POL00401634

FUJITSU

POST OFFICE

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

Throughout the Period 1 April 2017 to 31 December 2017

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

POL00401634

Table of Contents

POL00401634

1. Management Statement

9 March 2018

We have prepared the accompanying *Description of Fujitsu's system of IT infrastructure services supporting Post Office Limited's POLSAP, HNG-X and Credence applications Throughout the Period 1 April 2017 To 31 December 2017* ("Description") for Post Office Limited (POL) during the period 1 January 2017 to 31 August 2017, and the independent auditors of POL who have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by POL themselves, when assessing the risks of material misstatements of POL's financial statements.

We confirm, to the best of our knowledge and belief, that:

a. The Description fairly presents the IT Infrastructure services supporting POL's POLSAP, HNG-X and Credence applications ("System") made available to POL during the period 1 April 2017 to 31 December 2017 for providing Infrastructure services to the POLSAP, HNG-X and Credence applications.

b. The criteria we used in making this statement 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;
- specified control objectives and controls designed to achieve those objectives;
- controls that, in designing the System, Fujitsu 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.

c. the Description includes relevant details of changes to the System during the period from 1 April 2017 to 31 December 2017.

d. the controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period 1 April 2017 to 31 December 2017 to achieve those objectives if POL implemented the Complementary User Entity Controls. The criteria we used in making this statement were that:

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

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

POL00401634

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

GRO

Garry Stewart
Service Delivery Director Private Sector BAS

POL00401634

Building a better working world

2. Report of Independent Service Auditor

Fujitsu Services Limited
Lovelace Road
Bracknell
RG12 8SN

Scope

We have examined Fujitsu Services Limited ("Fujitsu")'s accompanying *Description of Fujitsu's system of IT infrastructure services supporting Post Office Limited's POLSAP, HNG-X and Credence applications Throughout the Period 1 April 2017 To 31 December 2017* (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 Post Office Limited (POL)'s controls are suitably designed and operating effectively, along with related controls at Fujitsu. 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 statement titled, *Management Statement* (Statement) on page 1 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 Statement, including the completeness, accuracy and method of presentation of the Description and the Statement and stating the control objectives in the Description.

Fujitsu is also responsible for providing the services covered by the Description, specifying the control objectives and stating them in the Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the Statement and designing, implementing and documenting controls to achieve the related control objectives stated in the Description.

Our Independence and Quality Control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies International Standard on Quality Control 1 and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

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 described therein to achieve the related control objectives stated in the Description, based on our examination. We conducted our examination 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. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented and the controls described therein were suitably

POL00401634

Building a better working world

designed and operating effectively to achieve the related control objectives stated in the Description throughout the Period 1 April 2017 to 31 December 2017.

An examination of a description of a service organisation's system, and the suitability of the design and operating effectiveness of the service organisation's controls described therein 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. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives were achieved. An examination 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 Statement. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls at Fujitsu and their effect on assessments of control risk at POL are dependent upon their interaction with controls and other factors present at POL. We have performed no procedures to evaluate the effectiveness of controls at POL.

Inherent limitations

Fujitsu's Description is prepared to meet the needs of POL and its independent auditors and may not 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

In our opinion, in all material aspects, based on the criteria described in Fujitsu's Statement:

a. the Description fairly presents the system that was designed and implemented throughout the Period 1 April 2017 to 31 December 2017.

b. the controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period 1 April 2017 to 31 December 2017 and if POL applied the complementary user entity controls contemplated in the design of Fujitsu's controls throughout the period 1 April 2017 to 31 December 2017.

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 2017 to 31 December 2017.

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, Testing and Results of Tests (Description of Tests and Results).

The information in Other Information Provided by Fujitsu is presented by Fujitsu to provide additional information, and is not part of the Description that may be relevant to Post Office's internal control. Such information has not been subjected to the procedures applied in the examination of the description of controls applicable to the processing of transactions for Post Office, and accordingly, we express no opinion on it.

POL00401634

Building a better working world

Restricted use

This report, including the description of tests of controls and results thereof in the *Description of Control Objectives, Controls, Testing and Results of Tests*, is intended solely for the information and use of Fujitsu, POL as the user of the system during some or all of the period 1 April 2017 to 31 December 2017 and the independent auditors of POL. This report is not intended to be and should not be used by anyone other than these specified parties.

Ernst & Young LLP

9 March 2018
London
United Kingdom

POL00401634

3. Description of Fujitsu's system of IT infrastructure services supporting Post Office Limited's POLSAP, HNG-X and Credence applications Throughout the Period 1 April 2017 to 31 December 2017

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 with Post Office which has links going back more than 40 years.

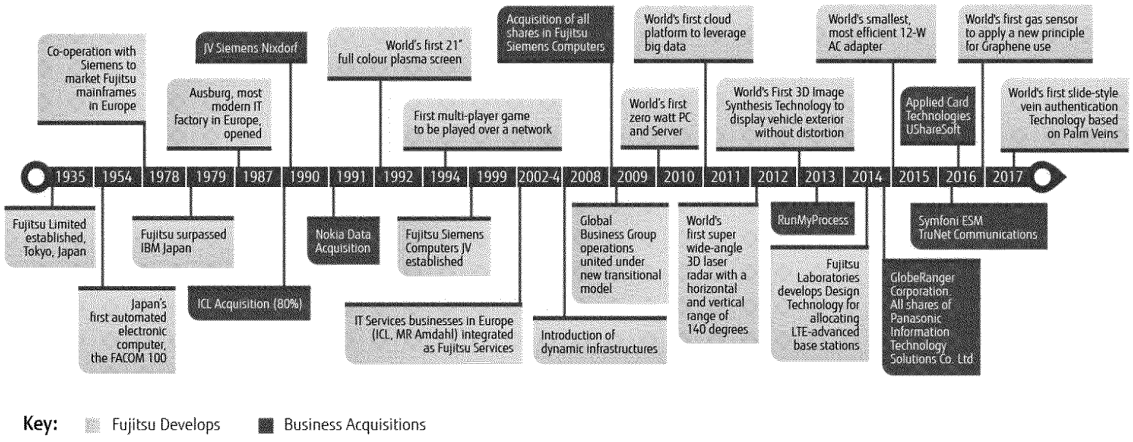


Figure 1. A long line of landmark achievements and product milestones for Fujitsu

3.1.2 Major Markets and Human Capital

Fujitsu UK and Ireland is a leading IT systems, services and products company employing approximately 14,000 people with an annual revenue of £1.8 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.

POL00401634

Figure 2. Delivery locations spread throughout the UK&I

3.1.3 Organisational Structure, including Business Units

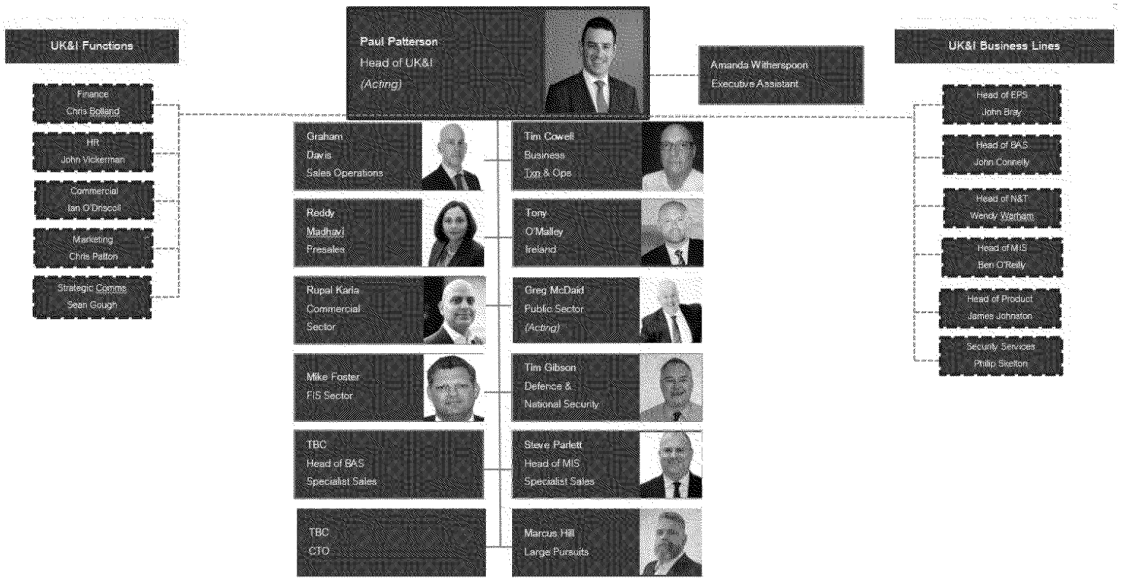
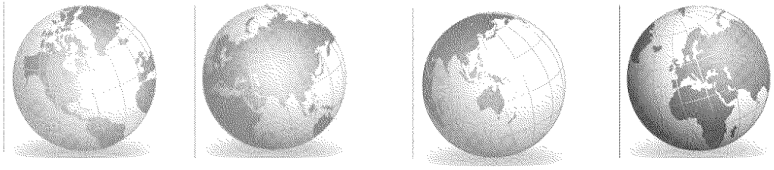


Figure 3. Fujitsu UK&I Organisation

POL00401634

3.1.4 Geographical Spread



Americas
Argentina, Brazil, Chile, Colombia, Canada, Mexico, Puerto Rico, United States of America, Venezuela Anguilla, Aruba, Bahamas, Barbados, Cayman Islands, Dominica, French Guiana, Guadalupe, Jamaica, Martinique, Montserrat, Netherlands Antilles, Saint Vincent and Grenadines, Trinidad-and-Tobago, Virgin Islands British, Virgin Islands U.S.

Asia
Japan, China, Hong Kong, India, Indonesia, Korea, Malaysia, Philippines, Singapore, SriLanka, Taiwan, Thailand, Vietnam

Oceania
Australia, New Zealand

EMEA
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, The Netherlands, Norway, Poland, Portugal, Romania, Russia, Serbia, Slovenia, Slovakia, Spain, Sweden, Switzerland, Tajikistan, Turkmenistan, Ukraine, United Kingdom, Uzbekistan, Afghanistan, Bahrain, Gaza, Iraq, Israel, Jordan, Kuwait, Lebanon, Malta, Oman, Pakistan, Palestine, Qatar, Saudi Arabia, Turkey, United Arab Emirates, West Bank, Yemen, 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 and Zimbabwe

Figure 4. Fujitsu Global Locations

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.

POL00401634

Fujitsu 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 subsection 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 recognises 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 characterised and reflected in the Fujitsu Way Code of Conduct, which is understood by all employees of the organisation. All employees are required to maintain ongoing compliance and compliance training. Compliance checks are undertaken to help ensure that employees understand and comply with the Fujitsu Way Code of Conduct.

4.3 Business Lines and Functions

The Business Lines and Functions that provide services or support the delivery of service to POL are as follows:

- Business and Applications Services (BAS).
- Compliance.
- Operations.
- Enterprise and Cyber Security (ECS).
- Operations:
    - Information & Technology Group.
    - Procurement.
    - Properties and Shared Services.
    - Responsible Business.
- Managed Infrastructure Services (MIS).
- Product Business.
- Legal and Commercial.
- Finance.
- Human Resources.
- Sales and Marketing.
- Strategy, Offerings, Governance and Assurance (SOGA).

The purpose of these Business Lines and Functions is to enable, organise and facilitate the delivery requirements placed on Fujitsu by the Post Office contract.

POL00401634

Each of the Business Lines or 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.

The Business Lines and Functions establish their own frameworks for the continuous formal support of the Fujitsu team managing the Post Office contract by their management and enforce this through their own policies, procedures and standards and registers, including, where applicable, internal and external audits. The controls in place at each of these 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 Fujitsu is able to provide to Post Office. Each of these Business Lines and Functions is also responsible for helping to ensure that their staff are appropriately trained and follow Fujitsu Corporate processes to achieve this.

4.4 Control Activities

4.4.1 Governance and Oversight of Control Activities

Fujitsu's has established the Corporate Governance Committee (CGC) and Audit Committee responsible to the Fujitsu UK and Ireland Board to oversee the company's 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 is responsible for monitoring performance of the Company on behalf of its shareholders and helping to ensure that Fujitsu satisfies regulatory and statutory requirements related to its operations. Authority for action and expenditure within Fujitsu Service flows from the Board and the Board has established that the necessary control systems are in place to help 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 EMEIA Business Management System (EBMS) is managed by Fujitsu's Business Assurance teams and comprises 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 the Fujitsu teams supporting POL, each Business Line and Function follows the EBMS. Where exceptions to the EBMS 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 EBMS.

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*

POL00401634

Fujitsu has industry acknowledged good practice embedded in its approach to performance management as recognised by our Investors in People Gold Accreditation and Champion status.

