranet.	Through discussion with management, identified the documents that define the data centre-specific physical access security policies and procedures for the in-scope data centre. Observed that these documents existed and were held on the Fujitsu intranet. Determined whether these were available to relevant Fujitsu employees.	No deviations noted.
1.2 Access Within the Data Centre Access beyond the security desk is protected by a key-card system that restricts individual access to specific data processing areas. Security management has determined appropriate levels of physical access to the data centre, which is based on the roles and responsibilities of staff. New users requiring access to the data centre must complete an access form, which must be signed as approved by the line manager responsible for the zones requested.	Observed the computer rooms and determined whether access doors are equipped with a card key lock or equivalent to restrict access to sensitive areas. Selected a sample of Fujitsu new starters to the site and sought to determine that the access has been granted and authorised in accordance with the defined procedure.	As there have been no new starters to the Fujitsu data centre for the period covered by this report, no occurrences of this control noted.
1.3 CCTV The data centre is controlled and monitored through the use of CCTV video cameras. Video cameras are placed at strategic locations around the perimeter of the building to help ensure that coverage of the data centre is obtained.	Observed that CCTV video cameras are placed at key locations around the data centre to monitor activity. Observed that these screens are monitored by security staff at the data centre.	No deviations noted.

Controls Specified by Fujitsu	*Testing Performed by Ernst & Young LLP*	*Results of Tests*
Control Objective 1: Controls provide reasonable assurance that access to the data centre and facilities with computer equipment, storage media and program documentation is restricted to properly authorised individuals.		
1.4 Security Guards Security guards are present at the data centre 24 hours per day, seven days per week. The data centre can only be accessed through a central area.	Through discussion with management and observation, determined that security guards (or equivalent) are in place at the data centre (24 hours a day and seven days per a week) and that the data centre can only be accessed through a central point (front desk), which has security guards (or equivalent) in place.	No deviations noted.
1.5 Data Centre Visitors Visitors are required to sign in at the reception area and temporary badges are issued. Visitors must have been pre-notified to data centre security by a Fujitsu employee.	Observed that visitors are granted access based on the pre-notification and that they are required to sign in at the reception area and temporary badges are issued.	No deviations noted.
1.6 Failed Access Monitoring Attempts to enter restricted areas without using authentication devices are denied and a security alert is triggered and logged. Data centre management proactively follows up on security alerts that are triggered.	Inspected a sample of the monthly security alert log reviews performed by Fujitsu and determined whether these were reviewed and followed up.	No deviations noted.
1.7 Review of User Access within the Data Centre Periodic reviews are performed of users who have access to the data centre to help ensure that their access rights are appropriate.	Obtained a quarterly periodic review of user access within the Data Centre and determined whether assigned access levels remain appropriate based on job responsibilities and appropriate actions had been taken as necessary.	No deviations noted.

Controls Specified by Fujitsu	***Testing Performed by Ernst & Young LLP***	***Results of Tests***
Control Objective 1: Controls provide reasonable assurance that access to the data centre and facilities with computer equipment, storage media and program documentation is restricted to properly authorised individuals.		
1.8 Deletion of User Access The managers of the various delivery teams are responsible for notifying the local site facilities team of terminations or transfers of their direct reports. Upon notification of employment changes, access through the security access control system is revoked.	Selected a sample of Fujitsu employees who were terminated from the POL Account during the period under review and determined whether their access to the data centre had been revoked in the access control system in a timely manner.	No deviations noted.

7.2.2 Control Objective 2

Controls Specified by Fujitsu	***Testing Performed by Ernst & Young LLP***	***Results of Tests***
Control Objective 2: Controls provide reasonable assurance that computer equipment and facilities are protected from damage by fire, flood and other environmental hazards and maintenance agreements are in place.		
2.1 Fire Suppression Fire detection and suppression devices, such as hand-held fire extinguishers, are strategically placed throughout the entire data centre.	Observed the existence of fire detection and suppression devices (e.g., gaseous fire suppression devices, hand-held fire extinguishers, smoke detectors and monitoring devices, dry pipe sprinklers and two-hour firewall).	No deviations noted.
2.2 Maintenance Schedule Periodic inspection and maintenance is performed on protection devices, sensors and alarm systems.	Enquired about the monitoring and inspection controls used to protect computer equipment from environmental hazard. Inspected the maintenance schedules (including backup generators, UPS, fire detection and suppression, heating, ventilation and air-conditioning) and service reports for a range of devices supporting environmental monitoring controls in each data centre and determined whether equipment had been maintained during the period.	No deviations noted.
2.3 Environmental Monitoring Smoke detectors and water, humidity and temperature monitoring devices are installed to detect abnormal environmental conditions.	Observed that smoke detectors and water, humidity and temperature monitoring devices have been installed to detect abnormal environmental conditions at each data centre.	No deviations noted.
2.4 UPS Supply A UPS system is installed to protect the facilities and computer equipment from electrical power fluctuations and outages.	Observed that a UPS system had been installed to protect the facilities and computer equipment from electrical power fluctuations and outages at each data centre.	No deviations noted.

7.2.3 Control Objective 3

Controls Specified by Fujitsu	*Testing Performed by Ernst & Young LLP*	*Results of Tests*
Control Objective 3: Controls provide reasonable assurance that programs, files and datasets that have been identified as requiring periodic backup are backed up and retained.		
3.1 Backup Definition The Backup High Level Design documents define Backup and recovery requirements and policy for the platform.	Selected a sample of platforms and determined whether the Backup High Level Design documents for these platforms defined backup and recovery requirements and policy for the platforms.	No deviations noted.
3.2 Backup Toolset Backups are performed using NetBackup or RMAN (automated tools).	Selected a sample of platforms and determined whether NetBackup or RMAN were installed to perform back-ups.	No deviations noted.
3.3 Backups are Written to a Secondary Location Backups performed are written to a separate disk array and are simultaneously written to a disk array at the disaster recovery site.	Selected a sample of servers and determined whether backups performed are written to a separate disk array and are simultaneously written to a disk array at the disaster recovery site.	No deviations noted.
3.4 Failed Backups are Tracked and Monitored Failed backups are signalled to the Master Batch Scheduling system which raises events in a generic manner to the SMC.	Selected a sample of failed backups and determined whether these had been signalled to the Master Batch Scheduling system which had then raised events in the SMC.	No deviations noted.

7.2.4 Control Objective 4

Controls Specified by Fujitsu	***Testing Performed by Ernst & Young LLP***	***Results of Tests***
Control Objective 4: Controls provide reasonable assurance that processing is appropriately authorised and scheduled and that deviations from scheduled processing are identified and resolved.		
4.1 Maintenance of Job Schedules Access to amend job schedules is restricted to appropriate Fujitsu personnel required to have this level of access by their role.	Obtained listings of access rights within the tools used to maintain HNG-X and POLSAP job schedules and determined who had access to amend job schedules. Assessed whether this access is restricted to appropriate Fujitsu personnel required to have this level of access by their role.	No deviations noted.
4.2 SAP Schedules are Continuously Monitored The SAP Basis team uses the SAP GUI and SAP transaction code SM37 to monitor the success / failure of SAP batch jobs. The SAP Basis team will also check and monitor the batch job start and end times and send the daily monitoring statistics to agreed parties.	Observed the SAP Basis team monitoring SAP schedules and that monitoring statistics were sent to agreed parties.	No deviations noted.
4.3 Failed Job Schedules are Monitored and Alerted Automated alerts are configured and sent to relevant parties upon the occurrence of a batch job failure. These are investigated in line with the incident management process.	Reviewed the TWS tool, which manages all batch jobs for in-scope applications, and determined that it is configured to raise an alert if a batch job fails and to then pass this alert to the Tivoli ITM tool. See control 6.6 for testing of alert handling.	No deviations noted.

7.2.5 Control Objective 5

Controls Specified by Fujitsu	***Testing Performed by Ernst & Young LLP***	***Results of Tests***
Control Objective: 5 Controls provide reasonable assurance that system availability, performance and capacity are routinely monitored to ensure that potential issues are captured and investigated.		
5.1 SAP Performance Monitoring The SAP Basis team regularly monitors table space and databases to help ensure there is sufficient system availability and capacity and that potential issues are captured and investigated.	Observed the SAP Basis team monitoring SAP table space and databases and where applicable, issues are captured and investigated appropriately.	No deviations noted.
5.2 SAP Capacity Alerting An automated alert will be generated in the Solution Manager System (PLM) if the table space is more than 95% filled and the SAP Basis team will monitor and review these alerts.	Identified a SAP server that exceeded the defined alerting parameters and determined whether the expected alerts had been generated, monitored, reviewed and then sent to the SAP Basis team.	No deviations noted.
5.3 SAP Availability Alerting Automated alerts are configured in Solution Manager to advise if a part of the system is shutdown / not available for users. These alerts go to the SMC team and they will create an incident.	Determined whether automated alerts are configured in Solution Manager to advise if part of the system is shutdown / not available for users. Followed through an alert and determined if this was sent to the SMC team who then created an incident.	No deviations noted.
5.4 HNG-X Performance Monitoring The SYSMAN3 tool (Tivoli ITM) proactively monitors CPU, Memory, Disk utilisation and capacity of internal services on these platforms, raising alerts for investigation by the SMC as appropriate.	Determined whether the Tivoli ITM tool was implemented on the HNG-X platforms and whether it is configured to look at the CPU, memory, disk utilisation and capacity of internal services on these platforms. Selected an alert from the Tivoli ITM tool and determined if this went to the SMC for review and investigation.	No deviations noted.