We call our approach Performance First and the key elements of this inclusive approach include:

- Managers across the business disseminate and share Fujitsu business goals with all employees by converting them into meaningful team and individual objectives.
- Monthly one-to-one discussions are held with direct reports, using coaching skills to ensure individuals have the support they need to take ownership of, and deliver against their objectives.
- Every individual creates their own personal development plan, which forms part of the monthly review, captures development needs and includes a suitable learning action for each need.
- Every employee has an interim quarterly review and an annual appraisal held to formally record achievement against objectives, noting outcomes and future development needs.
- Following the appraisal, on an annual basis, a performance rating is allocated to every employee based upon their achievements against objectives. These ratings are linked to salary review and bonus eligibility.

Within Fujitsu, employee performance management is recognised as key to delivering excellent customer service.

To support managers and employees through the process Fujitsu has a comprehensive "one stop shop" intranet portal that provides a wealth of collateral, guidance and training aids for each stage. As well as traditional training we have videos of employees and managers talking about the process and on-line demonstrations of the Performance First IT recording system. Our regional CEO is personally involved in filming communications and training material for all employees.

4.5 Information and Communication

Fujitsu UK and Ireland Business Lines and Functions have EMEIA Connect portals to enable sharing of knowledge across the company and throughout their own business areas.

These portals provide information about each of the Business 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 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.

Fujitsu also seeks the views of employees via representative groups in different parts of the Company. Fujitsu management consults regularly with these bodies, providing updates and seeking views on important issues. In addition Fujitsu has agreements with trades unions that include regular meetings with local and senior management to discuss issues affecting employees in the unions' area of interest.

Fujitsu Voice is the employee forum that allows for important issues affecting people in the UK to be shared with the senior leadership team. Topics discussed range from company strategy to restructuring, changes in HR policies to influencing key decisions executives need to take. Fujitsu Voice serves to represent

POL00401634

employees, and facilitates the communication of employee needs when considering key issues, and in many cases, influences those issues. The leadership team values the input and perspective from this group.

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.

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.

Audits by Fujitsu Business Assurance Teams 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.

4.7 Risk Assessment

4.7.1 Risk Policy and Implementation

Fujitsu manages risk and uncertainty in its business in order to improve performance and achieve objectives. All operating companies have a risk management framework. Each company has a designated Chief Risk Management Officer ("CRMO") whose responsibilities include bi-annual risk reporting and prompt escalation of significant risks in addition to managing and monitoring the risk process on behalf of the board. Fujitsu's risk management framework centres on the risk management policy which is a key management policy overseen by the Fujitsu Services Limited board.

Responsibility for implementation of the Manage Risk Policy is delegated throughout the business cycle. Management oversight at critical points in the business cycle is provided through the Review Framework, a structured set of formal management reviews. The management of risk is embedded throughout these structures such that any potential problems can be planned for and managed appropriately. From April 2016, a Risk and Governance Management Board ("RGMB") has directed the implementation of risk policy throughout Fujitsu Services, replacing the UK and Ireland Risk Management and Compliance Committee ("RMCC") and equivalent structures

4.7.2 Fujitsu's Risk Process

The Fujitsu Services Risk Process is used to support the evaluation, reporting and management of risks in the business and is consistent with industry best practice, particularly the International and British Standards and code of practice for risk management (ISO31000 and BS31100). Fujitsu Services uses the international standard (ISO31000) for risk management as the template to improve its risk framework and process.

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.

POL00401634

4.8 Description of Services provided

In relation to the scope of Fujitsu services and assurance provided by this ISAE 3402 report for the examination throughout period 1 April 2017 to 31 December 2017, please note the following changes to Fujitsu IT infrastructure services supporting POL below.

In addition, under POL's evolving service delivery model where reference is made below to 'POL approvals,' this may be provided by POL or their nominated agents.

Credence Application

Fujitsu is responsible for hosting the infrastructure and hardware supporting the Credence application. Fujitsu has no responsibility for application and database support and only provide limited infrastructure support such as monitoring the server health and utilisation. Accenture as the designated IT outsourcing third party provider, has been responsible for managing the Credence user interface functionality, which supports POL's central financial reconciliation process.

POLSAP Application

Fujitsu is responsible for hosting the infrastructure and hardware supporting the POLSAP application. Fujitsu has no responsibility for application and database support and only provide limited infrastructure support such as monitoring the server health and utilisation. User access management, change management and IT operations for the POLSAP application, are centrally managed by Accenture.

HNG-X Application

Fujitsu have continued to provide the same services throughout the period of examination as they have in the previous audit periods.

Please note that the Credence infrastructure is supported by the same people, processes and technology as are used to support HNG-X. On this basis, where the description of system below refers to HNG-X, this also describes how Fujitsu supports Credence for POL. The only exceptions to this are the areas in the table below, where Fujitsu has not been contracted to operate these controls by POL, designated by the not applicable (N/A) references in the ISAE 3402 controls matrix outlined below.

Therefore, this report shall provide assurance as up to the following date for the stipulated 3402 controls covered:

Controls	POLSAP	HNG-X	Credence
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	31 Dec 2017	31 Dec 2017	31 Dec 2017
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.	31 Dec 2017	31 Dec 2017	31 Dec 2017
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.	31 Dec 2017	31 Dec 2017	31 Dec 2017

POL00401634

Controls	POLSAP	HNG-X	Credence
Control Objective 4: Controls provide reasonable assurance that processing is appropriately authorised and scheduled and that deviations from scheduled processing are identified and resolved.	N/A	31 Dec 2017	N/A
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.	N/A	31 Dec 2017	31 Dec 2017
Control Objective 6: Controls provide reasonable assurance that significant operations incidents are adequately reported, tracked, monitored through resolution and resolved timely.	31 Dec 2017	31 Dec 2017	31 Dec 2017
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.	31 Dec 2017	31 Dec 2017	31 Dec 2017
Control Objective 8: Controls provide reasonable assurance that modifications to system software and networks are authorised, tested, approved, properly implemented and documented.	N/A	31 Dec 2017	31 Dec 2017
Control Objective 9: Controls provide reasonable assurance that new or modified application software development efforts are authorised, tested, approved, properly implemented and documented.	N/A	31 Dec 2017	N/A
Control Objective 10: Controls provide reasonable assurance that access to system resources, including computing platforms and operating systems, is restricted to properly authorised individuals.	31 Dec 2017	31 Dec 2017	31 Dec 2017
Control Objective 11: Controls provide reasonable assurance that access to databases, data files and programs is restricted to properly authorised individuals.	31 Dec 2017	31 Dec 2017	31 Dec 2017
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.	31 Dec 2017	31 Dec 2017	31 Dec 2017
Control Objective 13: Controls provide reasonable assurance that remote access is appropriately restricted to authorised personnel.	31 Dec 2017	31 Dec 2017	31 Dec 2017

4.8.1 Physical and Environmental Controls

POL00401634

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 and 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 to restrict individual access to specific data processing areas based on the access level granted. 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.
1.3	**CCTV:** The data centre access is monitored through the use of CCTV video cameras placed at strategic locations around the data centre. The CCTV video footage is monitored by security guards.
1.4	**Security guards:** Security guards are present at the data centre 24 hours per day and seven days per week. The data centre can only be accessed through the security desk manned by a security guard at all times.
1.5	**Data centre visitors:** Visitors are required to sign in at the reception areas and temporary badges are issued. Visitors must be pre notified to data centre security by a Fujitsu employee.
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 by the data centre facilities manager for users with access to the data centre on a quarterly basis.
1.8	**Deletion of user access:** Delivery team managers notify the local site facilities team of terminations or transfers of their direct reports. Upon notification user access is revoked from the security access control system.

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 throughout the data centre to detect abnormal environmental conditions.
2.4	**UPS Supply:** UPS systems are installed to protect the facilities and computer equipment from electrical power fluctuations and outages.

The Trident House campus in the IRE11 data centre 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

POL00401634

Phase I building and an entrance for the 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] systems, 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 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 is located in secure areas of the data centre facility with access restricted to appropriate personnel through the use of an electronic card access system (SAFE); the computer room employs keypad/PIN code technology as an additional level of access control **(1.2)**. All personnel are required to individually swipe in and where applicable, swipe out of an area using badge card readers. "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 follow up on security alerts that are triggered **(1.6 and 1.7)**.

Access to the data centre is secured based on access provided to users based on their role via the electronic card access systems **(1.2)**.

This access system controls entry for all entrances/rooms as per the access provided to personnel, while maintaining the security of the building.

When an employee leaves the data centre, the access card is removed from the system database and it would no longer provide access. 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 the 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 access to, or whether employees are attempting to get into areas at 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. 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.

POL00401634

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 from the data centre facilities manager; 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 authorised **(1.5)**.

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

Persons issuing visitor access cards (reception/site security/DC Operations team) 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 will be electronically disabled and enquiries will be made to the person who has been issued the access card, or the person they were visiting, for the return of the access card.

4.8.1.2 *Monitoring of Individuals with Access to the Data Centre*

The IRE11 Data Centre management and Fujitsu Group Security personnel periodically review reports of 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 servers and hardware equipment are mounted in locked racks or free standing cabinets on the raised floors.

Each computer room is supplied with 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 with 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 the 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 BMS 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).** Maintenance checks are performed at varying intervals dependent on the devices; however, devices are checked at least annually.

4.8.2 Backup

POL00401634

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 the backup and recovery requirements for each platform.
3.2	**Backup Toolset:** Backups are performed either using NetBackup or RMAN (automated tools) respectively for each platform.
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:** Failed backups are logged as events in the Tivoli Works Scheduler tool for System Management Centre (SMC) team review and resolution.

The Solution Owner is responsible for ensuring that, in the event of accidental deletion or corruption of data, 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 as well as the 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 tools 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. TWS 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 during out of office hours (**3.4**).

POL00401634

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 virtual tape or clone images and performing database recovery, such as archive log 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.

Audit retrievals are happening on a fairly frequent 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.

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.
4.2	**Failed job schedules are monitored:** Automated alerts are configured and sent to relevant teams 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*

Jobs are scheduled within the data centre environment with the Tivoli Workflow Scheduler (TWS) which 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 SMC to validate that the defined jobs are appropriately configured within TWS. SMC also performs day to day monitoring and management of the Tivoli toolsets.

If there are job errors/failures in the daily processing, alerts are sent to the Tivoli Business Service Manager (TBSM) via TWS. These alerts are then identified as part of the SMC proactive monitoring of the TBSM tool, further detailed in Control Objective 6 below. SMC will then raise a TFS ticket to the Unix Team based in IRE11 to investigate and resolve the job failure (**4.2**).

Access to maintain and amend schedules is restricted to the Systems Management based in Blackpool (**4.1**). If changes are required to the job schedule, it will follow the standard MSC process described in Control Objective 8.

4.8.4 Availability and Capacity Management

POL00401634

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	**HNG-X and Credence Performance Monitoring:** The SYSMAN 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.
5.2	**HNG-X and Credence Capacity and Availability Monitoring:** The Tivoli ITM tool proactively monitors the availability of Wintel, Oracle 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.
5.3	**HNG-X Monitoring of Service Delivery:** A monthly Service Review analysis is provided to POL to review details of capacity, availability and incident management performance against the agreed service level targets (SLTs).

4.8.4.1 *HNG-X/Credence Capacity and Availability Management*

SYSMAN (Systems Management) is a generic name for the set of platforms and software that provide System and Estate Management support to all HNG-X Platforms (including Credence infrastructure). This includes the capture of availability information for the in scope platforms via the IBM Tivoli Monitoring (ITM) tool (**5.1**).

Fujitsu does not monitor the Credence applications or middleware such as oracle databases supporting it. It only monitors the application servers from a hosting perspective such as health of the platform and disk space.

SYSMAN3 and SYSMAN4 (versions in use) comprises the following tools:

Tool	Scope
IBM Tivoli Monitoring (ITM)	Proactive monitoring of Data centre Platforms.
Tivoli 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.
Tivoli Netcool Reporter	Reporting Product for SYSMAN reports.
Oracle Enterprise Manager (Oracle Grid) (OEM)	Monitoring of Oracle Databases.

POL00401634

SYSMAN3 and SYSMAN4 collect events using Tivoli Omnibus and present this to the SMC team via the Tivoli Business Service Manager (TBSM) tool, which provides views and alerts in a business context, correlated to the application or system that is impacted (**5.2**).

- Events collected by a SYSMAN version from the counter estate are sent to the Audit Server from the SYSMAN platforms and includes details related to the following:
- Quality of Service.
- Operating System.
- Application and Branch Router.

Systems within the Data Centre are proactively monitored through the use of ITM agents which gather the event data at regular intervals and measure the data against thresholds and raise alerts if the thresholds are breached.