Controls Specified by Fujitsu	***Testing Performed by Ernst & Young LLP***	***Results of Tests***
Control Objective: 5 Controls provide reasonable assurance that system availability, performance and capacity are routinely monitored to ensure that potential issues are captured and investigated.		
5.5 HNG-X Capacity and Availability Monitoring The Tivoli ITM tool proactively monitors the availability of Wintel and Unix platforms, feeding platform availability data to Tivoli Business Service Manager (via Netcool Omnibus) about the availability of platforms. Tivoli Business Service Manager presents this data in a business context to the SMC, highlighting service affecting issues.	Obtained evidence of Tivoli ITM configurations and determined whether: • These showed that the Tivoli ITM tool monitors and manages availability and capacity of servers. • Thresholds were defined which, if breached, would send alerts as described. See control 6.6 for testing of alert handling.	No deviations noted.
5.6 Monitoring of Service Delivery A monthly Service Review Book is provided to POL to review its agreed Service Levels. Within this book are details of capacity, availability and incident management performance.	Selected a sample of months and determined whether the: • Monthly Service Review Book is provided to POL to review its agreed Service Levels. • Monthly Service Review Book contains details of capacity, availability and incident management performance.	No deviations noted.

7.2.6 Control Objective 6

Controls Specified by Fujitsu	***Testing Performed by Ernst & Young LLP***	***Results of Tests***
Control Objective 6: Controls provide reasonable assurance that significant operations incidents are adequately reported, tracked, monitored through resolution and resolved timely.		
6.1 Incident Policies and Procedures are in Place Fujitsu has documented policies and procedures for managing incidents impacting the in scope applications which are available via CafeVik to Fujitsu teams.	Through discussion with management, identified the documents that define the incident management processes for the POL account. Determined whether these were available to relevant Fujitsu employees.	No deviations noted.
6.2 Incident Prioritisation Incidents are assigned a priority in accordance with the severity levels agreed with POL.	Selected a sample of incidents and determined whether these had been assigned a priority in accordance with the severity levels agreed with POL.	No deviations noted.
6.3 Incident Resolution Incidents are handled in a timely manner, as per priority.	Selected a sample of incidents and determined whether these had been handled in a timely manner, as per priority.	No deviations noted.
6.4 Major & Security Incident Review Once a Major or Security Incident is resolved there is a formal closure of the incident and a review including, if applicable, a Root Cause Analysis.	Selected a sample of Major and Security Incidents and determined whether a Formal Closure of the Major Incident took place and a review of the Incident, including, if applicable, a Root Cause Analysis.	As there have been no Major or Security Incidents in the period covered by this report, no occurrences of this control noted.
6.5 Incident Reporting On a daily basis, the Fujitsu HSD / IMT reviews the number and severity of outstanding incidents in TFS.	Discussed with management that the Fujitsu HSD / IMT had reviewed the number and severity of outstanding incidents in TFS.	No deviations noted.

Controls Specified by Fujitsu	*Testing Performed by Ernst & Young LLP*	*Results of Tests*
Control Objective 6: Controls provide reasonable assurance that significant operations incidents are adequately reported, tracked, monitored through resolution and resolved timely.		
6.6 Alert Handling The Tivoli ITM and Netcool Omnibus automate the collection of events and using Tivoli Business Service Manager highlight areas of concern to the SMC.	Selected a sample of events and determined whether the Tivoli ITM and Netcool Omnibus tools automated the collection of events and used Tivoli Business Service Manager to highlight areas of concern to the SMC.	No deviations noted.