ITM includes operating system agents that alert on CPU and Disk space events. Databases are also monitored using Oracle Enterprise Manager (OEM). Custom Agents are used within HNG-X to capture:

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

SYSMAN feeds alerts into Tivoli Omnibus using event probes which include:

- SNMP Traps.
- Unix (Solaris and Redhat) Syslog probes.
- Unix SyslogNG (Syslog Server).
- Windows Event logs.
- Text file (Application logs).
- EIF Probe (Integration to Tivoli Monitoring ITM).

The SMC monitors the output from the Tivoli systems and raises appropriate alerts via the TFS toolset and where appropriate KEL fixes, incidents or major incidents are applied.

Fujitsu does not monitor the Credence applications or middleware such as oracle databases supporting it. It only monitors the application servers from a hosting perspective such as health of the platform and disk space.

Access to administer the tools is restricted to authorised users.

The Fujitsu Problem and Incident Management team report the branch and central branch and central network availability against the agreed SLTs including the 'Branch and Counter' availability as well as the network availability on a monthly basis to the SSC (**5.3**).

POL00401634

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:** Fujitsu has documented policies and procedures for managing incidents impacting the in scope applications which are available via EMEIA Connect 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 resolved in a timely manner, as per the assigned priority.
6.4	**Major & Security Incident review:** Once a Major or Security Incident is resolved, a formal closure and review is performed, 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 tools automate the collection of events and feed them to the Tivoli Business Service Manager to 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**). It has documented procedures for managing incidents impacting the in scope applications which are available via EMEIA Connect to Fujitsu teams. These documents are also available on Dimensions and the key ones are Customer Service Problem Management Procedure (SVM/SDM/PRO/0025), POA Incident Enquiry Matrix (SVM/SDM/PRO/0023), POA Operations Major Incident Procedure (SVM/SDM/PRO/0001) and POA Operations Incident Management Procedure (SVM/SDM/PRO/0018).

The process applies to all incidents raised by Fujitsu's POA Major Account Controllers (MAC) team or by the System Management Centre (SMC) (out of hours or for systems monitoring tools), where they are related to the Fujitsu outsourcing contract. Post Office Limited (the user entity) appointed Atos as their Service Integrator including the primary service desk function (Atos Service Desk, which may also be referred to as SISD).

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".

POL staff, e.g., Post Masters, either raise incidents with the ATOS Service Desk or POL's Network Business Support Centre (NBSC) and, where relevant, they are passed via the ATOS Service Desk on to the Fujitsu POA MAC or SMC desks. Fujitsu raised incidents are logged and managed using the Triole for Service (TFS) tool which also produces various reporting criteria on incidents. The ATOS Service Desk raise incident tickets in SDM12 which feed via a HDI link into TFS and, therefore, indirectly ATOS Service Desk can also raise TFS incidents. Feedback and responses on the ATOS Service Desk raised incidents can be sent back to SDM12 over the HDI link. This HDI link does not support incidents raised in TFS by Fujitsu teams.

Fujitsu POA incidents raised by the MAC team are either voiced to the ATOS Service Desk by phone or e-mailed. Fujitsu POA incidents raised by the SMC, e.g., those that are for external third party suppliers to POL, are generally phoned through to the ATOS Service Desk for them to manage the POL suppliers.

POL00401634

On a daily basis, the Fujitsu MAC team reviews the number and severity of outstanding incidents within TFS. The scope of the process is from the receipt of an incident by the MAC/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).
- Ensuring incident priorities are linked to business/user impact and business urgencies.
- Keeping the user informed of progress.
- Reduced unplanned downtime.
- Improved customer satisfaction.

All incidents reported by 'contact' with the MAC/SMC desks or the ATOS Service Desk, can transfer incidents from SDM12 into TFS. A Contact is defined as SDM12 incident transfer from ATOS Service Desk, voice, e-mail or a Tivoli Alert generated by the Tivoli Event Monitoring tool as the methods of communication with the MAC or SMC and fall into the following categories:

- Business process error.
- Hardware (Data-centres) 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. 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 MAC/SMC.

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

- Fujitsu Service Lines or Functions.
- POA IT Service Management.
- Third Parties.
- Fujitsu Service Delivery Management.
- ATOS Service Desk.

The main roles required by the process are:

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

POL00401634

- Service Desk Agent - To provide a single point of contact for users, dealing with the management of routine and non- routine Incidents, Problems and requests.
- Incident Resolver - To accurately diagnose and resolve Incidents and Problems within SLA, and to assess, plan, build/test and implement Changes in accordance with the Change Management Process. This role will typically be fulfilled by the support teams and service delivery units.

Once the details of the incident are recorded in TFS the MAC/SMC team assigns a priority level to the incident (ATOS Service Desk assign incident priority before transfer to TFS). If the call is classed as a Security Incident or Major Incident it follows a different route detailed overleaf.

Incidents in TFS are allocated a priority which should be aligned to the potential impact of the event and the urgency. The impact of an incident is derived from a combination of its criticality (also known as severity) and the number of users affected, whereas the urgency is calculated from the required speed of resolution for the agreed Service Level Agreement for the service(s).

Alternatively, the priority maybe assigned using the information contained within the Knowledge Entry Logs (KEL) within the Knowledge Database.

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.

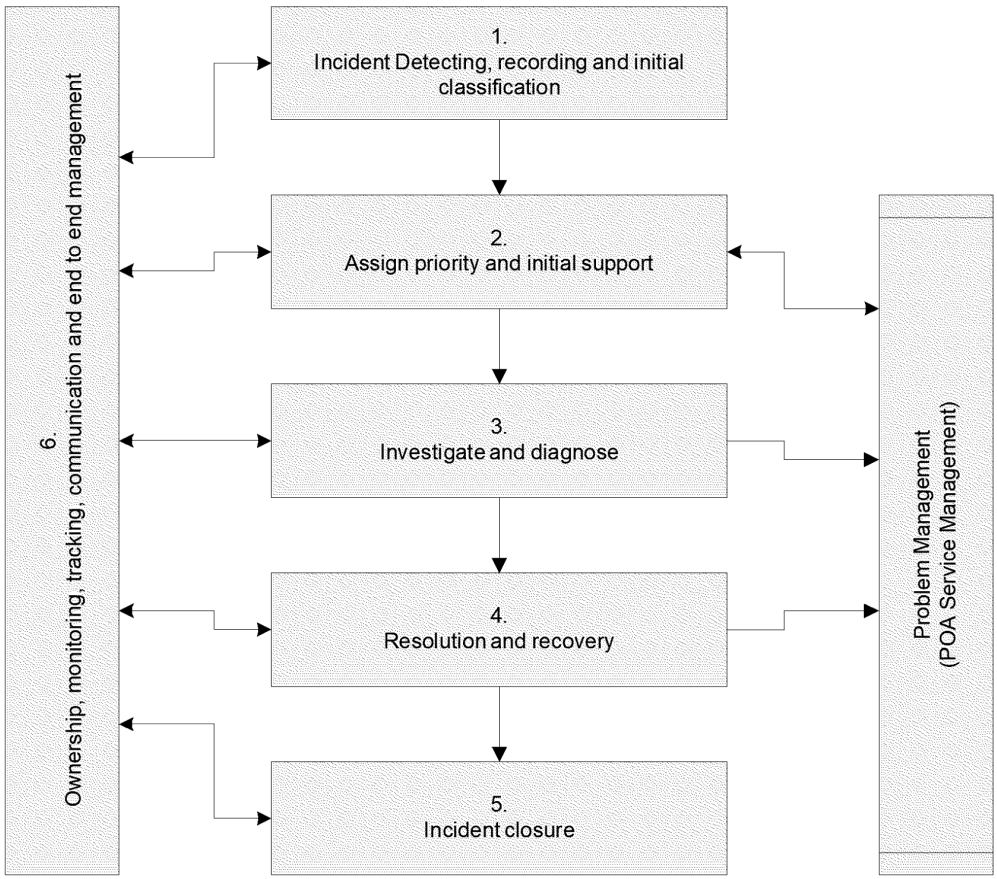


Figure 5. Incident Management Process

POL00401634

When a new TFS incident is raised or received, the Knowledge Database is checked for KEL information about the issue which provides avoidance actions. Where applicable, a resolution or work around is applied and details are linked to the parent Incident / error log for this known problem and the incident is closed. If the incident is not resolved by either the MAC or SMC teams, the TFS call is passed to the appropriate Service Delivery Unit (SDU).

Incidents are first assigned a criticality value and then an urgency value based on the criteria listed further below. Once these are determined, the incidents is assigned a priority value (1 - 5).

Criticality	Value (1-5)
Critical	1
High	2
Medium	3
Minor	4
(Cosmetic – Incident only) / Change (Incident & Problem)	5

Urgency	Definition
1	• Has a significant adverse impact on the delivery of service to a large number of end users. • Causes significant financial loss and/or disruption. • Results in any material loss or corruption of customer data. For example, incidents with this urgency may affect the COMPANY.
2	• Has a moderate adverse impact on the delivery of service to a large number of end users. • Causes a financial loss and/or disruption to the customer which is more than trivial but less severe than the significant financial loss described in the definition of an Urgency level of 1. For example, incidents with this urgency may affect a VIP SITE.
3	• Has a moderate adverse impact upon the delivery of service to a small or moderate number of end users. For example, incidents with this urgency may affect ALL COUNTERS IN A MULTIPLE COUNTER BRANCH or a SINGLE COUNTER BRANCH.
4	• Has a minor adverse impact upon the delivery of service to a small number of end users. For example, incidents with this urgency may affect a SINGLE COUNTER IN A MULTIPLE COUNTER BRANCH.
5	• Has no impact upon the delivery of service For example, incidents with this urgency may affect a SINGLE PERIPHERAL IN A MULTIPLE COUNTER BRANCH.

If the incident is a known current issue, then the ATOS Service Desk is advised of the status of the incident and the TFS parent incident is updated with the new child incident and the SDU(s) managing the parent incident's resolution are advised of another occurrence of the issue. The SDU investigates and diagnoses the incident, based on the information in TFS, together with new information. The SDU also coordinates where Fujitsu sub-contract third parties are involved.

POL00401634

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 MAC/SMC to implement. The parent incident record is the first incident for an issue in TFS and is used as a tracking call for incidents with children incidents.

The incident is then passed to the MAC/SMC to manage and when the call is resolved and this is agreed with the person, team or third party who raised it the TFS incident record can be closed. The MAC/SMC team may request incident closure from the POA Duty Manager, e.g., where neither POA nor an external POL third party has identified the underlying cause of an event which triggered an incident.

Throughout the incident life, the MAC/SMC retains ownership for monitoring and keeping the incident logger informed of its progress, unless the incident is specifically software related, in which case SSC holds the responsibility for confirming details of resolution.

The MAC/SMC manage the complete end-to-end incident process within the Fujitsu POA domain. Their activities include:

- Regularly monitoring the status and progress towards resolution of all open Incidents.
- Proactively keeping the ATOS Service Desk informed of progress.
- Monitoring Service Level target (SLT) information and escalating accordingly if an incident looks likely to breach SLA thresholds.

Fujitsu is required to work to POL Service Level agreements and availability targets and not incident resolution times. So Major incidents would be 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 ensures that the full resources required to resolve it are available and committed.

4.8.5.2 *Major Incidents Definition*

As a general rule, a Major Incident will always be an incident rated as priority 1 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 priority 1 qualify as Major Incidents. 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 priority 1.

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

In the event of a Security Major Incident (which may also include PCI Incidents), the POA Security Operations Team (SecOps) must be alerted, see details below. The POA incident procedure (SVM/SDM/PRO/0018) Appendix A and HNG-X Security Business Continuity Plan (SVM/SDM/PLA/0031) provides guidelines on potential security incidents.

4.8.6 Major Incident Process

An initial impact assessment of an incident is undertaken by members of the MAC team to determine if it should be classified as a priority 1 incident, as described above. The POA Duty Manager ultimately decides if the incident should be handled as a major incident. As a general rule the POA Duty Manager will undertake the role of the Major Incident Manager and generally calls a Technical Bridge.

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

POL00401634

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

Generally, ATOS Service Management will be informed by POA Service Management of the Major Incident, where impact is across domains.

Once a Major Incident is opened the relevant internal SDUs, Fujitsu teams and Fujitsu third party suppliers are contacted to initiate investigation and diagnosis. A Technical Bridge (technical conference for Technical experts and SDU's to discuss and analyse the incident and to formulate an action plan to restore the service to POL without delay), which is managed as an internal conference call, is scheduled. This generally has a standard agenda and all the relevant Service Delivery Units, support teams and Service Delivery Managers (SDM) are invited. The Technical Bridge is technically focused and the Major Incident Manager should document the activities and actions of the Technical Bridge so that a Major Incident Report can be produced.

The Technical Bridge aims:

- To discuss and 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 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.

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 Technical Bridge conference call. If during the Technical Bridge a clear recovery path is identified, this is discussed and agreed on the call. Where co-operation or approval is required from ATOS Service Management or POL, and their third party suppliers, the POA SDMs or Senior SDMs will contact them and request the approval or assistance. Following agreement the recovery is implemented.

After the Technical Bridge, the Technical Recovery Manager will liaise with the SDUs and/or Fujitsu third parties to progress either the investigation or recovery. If no clear recovery path is identified, the decision is then taken on whether to escalate for Service Bridge direction. Service Bridges conference calls are held with ATOS Service Management and/or Post Office Limited (and possibly their third suppliers).

The nature of the Major Incident determines which POA BU Service Team members and ATOS and/or 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.

POL00401634

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.

Note: Where the underlying cause of a Major Incident is in a third party domain, e.g., a Fujitsu non-POA team or POL third party supplier it is expected that they, or ATOS as Service Integrator, arrange the conference calls, hold the formal closure review and produce the Major Incidents reports.

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 also extends 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 either the MAC or SMC Team then transferred to the SecOps call stack, once it is initially assessed as a Security Incident by MAC/SMC.

Security Incidents may also be reported directly into the POA SecOps team via the reporting button on the POA Portal. The initial report will be validated & clarified by SecOps, with calls made to the initiator if more information is required. SecOps will follow team work instructions to progress their investigation.

All Security Incidents are reported to the SecOps team via a dedicated mailbox and escalated by phone if necessary. Depending on the type of Incident and the severity of the incident, POA Security makes the decision to escalate details to the POL/ATOS Security teams. In the case of Data Centre incidents, POA Security also informs the Data Centre Manager if this has not already been done.

POL00401634

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.

The investigation of a reported incident is carried out by a nominated investigator from the POA SecOps team. ATOS and POL Security Teams will be on hand to provide support as required and in accordance with the POL/ATOS Information Security Incident Management Procedure. The investigator will obtain as much original evidence as possible to ensure that is admissible in court, if required.

Following the initial investigation and where considered appropriate, the appropriate senior manager within POL liaises with the local Police or other external agencies.

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 Route Cause Analysis, trending & lessons learned.

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). POA will also submit a quarterly report to the Fujitsu Security Management Forum, to ensure that Fujitsu Security Incident trends can be reviewed in the round.

4.8.7.2 *Incident Reporting*

The Communications Management Team (CMT) prepares a daily status report of all open incidents affecting the branch and counter availability. The report is sent to Fujitsu Incident Management, Atos and POL for review.

4.8.7.3 *Alert Handling*

As mentioned in the Control Objective 5 process narrative above, The ITM and Netcool Omnibus tools monitor the platforms for availability and feed the alerts logged in TBSM for SMC review. Incidents are only logged in TFS for alerts that trigger a status change, which then follow the incident management process described above.

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
5.3	**Monitoring of Service Delivery:** A monthly Service Review analysis is provided to POL to review details of capacity, availability and incident management performance against the agreed service level targets (SLTs).
7.1	**Network performance criteria:** Network availability and performance requirements are clearly defined between Fujitsu and POL in the Network Service policies and network service is measured and monitored using these agreed service levels.

POL00401634

#	Control
7.2	**Network change management:** Network changes are managed using the standard Fujitsu MSC process which includes authorisation, testing (where deemed appropriate) and approval prior to deployment.
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.

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) which define the following (**7.1**):

- The Service definitions.
- Availability Requirements.
- Service levels targets.
- Assets and license.
- Dependencies and Interfaces with other Operational Services.
- Post Office Dependencies and responsibilities.
- Business Continuity.
- The Documents set supporting the Service.

4.8.9.2 *Provision of the Network Service*

Fujitsu provides network services 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 networks.

Wide Area Network Services are provided through a number of third parties (such as Vodafone, Virgin Media, and BT) 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 Control Objective 8 (**7.2**).

4.8.9.4 *Network Availability Monitoring*

Fujitsu has its own dedicated NOSS team to monitor the availability of Network Services to POL using TFS (and MSC if applicable) to raise problems or incidents to the Network, Firewall or IDS teams for resolution which, where applicable, follow the standard Incident management process described in Control Objective

POL00401634

6 above (**7.4**). Networks are monitored for availability via the Spectrum, Netcool and HP Openview tools which send automated alerts to NOSS.

4.8.9.5 *Network Service Monitoring*

The Fujitsu Problem and Incident Management team report the branch and central branch and central network availability against the agreed SLTs including the 'Branch and Counter' availability as well as the network availability on a monthly basis to the SSC (**5.3**).

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 below:

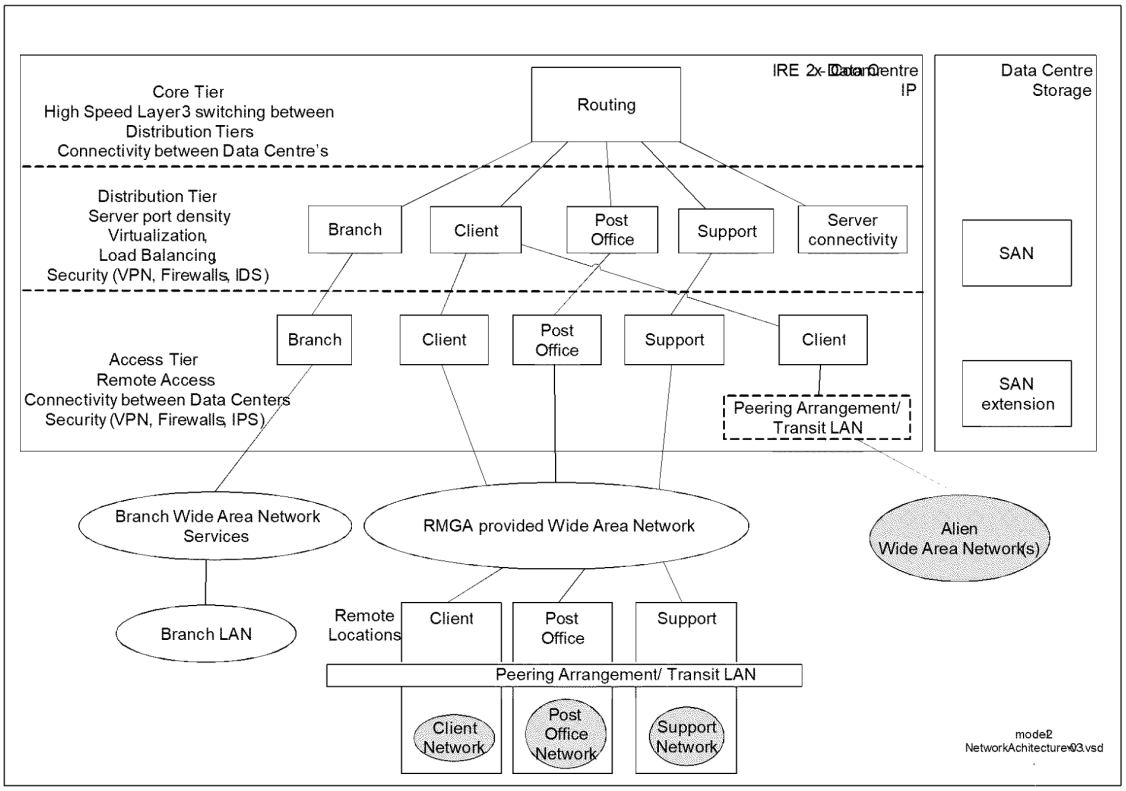


Figure 6. Network Design

Testing is provided through the standby data centre for Live System Test and System and Volume Integration during normal operations. This test support would cease, if the standby data centre was required to act as the primary. Under normal business as usual conditions, the traffic is segregated between the production and test environments by means of various physical devices and logical means of separation

POL00401634

as appropriate. Change Management is strictly controlled through a variety of internal change & release processes and procedures – see Control Objective 8 below for more information on change management for network components.

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 diagram overleaf illustrates how Network Domains fit within the Network tier model.

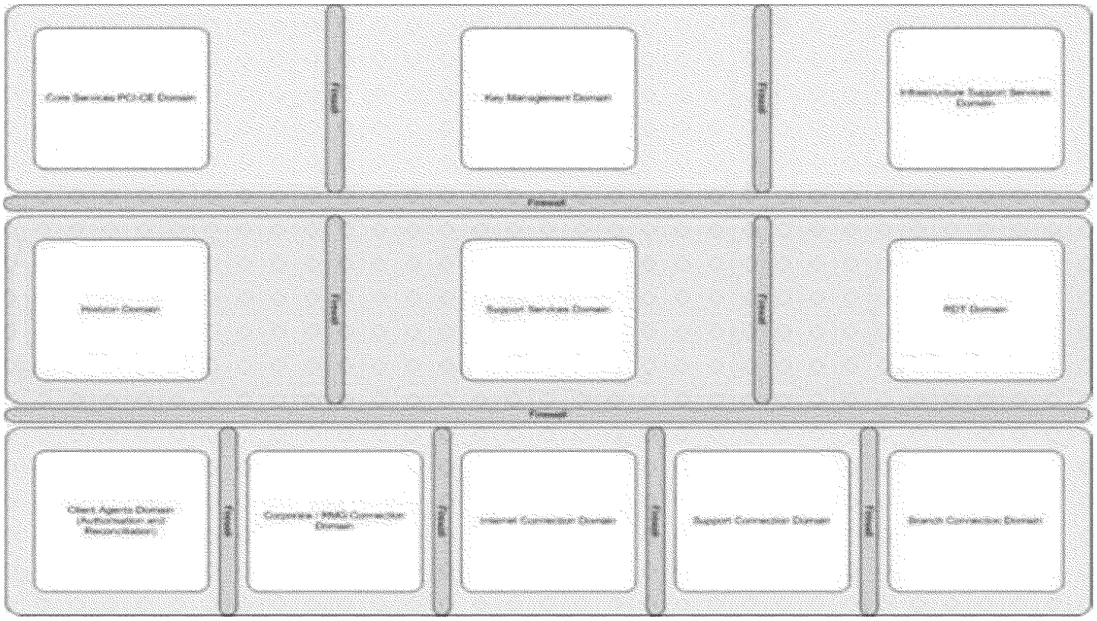


Figure 7. Network Tier

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, which 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. The perimeter can be best described as the collection of devices managed (or monitored) by Fujitsu Services. At the boundary of these managed devices are firewalls (hardware or software-based), 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.

POL00401634

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 changes that affect service or operational change and require formal release are subject to the Managed System Change (MSC) change process (**8.1**). Key change types that fall into scope for this process are listed below:

- Major Business Change – Request from Customer or Fujitsu for large-scale change to the service or service infrastructure, such as business platform, operating system, business unit location move, add new business or major location to service.
- Business Change – Request for catalogue or other change for which impact assessment, planning and costing are required.
- Minor Change – Request for a standard catalogue service or administrative change of known low impact.
- There are three distinct priorities of change:
    - Emergency/RetrospectiveChanges – These types of changes exists for the sole purpose of implementing a critical modification to a live environment to ensure the continuation of an existing service, and preventing interruption to business activities. The life cycle is followed either as an Emergency change needed to be implemented within up to four hours' time or retrospectively for a change already made and both requires the duty service manager's prior authorization.
    - Expedited Changes - An expedited change is made when a compelling business reason exists to make the change within a shorter time scale than that agreed within the SLA. Expedited changes follow the complete Change life cycle, but in an accelerated form, and require an increased level of delegated authorization and may be subject to CAB approval.
    - Normal Changes - A normal change is made in line with the time scale contained within the SLA or for internal changes as mutually agreed and may be subject to CAB approval.

These changes include POL authorised project work with Fujitsu, POL 3rd Party or POL Network Partners. These types of changes are supplied by POL and are then recorded in a 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.

POL00401634

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, 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 for major changes 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).

A change goes through following stage gates before being implemented to production:

- The request for the change from POL (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).
- 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 is responsible for the following(Operational Changes):
    - Facilitating authorisation to implement change.
    - Authorising and Communicating the Change Schedule.
    - Chairing the CAB/s (see CAB).
    - Approving or rejecting changes.
    - Reviewing and ensuring process conformance.

POL00401634

- If the above are in place, the designated 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 a 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.