7.2.7 Control Objective 7

Controls Specified by Fujitsu	*Testing Performed by Ernst & Young LLP*	*Results of Tests*
Control Objective: 7 Controls provide reasonable assurance that networks are managed to contractual and site requirements, monitored for availability and response times and issues are identified, tracked and resolved.		
5.6 Monitoring of Service Delivery A monthly Service Review Book is provided to POL to review its agreed Service Levels. Within this book are details of capacity, availability and incident management performance.	Selected a sample of months and determined whether the: • Monthly Service Review Book is provided to POL to review its agreed Service Levels. • Monthly Service Review Book contains details of capacity, availability and incident management performance.	No deviations noted.
7.1 Network Performance Criteria Network availability and performance requirements are clearly defined between Fujitsu and POL in the Network Service descriptions and network service is measured and monitored using these agreed service levels.	Through discussion with management, we confirmed that documents that define the network availability for the POL account are in place. Determined whether these were available to relevant Fujitsu employees and were used to measure and monitor SLAs.	No deviations noted.
7.2 Network Change Management Network changes are managed using the standard Fujitsu MSC process including authorisation, testing (where deemed appropriate) and approval of changes before they are implemented.	Selected a network change and determined whether this change was managed using the standard Fujitsu MSC process including authorisation, testing and approval of the changes before it was implemented.	No deviations noted.
7.3 Network Availability Monitoring Network availability is monitored using several tools, which send automated alerts to the Network Operating Support Service Team (NOSS) if key components are unavailable, or if traffic levels breach predefined thresholds.	Observed the HP Openview, CACTI and Tivoli Netcool tools monitoring network availability, including that they are configured to send automated alerts to the Network Operating Support Service Team (NOSS).	No deviations noted.

Controls Specified by Fujitsu	Testing Performed by Ernst & Young LLP	Results of Tests
Control Objective: 7 Controls provide reasonable assurance that networks are managed to contractual and site requirements, monitored for availability and response times and issues are identified, tracked and resolved.		
7.4 Network Incident Management Incidents relating to network availability are managed using standard incident management procedures used on the POA, and are included in the standard incident management reporting to POL.	Selected a network incident and determined whether it was managed using standard incident management procedures used on the POA, and are included in the standard incident management reporting to POL.	No deviations noted.

7.2.8 Control Objective 8

Controls Specified by Fujitsu	Testing Performed by Ernst & Young LLP	Results of Tests
Control Objective 8: Controls provide reasonable assurance that modifications to system software and networks are authorised, tested, approved, properly implemented and documented.		
8.1 Change Management The MSC toolset is used to manage all changes with a joint decision between Fujitsu and POL as to which parts of the tool are relevant for a change.	Selected a sample of changes and determined whether the MSC toolset had been used to manage these changes in accordance with the defined procedures.	No deviations noted.
8.2 Change Approval All changes must be authorised by the Fujitsu Duty Manager or technical bridge, with approval being documented in the MSC system. Changes that cause major service interruption must also be authorised by the Change Advisory Board (CAB), with approval being documented in the meeting minutes and within the MSC system.	Selected a sample of changes and determined whether these had been authorised, with approval being documented in meeting minutes and within the MSC system.	No deviations noted.
8.3 Emergency Changes Any change deemed necessary in order to resume live service will be agreed and authorised and documented during the incident along with updates to POL at an agreed timeframe dependent on the severity of the incident.	Selected a sample of emergency changes and determined whether these had been agreed and authorised and documented during the incident along with updates to POL at an agreed timeframe dependent on the severity of the incident.	No deviations noted.

7.2.9 Control Objective 9

Controls Specified by Fujitsu	*Testing Performed by Ernst & Young LLP*	*Results of Tests*
Control Objective 9: Controls provide reasonable assurance that new or modified application software development efforts are authorised, tested, approved, properly implemented and documented.		
9.1 System Development and Maintenance Policies and Procedures Fujitsu has a formal Systems Development Life Cycle (SDLC) which incorporates phases including Initiation, Requirements, Definition, Design, Development, Deployment and Maintenance.	Through discussion with management, we confirmed that the documents that define the SDLC for the POL account are in place. Determined whether these were available to relevant Fujitsu employees, and whether these included phases including: • Initiation • Requirements • Definition • Design • Development • Deployment • Maintenance.	No deviations noted.
9.2 Change Control Board Depending on the nature, changes must either be approved by the Change Control Board (CCB) before progressing into development or by the PEAK Targeting Forum (PTF).	Selected a sample of changes and determined whether these had been approved by either the Change Control Board (CCB) or the PEAK Targeting Forum (PTF) before progressing into development.	No deviations noted.
9.3 Design Proposal Projects are outlined in a Design Proposal (DPR) that is held in DOORS or Sharepoint and is reviewed and approved by POL as well as Fujitsu management.	Selected a sample of projects and determined whether these had a Design Proposal (DPR) document that had been reviewed and approved by POL as well as Fujitsu management.	No deviations noted.