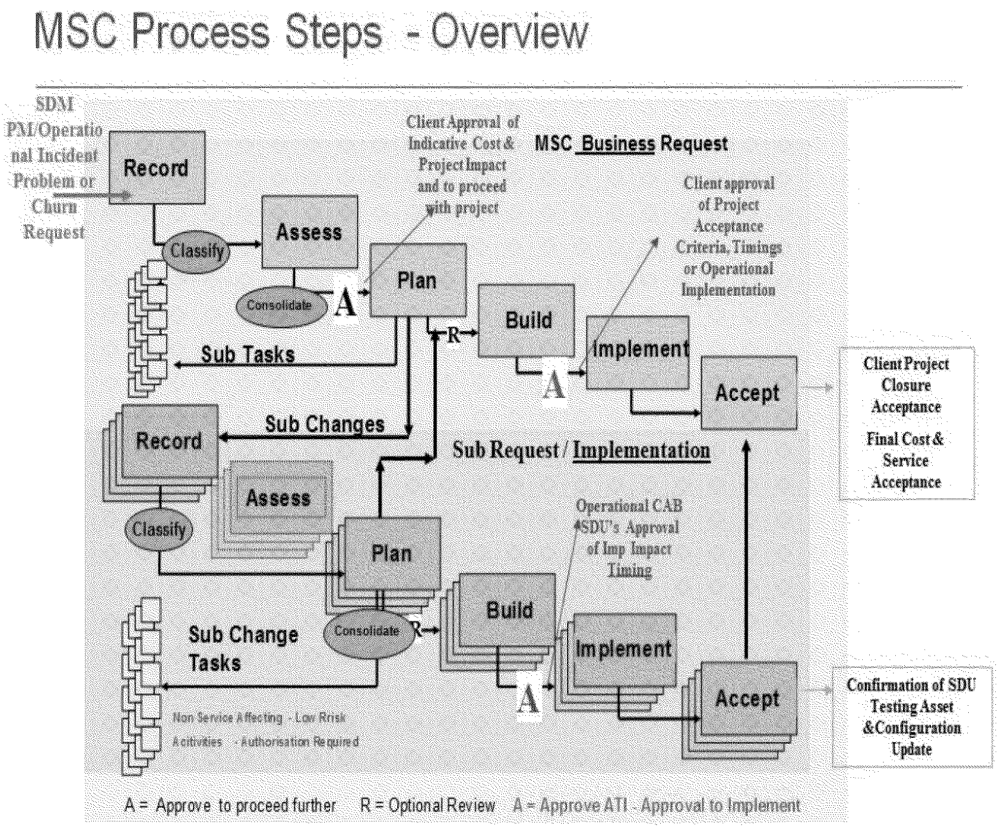


Figure8. MSC Process

4.8.10.2 *Emergency Changes*

Emergency changes are progressed through one of following two methods:

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

Both processes will document changes required in the MSC toolset.

POL00401634

A service-affecting incident calls for a Technical Bridge which is convened (see the Incident Management section in 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 of a lower impact such as a disk failure, the resolver (often an incident manager) will request that an E-CAB be 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 sent to the mandatory assessment teams with a timeframe of turning around the assessments tasks within an hour and this is documented with the MSC ticket and TFS is updated accordingly. The incident or change manager will contact the POL Change Control to discuss the emergency and ask for verbal approval 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 stored in SharePoint and is reviewed and approved by POL and 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 to move code builds between environments or promote transports to live. Segregation of duties is enforced between users able to develop and implement changes respectively.
9.6	**Approval to implement changes:** POL approval is required to promote application 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*

External requests for changes are be raised by POL 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) by Fujitsu.

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.

POL00401634

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 be able 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 and then once successfully approved, a formal agreement is signed which then allows the CP to be progressed.

Project Changes are allocated unique numbers and logged within a database (PVCS) and updated 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 action points from the same are recorded in the change history of the change vehicles in the database. Comments and decisions around the changes are also logged in the change history.

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

POL00401634

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.

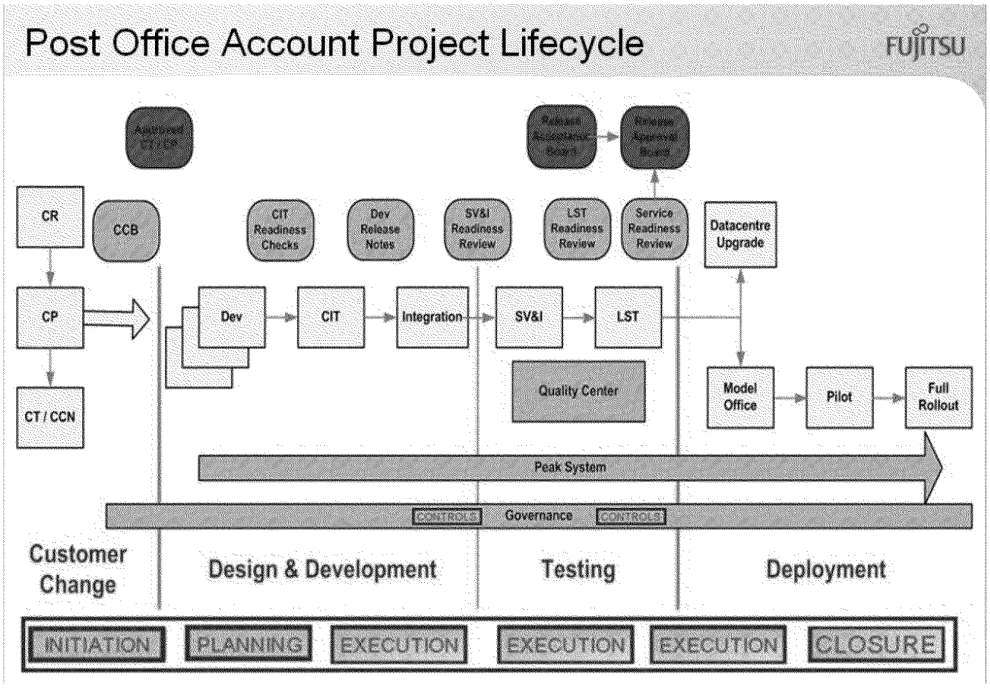


Figure 9. Project Lifecycle

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.

POL00401634

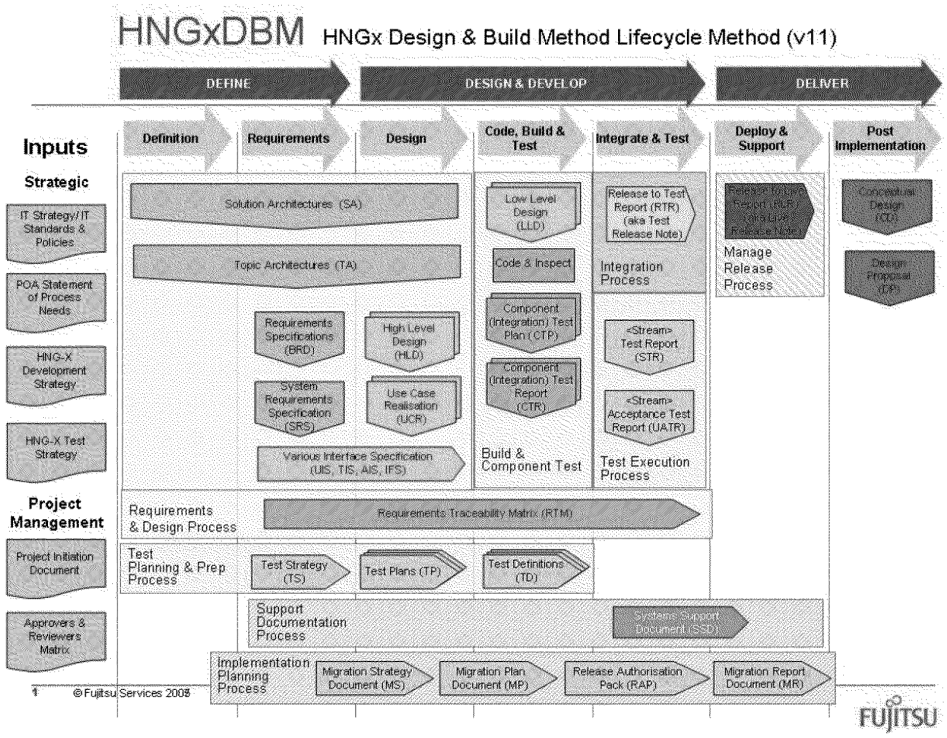


Figure 10. Design and Build Method

4.8.10.5 *Definition*

POL defines projects according to their business needs and provides these to Fujitsu with the 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**).

The Design Proposal contains three key elements:

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

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)

POL00401634

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 and Credence projects are approved by one of the approvers defined in PGM/DCM/ION/0001 & PGM/DCM/PRO/0001 (**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 within the Dimensions CM tool (formerly Serena) including locking the code, the checking the 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 checked out by developers with update access in the tool 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 which are reviewed by a separate developer. The initial developer will 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.

4.8.10.10 *Integration and Test*

HNG-X and Credence 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.

POL00401634

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 (PTF's) assign defects into appropriate maintenance releases.

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

LST puts test plans together which are stored 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 has been tested and is either not met or partially met.

A joint Release Acceptance Board is then held with POL to agree on 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 to approve implementation based on whether:

- 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 stored in Dimensions.

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

POL00401634

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 PTF meets on a weekly basis to review the open PEAK tickets and groups these into deployment groups of typically, no more than 20 PEAK tickets.

Development creates 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, 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 tests 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, a PEAK Deployable Product Version Baseline (DPVB) is then created to enable further progression into the Release process.

The package created by Development (PVB) & then Integration (DPVB) respectively is then made available to Release management 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 Enterprise Provisioning Management (EPM) server where TPM resides based on receiving authority from Release Management in the Release Note. SCM is the only team with access rights to move software into the EPM 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 releases 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 EPM server, based on receiving authority from Release Management, in the Release Note.

The final move into production is then made by the relevant deployment team, depending on the platform the change is being made to using the TPM tool via the EPM Linux server (**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.

POL00401634

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 *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 stored in the appropriate Fujitsu's document repositories Dimensions or SharePoint.

4.8.10.17 *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.

POL00401634

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 after approval 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.
10.6	**Periodic User Reviews:** Fujitsu and POL review user access to systems on a quarterly basis to determine the appropriateness of access, and changes performed as deemed necessary.
10.7	**Two-Factor Authentication:** Access to POL systems is controlled using two-factor authentication.

4.8.11.1 *Policies and Procedures*

Fujitsu employees adhere to the over-arching Security Policy Manual (CMP20-01) which is ISO27001 compliant. This policy manual outlines the responsibility for the identification of risks to information security arising through the activities it undertakes and the services it provides, and for the implementation and operation of appropriate countermeasures to manage those risks down to an acceptable level and in line with best practice. The policy addresses security based upon an understanding of the organisation's security objectives, an analysis of security risks and a suite of properly aligned and managed controls in the areas of:

- Organising security.
- Human resources.
- Asset management.
- Logical access control.
- Cryptography.
- Physical and environmental security.
- Secure operations, Communications management.
- Information systems acquisition.
- Development and maintenance.
- Supplier relationships.
- Security incident management.
- Business continuity management and Compliance.

POL00401634

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**). This document will be phased out in 2018 and will be aligned to the EMEIA Security Policy/manual.

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 POLSAP, HNG-X and Credence (e.g., Windows, Red Hat Linux, Solaris, Oracle), 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 (**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 include 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 active 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 to, 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.

POL00401634

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 stored 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 estate which is determined 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 a 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 Service Delivery Teams 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 updated by default 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).

POL00401634

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 described in this report.

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, the 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).

POL00401634

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 which are shown in the Figure 11 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 12 (**10.4**).

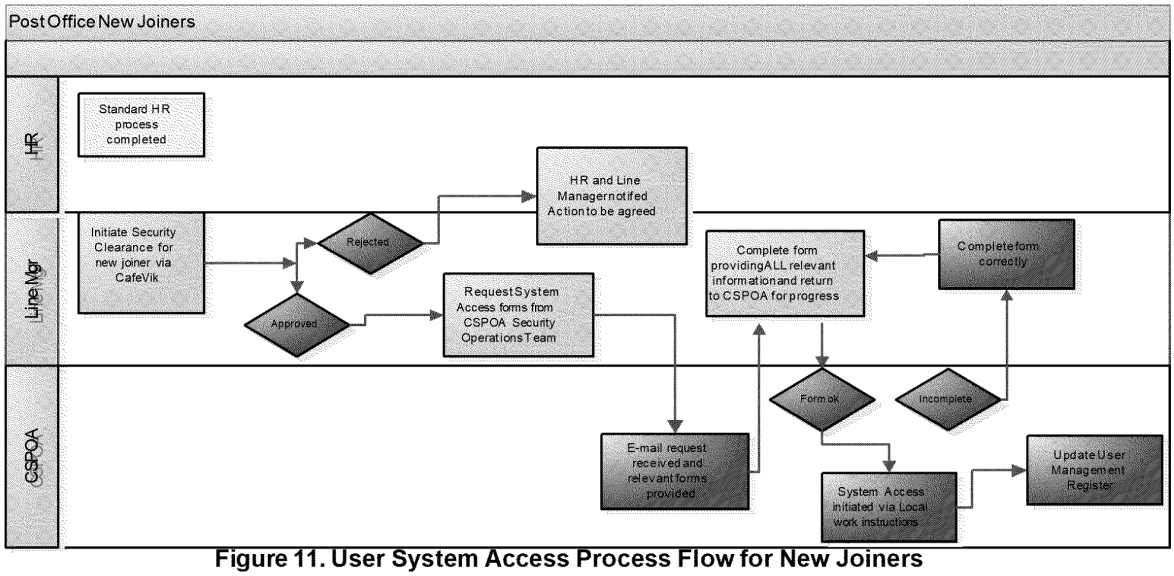


Figure 11. User System Access Process Flow for New Joiners

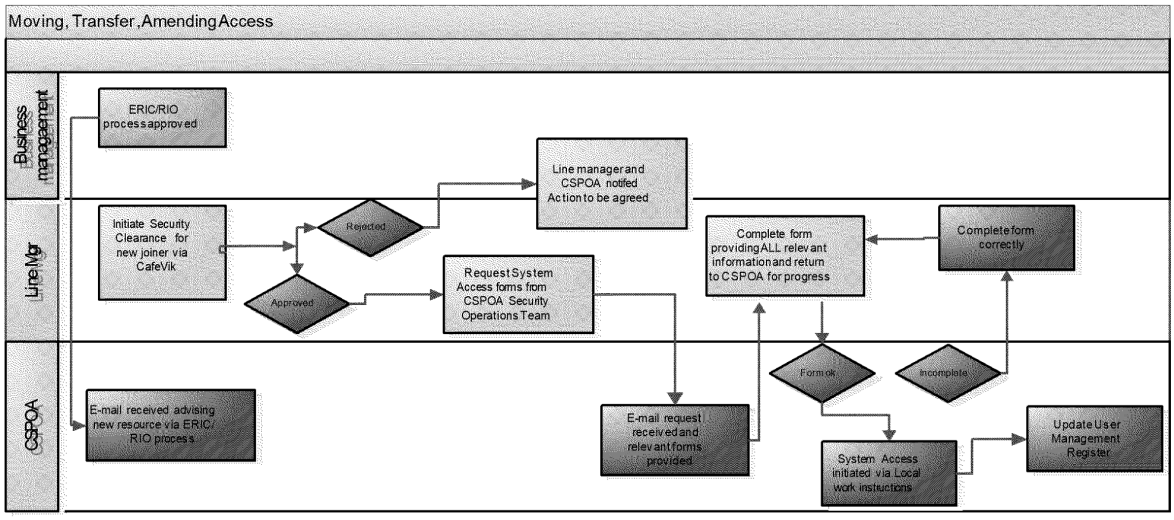


Figure 12. User System Access Process Flow for Movers, Transfers and Access Amendments

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.

POL00401634

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 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 below of the 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.

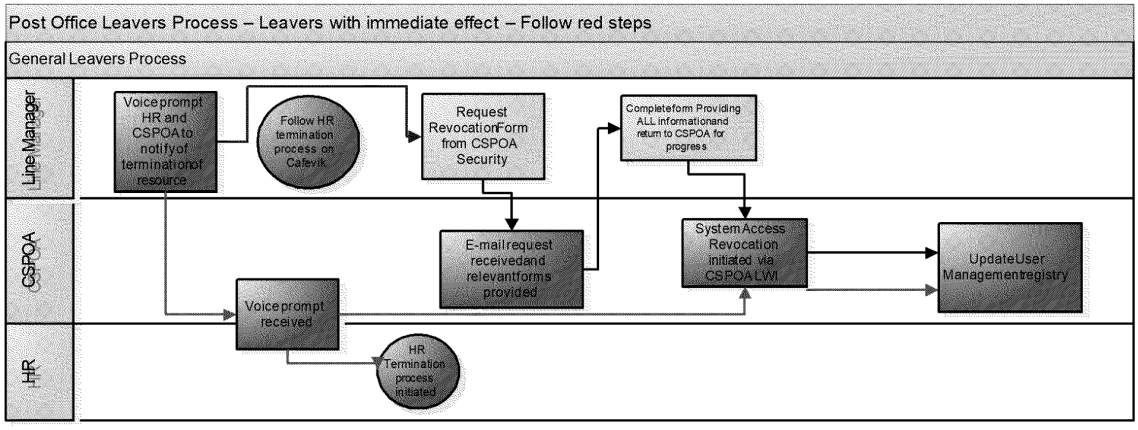


Figure 13. User System Access Process Flow for Leavers

4.8.11.11 *Information Security Management Forum*

The Information Security Management Forum (ISMF) or also known as M6 is a formalised quarterly forum where Post Office and Fujitsu Security operations and governance/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.

POL00401634

The Security Operations quarterly and/or 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.
- Security Reports
- Supplier Compliance Status
- Privileged Accounts Review (**10.6**).

4.8.11.12 *User Authentication Technologies*

User authentication is two-factor, including dynamic password authentication against an external database. Further defence is ensured through the Network Team requiring system access via TACAS+ authentication (**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 and Credence platform. Users must connect to SSN Terminal Servers in order to access to HNG-X and Credence platforms within the data centre. As such, all HNG-X and Credence 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 is restricted to appropriate Fujitsu personnel.
11.3	**Database Administrators:** Access to administer POL databases is restricted to appropriate Fujitsu personnel.
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.
11.5	**Unauthorised 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.
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.

POL00401634

4.8.12.1 *Patch management*

Fujitsu's POA SOT and the Service Delivery teams (SDT) 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 is stored within SharePoint.

The Deployment Spreadsheet is reviewed by the SDTs 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 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*

System or Database Administrator user management controls are only implemented once Corporate Fujitsu approval has been granted for access to various sites and systems. 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.

POL00401634

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 ensures 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 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. It is important to note that Tripwire does not cover the SAP environment as SAP application data cannot be modified at an infrastructure level for this solution.

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 a formal closure and review is performed including, if applicable a Root Cause Analysis.
12.1	**Firewall Configuration Access:** Access to set-up and configure firewalls is restricted to appropriate users from the Networks team.
12.2	**Configuration Changes:** Changes to firewall configuration follow the standard Fujitsu MSC process including authorisation, testing (where deemed appropriate) and approval of changes before they are implemented.
12.3	**Anti-virus software:** Anti-virus software is installed on critical Windows and Red Hat Linux network platforms as agreed with POL. Installed anti-virus software is up to date in line with agreed contractual requirements.
12.4	**Intrusion Detection System (IDS):** IDS is installed on critical network segments as per POL contractual requirements to detect threats and alert the networks team.

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 possibility of a potential attack. By restricting the 'attack surface' to a limited number of systems, damage caused as a consequence of the attack, can be kept to a minimum.

The network segmentation is achieved using a combination of physical and virtual controls. Dependent on the Security Domain and specific contractual agreements with third parties, the network segmentation is enforced using VLANs, IP's and Stateful Inspection Firewalls, ACLs, AES Encryption and physical separation.

POL00401634

Network segmentation will also be used to provide separate 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 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 mask internal addresses to the internet using NAT technologies.

Access to set-up and configure firewalls is restricted to appropriate Fujitsu network personnel (**12.1**). MSC process is followed to raise rule set changes to 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 documented in the document SVM/SEC/STD/1985 which is stored securely in Dimensions. This document is compared against the appropriate device's active configuration and helps to ensure these are in line with the recommended 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 the recommended configuration within SVM/SEC/STD/1985 and the operational configuration, they are then investigated to determine whether the environment has been compromised or not and also ascertain why the correct process was not followed.

The SVM/SEC/STD/1985 document is updated every 6 months to keep it up to date.

4.8.13.4 *Anti-Virus Software*

The ESET Anti-virus product is a real-time protection tool and performs automatic, scheduled and manual scans on all managed platforms, in order to identify, 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 any computer.

For the in-scope Linux systems, 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 UNIX (Solaris) 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.

POL00401634

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 updates.

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 Objective 6 above 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.

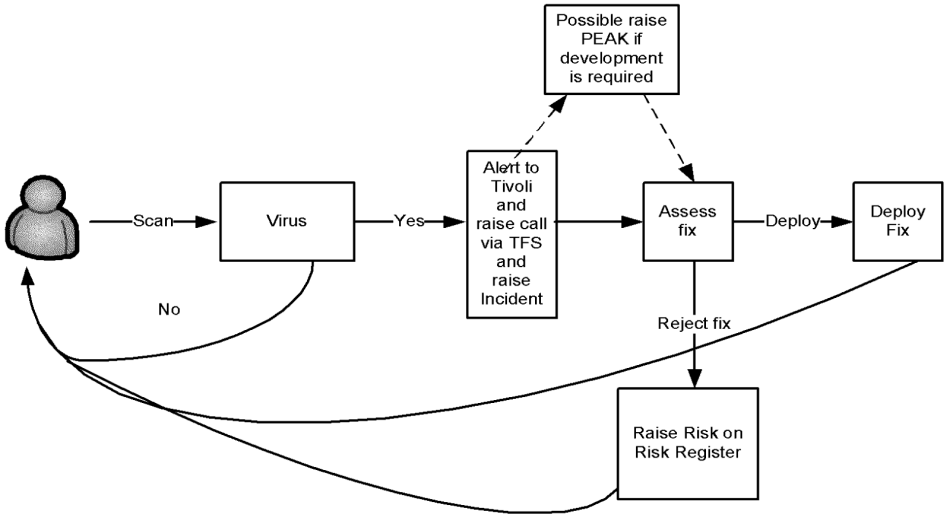


Figure 14. AV Scanning Process

POL00401634

4.8.13.5 *Intrusion Detection System (IDS)*

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

The traffic paths to be monitored were identified by risk assessment during the IDS design phase and are documented in the IDS Appliance Low Level Design (LLD) document (SVM/SDM/OLA/0030). As part of the system design process for new services, additional paths may be included in the monitoring with updates to the IDS Appliance LLD as required.

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

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

To reduce processing overhead on core HNG-X systems, Host Based IDS (HIDS), is not deployed. The inherent security of the platform foundation builds, the hardening process, the implementation of file and process auditing, the network security controls and the implementation of anti-virus on Windows platforms significantly reduce the need for HIDS. This decision came from POL, since POL felt that IDS could affect business transactions at critical business times.

Traffic types that are not inspected by the IDS are:

- SSH traffic originating from the SAS servers to the Counters.
- SSH traffic originating from the SAS servers to the Campus (Data Centre), servers.
- SSH traffic originating from the network management group connecting to the Branch Router.

Any use of other support tools such as Session control protocol (SCP) or SSH File Transfer Protocol (SFTP) are also logged to ensure an audit trail is available in the event of an incident.

For the purposes of IDS coverage, it is assumed that this is acceptable to Post Office Information Security, as the encrypted traffic is tightly access-controlled and is only permitted between specific end-points. Access control is enforced at both the platform level and the network level through the use of strong authentication and restrictive firewall rules.

The Horizon-Online Tivoli Event Management system ensures that any false positives and false negatives are reduced to a minimum. The Incident Management Policy and Security Incident Management Policy documents are updated accordingly. Additionally, intrusion attempts are detected through the use of the Tivoli event management system and specifically, alerts raised as a result of failed attempts to logon or to access data with invalid permissions.

Distributed denial of service (DDOS) attacks are considered to be a low risk for the Horizon-Online system as it operates as a closed network system and therefore the possibilities of attack from Internet (the most significant threat source), although present, are very low. However, to ensure that such attacks do not originate from within the Horizon-Online infrastructure or through connections to and from third-parties, all edge routers and firewalls are implemented with denial-of-service protection. In addition, the segmentation of the Horizon-Online WAN and Data Centre LAN ensures that a successful denial of service attack is extremely difficult to perform.

Daily high alerts and attack type reports are produced by the IDS for POA Security Operations team's review and reference.

POL00401634

4.8.14 Remote Access

13. 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 POL systems are set up appropriately after approval by an appropriate Fujitsu line manager
10.7	**Two-Factor Authentication:** Access to POL 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 mentioned in the **Control Objective 10** process above, remote access for individual users is managed through 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 authorised connection utilising the CHAP Protocol. CHAP requires that both connecting parties (the data centre server 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 by virtue of a one-way hash algorithm.

This expected response must be generated by the counter using both the CHAP secret, and the data centre server challenge value, which ensures 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.

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.

POL00401634

5. Third Party Considerations

We have detailed in the table below the third party considerations whereby additional contractors and sub-contractors (acting as agents of POL) are responsible in part for management of particular ISAE 3402 controls.

ISAE 3402 Control	Third Party	Relationship to Fujitsu and/or POL
3.4 Failed Backups are Tracked and Monitored Failed backups are logged as events in the Tivoli Works Scheduler tool for SMC review and resolution. 4.2 Failed Job Schedules are Monitored Automated alerts are configured and sent to relevant teams upon the occurrence of a batch job failure. These are investigated in line with the incident management process.	Accenture	Accenture acts on behalf of POL and monitors and manages the database backups, including jobs, for Credence and POLSAP.
5.3 HNG-X Monitoring of Service Delivery A monthly Service Review analysis is provided to POL to review details of capacity, availability and incident management performance against the agreed service level targets (SLTs).	ATOS	ATOS are engaged in the monthly Service Review meetings between Fujitsu and POL to assist in the management of key business services; Branch & Central Network, Data Centre Operations, Operational Business Change, service management and, Service level targets analysis for the supporting services to POL. They are also responsible for monitoring the service delivery for Credence and POLSAP.