Controls Specified by Fujitsu	*Testing Performed by Ernst & Young LLP*	*Results of Tests*
Control Objective 9: Controls provide reasonable assurance that new or modified application software development efforts are authorised, tested, approved, properly implemented and documented.		
9.4 Change Testing Changes are tested in line with the defined procedure.	Selected a sample of changes and determined whether, where applicable, for these changes: • Testing had been done by the relevant Fujitsu team and POL team. • Test plans had been placed in the Quality Centre application. • The POL Testing Manager had emailed to indicate their approval that testing has been successfully completed.	No deviations noted.
9.5 Ability to Implement Changes Only appropriate individuals have access needed to move code builds between environments or promote transports to live. Segregation of duties is enforced between users able to develop and implement changes.	Selected a sample of application servers and determined who had access to implement changes, and assessed whether these users were appropriate and that segregation of duties is enforced between users able to develop and implement changes.	No deviations noted.
9.6 Approval to Implement Changes POL approval is required to promote software changes to the live environment. Approval is captured within the relevant MSC.	Selected a sample of changes and determined whether PO approval to implement the change was recorded within the relevant MSC.	No deviations noted.

7.2.10 Control Objective 10

Controls Specified by Fujitsu	***Testing Performed by Ernst & Young LLP***	***Results of Tests***
Control Objective 10: Controls provide reasonable assurance that access to system resources, including computing platforms and operating systems, is restricted to properly authorised individuals.		
10.1 Client Security Policies Security requirements for infrastructure and software are designed, documented and agreed by both POL and Fujitsu.	Through discussion with management, identified the documents that define the information security architecture and procedures for the POL account. Determined whether these were available to relevant Fujitsu employees, and whether these had been reviewed and approved in line with contractual requirements.	No deviations noted.
10.2 Baseline Operating System Standards Platforms in operational use have defined baseline standards that document their set up and configurations, as agreed by Post Office Limited.	Selected a sample of platforms in operational use and determined whether baseline standards had been defined and agreed with POL.	No deviations noted.
10.3 Baseline Operating System Standards Implementation Platforms in operational use are set up and configured in line with documented and agreed baseline standards. Variances from the baseline standard are fully documented and appropriately approved.	Selected a sample of platforms in operational use and determined whether the platforms had been set up and configured in line with documented and agreed baseline standards. Determined whether variances from the baseline standard had been documented and approved in accordance with defined procedures.	No deviations noted.
10.4 User (Fujitsu) Set-up and Amendment Fujitsu users requiring new or modified access to Post Office Limited systems are set up appropriately, and approved by an appropriate Fujitsu line manager.	Selected a sample of Fujitsu users given access to POL systems during the period under review and determined whether these users had been set up in accordance with the access request, and that the request had been approved by an appropriate Fujitsu line manager.	No deviations noted.

Controls Specified by Fujitsu	Testing Performed by Ernst & Young LLP	Results of Tests
Control Objective 10: Controls provide reasonable assurance that access to system resources, including computing platforms and operating systems, is restricted to properly authorised individuals.		
10.5 User (Fujitsu) Deletion Access to Post Office Limited systems for Fujitsu users is removed in a timely manner once no longer required.	Selected a sample of Fujitsu staff that left the POL account during the period under review and determined whether their access had been removed on a timely basis.	No deviations noted.
10.6 Periodic User Reviews Fujitsu and POL meet regularly in the ISMF to review whether user access to systems remains appropriate, with changes then processed as necessary by POL.	Selected a sample of ISMF meeting minutes and determined whether roles and access rights had been reviewed as defined.	No deviations noted.
10.7 Two-Factor Authentication Access to Post Office Limited systems for Fujitsu users is controlled using two-factor authentication.	Observed Fujitsu staff logging on to POL systems and determined whether this required two factor authentication.	No deviations noted.