POL00401634

ISAE 3402 Control	Third Party	Relationship to Fujitsu and/or POL
6.3 Incident Resolution Incidents are resolved in a timely manner, as per the assigned priority.	Computacenter ATOS Accenture	ATOS as the service integrator is involved in the priority assignment to incidents logged in TFS where the incident resolution is their responsibility. As part of the Tower Model service delivery model, Computacenter manages the End User Computing Tower unit. Fujitsu is not responsible for 1st level support for these services but currently still supports 2nd,3 rd and 4th level support operations. Computacenter hosts the front desk operations for POL's branches and head office users, and has taken ownership for 1st level support calls. Accenture are responsible for managing POLSAP and Credence and therefore are involved in resolving any incidents through Fujitsu's incident management procedures.
6.5 Incident reporting On a daily basis, the Fujitsu HSD/IMT reviews the number and severity of outstanding incidents in TFS.	ATOS	ATOS is responsible for monitoring the daily open incidents report provided by Fujitsu as part of their incident management responsibilities.
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.	ATOS	During the change request process, approval is required for certain types that impact the POL estate and in some cases approval is also required from ATOS and other POL agents and third parties.
8.2 Change approval (Operational) 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 the approval documented in the meeting minutes and within the MSC system.	ATOS	After a change has been developed, ATOS are often required to review and approve the change (including performing independent testing) prior to deployment into production. For changes that require CAB approval (including major service interruptions), ATOS actively participate in the CAB process to review and approve changes prior to deployment.

POL00401634

ISAE 3402 Control	Third Party	Relationship to Fujitsu and/or POL
9.3 Design Proposal Projects are outlined in a Design Proposal (DPR) that is stored in SharePoint and is reviewed and approved by POL and Fujitsu management.	ATOS	As part of the design proposal process, ATOS are responsible for participating in the review process of change projects. ATOS liaise with the impacted programme teams, Change Managers and Changer Owners as part of obtaining the Design Authority Board (DAB) approval required to progress change requests to the Programme Change Control Board which in turn is submitted to the Change Control Board for change approval or rejection.
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.	ATOS	ATOS act on behalf of POL as authorising and approving agents for operation business changes applied to POLSAP, HNG-X and Credence which is documented via the Manage Service Change (MSC) process. Depending on the nature of the change request proposed (e.g. business service impacting), the Fujitsu change sponsor is required to seek ATOS approval as part of the change review process to ensure that the change had met the business requirements prior to deployment into production.
10.6 Periodic User Reviews Fujitsu and POL review user access to systems on a quarterly basis to determine the appropriateness of access, and changes performed as deemed necessary.	ATOS	ATOS actively participate on the behalf of POL in the quarterly ISMF M6 meetings across a range of topics including; security operations, governance and compliance, privileged user access reviews, incident analysis, risk register updates, cyber assurance and business continuity around security improvement plans.

POL00401634

6. Complementary User Entity Controls

In designing its system, Fujitsu has contemplated that certain complementary controls would be implemented by POL, or POL's agents to achieve certain control objectives included in this report. There may be additional control objectives and related controls that would be appropriate to the processing of POL's transactions that are not identified in this report. POL should review its contract with Fujitsu to reinforce its understanding of the scope of services provided by Fujitsu and hence the relevance of the controls described and tested in this report.

This section describes other internal controls that should be in operation at POL (including PO third parties) to complement the internal controls at Fujitsu. POL's independent auditors should consider whether the following internal controls are present and operating effectively.

- **Organisation and Administration**

  Controls should be established to:

  - Evaluate that the contracted processes and controls have been implemented.
  - Evaluate and monitor Fujitsu's delivery of services to ensure conformance with contractual obligations.
  - Designate their own internal client representative to ensure 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 non Fujitsu employee access to computer rooms in a manner 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 (including backups) if necessary.
  - Inform Fujitsu of critical scheduled jobs and the appropriate escalation procedures for those jobs.
  - Data Retention requirements are documented and agreed with Fujitsu.
  - Periodically, request restores from backup to validate that programs, files and data are recoverable.
  - Formally agree with all third parties access boundaries to POL's IT infrastructure.

- **Availability and Capacity Management**

  Controls should be established to:

  - 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.

POL00401634

- **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.
  - Formally agree with all third parties access boundaries to POL's IT infrastructure.

- **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 has and they carry out a risk assessment prior to authorising a change.
  - Ensure that client representative participates in, or has input to, the system development activities that are relevant to Post Office, including participation in testing activities, if applicable.

- **Logical Access**

  Controls should be established to:

  - Ensure and implement procedures and documentation for authorising user access to terminals and application functions exist.
  - Periodically, review access granted to users at the application layer, to confirm that such access remains appropriate based on users' job functions.
  - 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.
  - Ensure 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.
  - To 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.
  - Implement procedures to review operating system configurations to ensure settings provide adequate security, particularly where security parameters are maintained at the original client settings when transferred to Fujitsu.
  - Ensure that POL's information security requirements in relation to services provided by Fujitsu are periodically reviewed, discussed with Fujitsu and any necessary changes then made.
  - Review and approve any standard operating system builds and agree on the timeframes for them to be deployed to the POL estate. Ensure that the privileged accounts reviewed in the quarterly meeting with Fujitsu are appropriate.
  - Ensure that that Platform Hardware Instance list is reviewed periodically to confirm the POL infrastructure is appropriate.

POL00401634

- **Incident Management**

  Controls should be established to:

  - Report timely to Fujitsu and/or other vendors of any issues, incidents, or problems with appropriate incident priority ratings that impact the processing of data through HNG-X, POLSAP or Credence.
  - Respond to Fujitsu requests for information in a timely manner and to confirm that issues, incidents, or problems are resolved to their satisfaction.
  - Ensure that POL has appropriate policies and procedures in place to track and monitor major and security incidents to a timely resolution.

- **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.

- **Design and Test**

  Controls should be established to:

  - Ensure that agreements from authorised individuals are made with POL outlining requirements captured in the design and test documents (with sign off) such as Requirements Traceability Matrix (RTM), which are maintained throughout development/test cycles.
  - Agree with Fujitsu an approved, documented process to guide the testing (validation & verification) of software, system and service solutions.
  - Agree actions with Fujitsu regarding the resolution path for recorded deviations from expected outcomes of tests via a bug fix management tool, and reported in a standard format as defined in the EBMS process.
  - Ensure that whenever the customer is performing testing, testing is conducted by appropriately trained and skilled resources (using industry approved testing standard qualification boards).
  - Confirm with Fujitsu that testing is risk based, which will ensure the testing extent is appropriate.

- **Business Change**

  Controls should be established to:

  - Ensure that POL agrees commercial terms definition, costs, resources and requirements of projects prior to initiation of project development.

POL00401634

- **Legal obligations**

  Controls should be established to:

  - Ensure that POL agrees and defines the legal and regulatory standards that Fujitsu is required to meet. Legal and regulatory standard agreements should be formally agreed, documented and signed at executive level.

- **Project Management**

  Controls should be established to:

  - Document, review and approve the lifecycle of new projects, from gathering requirements, through to design, development and deployment into operational running.
  - Agree with POL accepted methods for identifying and rectifying problems and issues early in the project lifecycle, and so reduce the need for costly rework and fixes.
  - Ensure that during the initiation phase of the Project Lifecycle, document, review and sign off customer change requests prior to development work.
  - Review results of test-specific requirements and provide approval sign off at end of testing process.
  - Formally communicate that upon successful testing review, changes developed have satisfied business objectives in the Release Acceptance Board/Requirements Acceptance Board.

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.

POL00401634

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 EY 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, HNG-X and Credence 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.

Remote Access Procedures for Assessing Completeness and Accuracy of Information Produced by the Entity (IPE)

For tests of controls requiring the use of Information Produced by the Entity (IPE), procedures were performed to assess the reliability of the information, including completeness and accuracy of the data or reports, to determine whether the information can be relied upon in the examination procedures. This includes IPE produced by Fujitsu and provided to POL (if relevant and defined as part of the output control objectives), IPE used by Fujitsu management in performance of controls (i.e., periodic review of user listings), and IPE used in the performance of our examination procedures.

Based on the nature of the IPE, a combination of the following procedures were performed to address the completeness and accuracy of the data or reports used: (1) inspect source documentation relating to the IPE, (2) inspect the query, script, or parameters used to generate the IPE, (3) agree data between the IPE and the source, and/or (4) inspect the IPE for anomalous gaps in sequence or timing.

POL00401634

7.2.1 Control Objective 1

Controls Specified by Fujitsu	*Testing Performed*	*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 and made available to Fujitsu staff via the intranet.	Obtained and inspected the data centre and sensitive area specific physical access security policies and procedures for the in-scope Data Centre and determined whether these were made available to Fujitsu staff via the Fujitsu intranet.	No deviations noted.
1.2 Access Within the Data Centre Access beyond the security desk is protected by a key-card system to restrict individual access to specific data processing areas based on the access level granted. 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 that access doors are equipped with a key-card system or equivalent to restrict individual access to specific data processing areas. Obtained and inspected the system generated data centre user listing to determine whether users were granted access levels in order to restrict individual access to specific data processing areas based on the access level assigned. Determined the population of new users granted access to the data centre for the purposes of sample testing the new users to determine whether access was approved by the line manager and access levels specified and actioned as requested.	No deviations noted. Based on inspection of the data centre system access listing, we determined there were no new users to the Fujitsu data centre for the period under examination.
1.3 CCTV The data centre access is monitored through the use of CCTV video cameras placed at strategic locations around the data centre. The CCTV video footage is monitored by security guards.	Observed that CCTV video cameras are placed at key locations around the data centre to monitor user activity. Observed that the CCTV video footage is monitored by the security staff at the data centre.	No deviations noted.

POL00401634

Controls Specified by Fujitsu	Testing Performed	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 and seven days per week. The data centre can only be accessed through the security desk manned by a security guard at all times.	Inspected the data centre security guard log to determine that security guards are present at the data centre (24 hours a day and seven days per week), and that the data centre can only be accessed through a central point (security 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 be pre-notified to data centre security by a Fujitsu employee.	Observed that visitors are granted access to the data centre based upon pre-notification and that they are required to sign in at the reception area and temporary badges are issued after inspection of photo identification. Observed that visitors are escorted by a Fujitsu staff at all times in the data centre.	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.	For a sample of months, inspected the monthly security alert log reviews performed by the data centre facilities manager and determined whether these were reviewed for suspicious activity and proactively followed up.	No deviations noted.
1.7 Review of User Access within the Data Centre Periodic reviews are performed by the data centre facilities manager for users with access to the data centre on a quarterly basis.	For a sample of quarters, obtained the quarterly periodic review of user access performed by the data center facilities manager and inspected it to determine whether the review was performed timely and user access was amended appropriately based on the output of the review.	No deviations noted.

POL00401634

Controls Specified by Fujitsu	Testing Performed	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 Delivery team managers notify the local site facilities team of terminations or transfers of their direct reports. Upon notification user access is revoked from the security access control system.	Obtained the system generated HR leavers list and determined the complete and accurate population of leavers. We observed that there had not been any leavers in the review period.	No deviations noted. As there have been no identified leavers that require their access to the data centre to be removed in the period covered by this report, no occurrences of this control noted.

POL00401634

7.2.2 Control Objective 2

Controls Specified by Fujitsu	*Testing Performed*	*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) throughout the data centre.	No deviations noted.
2.2 Maintenance Schedule Periodic inspection and maintenance is performed on protection devices, sensors and alarm systems.	Inspected the maintenance schedules (including backup generators, UPS, fire detection and suppression, heating, ventilation and air-conditioning units) and service reports for these devices supporting the environmental monitoring controls in the data centre and determined whether the devices had been inspected and serviced during the period of examination.	No deviations noted.
2.3 Environmental Monitoring Smoke detectors and water, humidity and temperature monitoring devices are installed throughout the data centre 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 the data centre.	No deviations noted.
2.4 UPS Supply UPS systems are installed to protect the facilities and computer equipment from electrical power fluctuations and outages.	Observed that UPS systems have been installed to protect the facilities and computer equipment from electrical power fluctuations and outages at the data centre.	No deviations noted.