7.2.11 Control Objective 11

Controls Specified by Fujitsu	***Testing Performed by Ernst & Young LLP***	***Results of Tests***
Control Objective 11: Controls provide reasonable assurance that access to databases, data files and programs is restricted to properly authorised individuals.		
11.1 Patch Management In-scope platforms are maintained with vendor released security updates and patches in line with agreed procedures and timescales.	Selected an in-scope platform and determined whether the most recent patches had been applied. Determined that patches are applied using the same change process and controls as tested for Control Objective 8.	No deviations noted.
11.2 System Administrators Access to perform system administrator functions restricted to appropriate Fujitsu personnel required to have this level of access by their role.	Selected a sample of servers and determined whether access to perform system administrator functions was restricted to appropriate Fujitsu personnel required to have this level of access by their role.	No deviations noted.
11.3 Database Administrators Access to administer POL databases is restricted to appropriate Fujitsu personnel required to have this level of access by their role.	Selected a sample of in-scope databases and determined whether access to administer those databases was restricted to appropriate Fujitsu personnel required to have this level of access by their role.	No deviations noted.
11.4 Administration Tools and System Utilities Access to administration tools and system utilities on Post Office Limited infrastructure is restricted to appropriate Fujitsu personnel required to have this level of access by their role.	Selected a sample of platforms and determined whether access to administration tools and system utilities on Post Office Limited infrastructure is restricted to appropriate Fujitsu personnel required to have this level of access by their role.	No deviations noted.

Controls Specified by Fujitsu	*Testing Performed by Ernst & Young LLP*	*Results of Tests*
Control Objective 11: Controls provide reasonable assurance that access to databases, data files and programs is restricted to properly authorised individuals.		
11.5 Unauthorized Changes are Monitored The TripWire system is configured to monitor and alert on changes made to in-scope applications and underlying data within the HNG-X estate.	Selected a sample of application servers and determined whether the TripWire system was configured to monitor and alert on changes made to in-scope applications and underlying data.	No deviations noted.
11.6 Access to Data Files / Programs Access is restricted to production program and data files through the use of user groups to restrict and allow access.	Selected a sample of platforms and determined whether access to significant production program and data files was appropriately restricted.	No deviations noted.

7.2.12 Control Objective 12

Controls Specified by Fujitsu	*Testing Performed by Ernst & Young LLP*	*Results of Tests*
Control Objective 12: Controls provide reasonable assurance that networks and system resources are protected from external threats and access violations are detected, reported and investigated.		
6.4 Major & Security Incident Review Once a Major or Security Incident is resolved there is a formal closure of the incident and a review including, if applicable, a Root Cause Analysis.	Reviewed the Incident Management log for any Major and Security Incidents and determined whether a Formal Closure of the Incident took place including a review of the Incident with, if applicable, a Root Cause Analysis.	As there have been no Major or Security Incidents in the period covered by this report, no occurrences of this control noted.
12.1 Configuration Access Access to set-up and configure firewalls is restricted to appropriate Fujitsu personnel required to have this level of access by their role.	Selected a sample of firewalls and determined who had access to set up and configure these devices. Assessed whether personnel with these rights were appropriate.	No deviations noted.
12.2 Configuration Changes Changes to firewall configuration are managed using the standard Fujitsu MSC process including authorisation, testing (where deemed appropriate) and approval of changes before they are implemented.	Selected a change to firewall configuration and determined whether this: • had been authorised, tested and approved before being implemented; and • was managed using the MSC process tested under Control Objective 8.	No deviations noted.
12.3 Anti-virus Software Anti-virus software is installed on critical networked Windows and Red Hat Linux platforms as agreed with POL. Installed anti-virus software is up to date in line with agreed contractual requirements.	Selected a sample of servers and determined whether Anti Virus software was installed and up to date.	No deviations noted.

7.2.13 Control Objective 13

Controls Specified by Fujitsu	***Testing Performed by Ernst & Young LLP***	***Results of Tests***
Control Objective 13: Controls exist to provide reasonable assurance that remote access is appropriately restricted to authorised personnel.		
10.4 User (Fujitsu) Set-up and Amendment Fujitsu users requiring new or modified access to Post Office Limited systems are set up appropriately, and approved by an appropriate Fujitsu line manager.	Selected a sample of Fujitsu users given access to POL systems during the period under review and determined whether these users had been set up in accordance with the access request, and that the request had been approved by an appropriate Fujitsu line manager.	No deviations noted.
10.7 Two-Factor Authentication Access to Post Office Limited systems for Fujitsu users is controlled using two-factor authentication.	Observed Fujitsu staff logging on to POL systems and determined whether this required two factor authentication.	No deviations noted.
13.1 Remote Access Authorisation The use of Radius Authentication and CHAP for Counters accessing the data centre ensures that access is restricted to approved devices.	Obtained network documentation and determined whether Radius Authentication and CHAP for Counters validation is in place for remote access requests.	No deviations noted.