POL00401634

7.2.3 Control Objective 3

Controls Specified by Fujitsu	*Testing Performed*	*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 the backup and recovery requirements for each platform.	Obtained the Platform Hardware Instance List (PHIL) from the POL owned Dimensions system which details the current listing of all platforms and servers in operational use within the POL account estate. For a sample of platforms, inspected the Backup High Level Design documents to determine whether they listed the backup and recovery requirements for the platform.	No deviations noted.
3.2 Backup Toolset Backups are performed either using NetBackup or RMAN (automated tools) respectively for each platform	Obtained the PHIL listing and selected a sample of platforms. Inspected the tool configuration and determined whether NetBackup or RMAN were installed on the platform to perform automated 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.	Obtained the PHIL listing and selected a sample of servers. Inspected the tool configuration on each server to determine 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 Failed backups are logged as events in the Tivoli Works Scheduler tool for SMC review and resolution.	For a sample backup failure logged in TWS, inspected the alert to determine whether a TFS ticket was logged and resolved appropriately. Please refer to control 4.2 for the TWS configuration for detecting job failures.	No deviations noted.

POL00401634

7.2.4 Control Objective 4

Controls Specified by Fujitsu	*Testing Performed*	*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.	Obtained a system generated listing of access rights within the scheduling tool, TWS, used to maintain the HNG-X job schedules. Inspected the users with access to amend job schedules to determine whether the access was restricted to appropriate personnel based on their job responsibilities.	No deviations noted.
4.2 Failed Job Schedules are Monitored Automated alerts are configured and sent to relevant teams upon the occurrence of a batch job failure. These are investigated in line with the incident management process. *Changes to tool configuration follow the change management process in Control Objective 8.*	Inspected 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 TBSM tool. Refer to control 6.6 for our testing procedures over the handling of alerts.	No deviations noted.

POL00401634

7.2.5 Control Objective 5

Controls Specified by Fujitsu	Testing Performed	Results of Tests
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.		
5.1 HNG-X and Credence Performance Monitoring The SYSMAN tools (Tivoli ITM and OEM) proactively monitor CPU, Memory, Disk utilisation and capacity of internal services on the platforms, raising alerts for investigation by the SMC as appropriate. Administrator access to the tools is restricted to authorised users. *Changes to tool configuration follow the change management process in Control Objective 8.*	Inspected the configuration of the Tivoli ITM and OEM tools on the HNG-X and Credence platform and determined whether they are configured to monitor the CPU, memory, disk utilisation and the capacity of internal services on the servers. Inspected the users with access to the tools used to monitor the environment, and ascertained that it is restricted to authorised users based on their job responsibilities. Refer to control 6.6 for our testing procedures over the handling of alerts.	No deviations noted.
5.2 HNG-X and Credence Capacity and Availability Monitoring The Tivoli ITM and OEM tools proactively monitor the availability of Wintel, Oracle and Unix platforms, feeding platform availability data to Tivoli Business Service Manager (via Netcool Omnibus) about the availability of platforms. Tivoli Business Service Manager (TBSM) presents this data in a business context to the SMC, highlighting service affecting issues. Administrator access to Netcool Omnibus is restricted to authorised users *Changes to tool configuration follow the change management process in Control Objective 8.*	Inspected the Tivoli ITM and OEM tool configurations and determined whether: • These showed that the tools monitor and manage availability and capacity of servers. • Thresholds were defined which, if breached, would send alerts to TBSM for SMC review. Refer to control 6.6 for our testing procedures over the handling of alerts. Inspected the users with access to administer Netcool Omnibus used to monitor the environment, and ascertained that it is restricted to authorised users based on their job responsibilities.	No deviations noted.

POL00401634

Controls Specified by Fujitsu	Testing Performed	Results of Tests
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.		
5.3 HNG-X Monitoring of Service Delivery A monthly Service Review analysis is provided to POL to review details of capacity, availability and incident management performance against the agreed service level targets (SLTs).	For a sample of months inspected the Service Review book to determine whether the: • analysis was provided to POL to review its agreed SLTs. • book contained details of capacity, availability and incident management performance.	No deviations noted.

POL00401634

7.2.6 Control Objective 6

Controls Specified by Fujitsu	Testing Performed	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 Fujitsu has documented policies and procedures for managing incidents impacting the in scope applications which are available via EMEIA Connect to Fujitsu teams.	Through enquiry with management, identified the documents that define the incident management processes for the POL account. Inspected the policies to determine whether these were available to relevant Fujitsu employees via EMEIA Connect.	No deviations noted.
6.2 Incident Prioritisation Incidents are assigned a priority in accordance with the severity levels agreed with POL.	Obtained a system generated listing of incidents from the incident management tool, Information Direct. For a sample of incidents, inspected the incident tickets to determine whether they had been assigned a priority in accordance with the severity levels agreed with POL.	No deviations noted.
6.3 Incident Resolution Incidents are resolved in a timely manner, as per the assigned priority.	For a sample of incidents selected from the incident management tool, Information Direct, inspected the incident tickets to determine whether they had been resolved in a timely manner, as per the assigned priority.	No deviations noted.
6.4 Major & Security Incident Review Once a Major or Security Incident is resolved, a formal closure and review is performed, including, if applicable, a Root Cause Analysis.	Selected a sample of Major and Security Incidents from the incident tool (Information Direct), and inspected the incident tickets and incident reports to determine whether a formal closure and review was performed, including, if applicable, a Root Cause Analysis.	No deviations noted.
6.5 Incident Reporting On a daily basis, the Fujitsu HSD / IMT reviews the number and severity of outstanding incidents in TFS.	For a sample of days, inspected the incident reports to determine whether the Fujitsu HSD/IMT had reviewed the number and severity of outstanding incidents in TFS.	No deviations noted.

POL00401634

Controls Specified by Fujitsu	Testing Performed	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 tools automate the collection of events and feed them to the Tivoli Business Service Manager to highlight areas of concern to the SMC. *Changes to tool configuration follow the change management process in Control Objective 8.*	Obtained a system generated listing of alerts from Tivoli Business Service Manager. For a sample of key events, inspected the alert and TFS ticket to determine whether the alerts were flagged to the SMC for resolution and that the events were resolved in a timely manner.	No deviations noted.

POL00401634

7.2.7 Control Objective 7

Controls Specified by Fujitsu	*Testing Performed*	*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.		
5.3 HNG-X Monitoring of Service Delivery (A monthly Service Review analysis is provided to POL to review details of capacity, availability and incident management performance against the agreed service level targets (SLTs).	For a sample of months, inspected the Service Review book to determine whether the: • analysis was provided to POL to review its agreed SLTs. • book contained 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 policies and network service is measured and monitored using these agreed service levels.	Inspected the network service policy documentation on EMEIA Connect to determine whether these are available to Fujitsu employees and are used to measure and monitor service levels.	No deviations noted.
7.2 Network Change Management Network changes are managed using the standard Fujitsu MSC process which includes authorisation, testing (where deemed appropriate) and approval prior to deployment. *Network Changes follow the change management process in Control Objective 8.*	Obtained a system generated listing of network changes from the change management tool, MSC. Selected a network change and inspected documentation to determine whether this change was managed using the standard Fujitsu MSC process including authorisation, testing and approval prior to deployment.	No deviations noted.

POL00401634

Controls Specified by Fujitsu	Testing Performed	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.		
7.3 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. *Changes to tool configuration follow the change management process in Control Objective 8.*	Inspected the configuration of the HP Openview, Spectrum and Tivoli Netcool tools monitoring network availability, to determine whether they are configured to send automated alerts to the Network Operating Support Service Team (NOSS).	No deviations noted.
7.4 Network Incident Management Incidents relating to network availability are managed using standard incident management procedures.	Selected a network incident and inspected documentation to determine whether it was managed using the standard POL incident management procedures, and is included in the standard incident management reporting to POL. Refer to control 6.2 for our test of the incident management process.	No deviations noted.

POL00401634

7.2.8 Control Objective 8

Controls Specified by Fujitsu	*Testing Performed*	*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.	Obtained a system generated listing of system software and networks changes from the change management tool, MSC. Selected a sample of changes and inspected documentation to determine 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 the approval documented in the meeting minutes and within the MSC system.	Obtained a system generated listing of system software and network changes from MSC. For a sample of changes, inspected documentation to determine whether these had been authorised and the approval was documented in meeting minutes (including CAB approval for major service interruption changes) and within MSC.	No deviations noted.
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.	Obtained a system generated listing of system software and network changes from MSC. For a sample of emergency changes, inspected documentation to determine whether: • they had been agreed, authorised and documented during the incident. • updates to POL had been sent as per the agreed timeframes dependent on the severity of the incident.	No deviations noted.

POL00401634

7.2.9 Control Objective 9

Controls Specified by Fujitsu	*Testing Performed*	*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.	Inquire with management to determine whether documents that define the SDLC for the POL account are in place. Inspected documentation on EMEIA Connect to determine whether these were available to relevant Fujitsu employees, and whether these phases include: • 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).	Obtained a system generated listing of new or modified application software changes from MSC. For a sample of changes inspected documentation to determine whether these had been appropriately approved by either the Change Control Board (CCB) or the PEAK Targeting Forum (PTF) before progressing into development based on the nature of the change.	No deviations noted.

POL00401634

Controls Specified by Fujitsu	Testing Performed	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.		
9.3 Design Proposal Projects are outlined in a Design Proposal (DPR) that is stored in SharePoint and is reviewed and approved by POL and Fujitsu management.	Obtained a system generated listing of new or modified application software changes from MSC. Selected a sample of projects and inspected documentation to determine whether the projects had a Design Proposal (DPR) document that had been reviewed and approved by POL as well as Fujitsu management and was stored in SharePoint.	No deviations noted.
9.4 Change Testing Changes are tested in line with the defined procedure.	Obtained a system generated listing of new or modified application software changes from MSC. For a sample of changes inspected documentation to determine 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 to move code builds between environments or promote transports to live. Segregation of duties is enforced between users able to develop and implement changes respectively.	Obtained the list of users from the EPM server and inspected the users with access to implement changes and determined whether it was restricted to authorised users based on their job responsibilities. Obtained the list of users from the Serena Dimensions tool server and inspected the users with access to develop changes and determined whether segregation of duties was enforced between users able to develop and implement changes.	No deviations noted.

POL00401634

Controls Specified by Fujitsu	Testing Performed	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.		
9.6 Approval to Implement Changes POL approval is required to promote application software changes to the live environment. Approval is captured within the relevant MSC.	Obtained a system generated listing of new or modified application software changes from MSC. For a sample of changes inspected documentation to determine whether POL approval to implement the change was documented within the ticket.	No deviations noted.

POL00401634

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.	Inquired with management to determine the documents that define the information security architecture and procedures for the POL account. Inspected documentation on EMEIA Connect to determine 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.	Obtained the Platform Hardware Instance List (PHIL) from the POL-owned Dimensions system which details the listing of platforms and servers in operational use within the account estate. For a sample of Branch Database platforms in operational use, inspected documentation to determine whether baseline standards had been defined and agreed with POL for these server technologies.	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.	Obtained the PHIL and selected the Branch Database platforms in operational use and inspected key configuration settings to determine whether the platforms had been set up and configured in line with documented and agreed baseline standards. Where settings differed from the baseline, inspected documentation to determine whether these variances had been documented and approved in accordance with defined procedures.	No deviations noted.

POL00401634

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.		
10.4 User (Fujitsu) Set-up and Amendment Fujitsu users requiring new or modified access to POL systems are set up appropriately after approval by an appropriate Fujitsu line manager.	Obtained a system generated listing of users from the POL managed starters, transfers and leavers management tool, EMEIA Connect. For a sample of Fujitsu users inspected documentation to determine whether the users had been set up in accordance with the access request based on the approval by an appropriate Fujitsu line manager.	No deviations noted.
10.5 User (Fujitsu) Deletion Access to Post Office Limited systems for Fujitsu users is removed in a timely manner.	Obtained a system generated EMEIA Connect report of leavers. For a sample of Fujitsu staff that left the POL account inspected the POL account user access lists to determine whether their access had been removed in a timely basis.	No deviations noted.
10.6 Periodic User Reviews Fujitsu and POL review user access to systems on a quarterly basis to determine the appropriateness of access, and changes performed as deemed necessary.	For a sample of quarterly reviews inspected the ISMF M6 meeting minutes to determine whether users and their access rights had been reviewed by Fujitsu security management and POL, and changes requested were actioned appropriately.	No deviations noted.
10.7 Two-Factor Authentication Access to POL systems for Fujitsu users is controlled using two-factor authentication.	Observed a Fujitsu staff logging on to the POL systems network and determined whether it required two factor authentication.	No deviations noted.

POL00401634

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. *Patch updates follow the change management process in Control Objective 8.*	Obtained the Platform Hardware Instance List (PHIL) from the POL-owned Dimensions system which details the current listing of platforms and servers in operational use within the POL estate. For an in-scope sample platform inspected documentation to determine whether the most recent patches had been applied as per the MSC change process.	No deviations noted.
11.2 System Administrators Access to perform system administrator functions is restricted to appropriate Fujitsu personnel.	Obtained the PHIL listing of live POL platforms. For a sample of servers inspected system-generated lists of users with system administrator rights to determine whether access to perform system administrator functions was restricted to appropriate users based on their job responsibilities.	No deviations noted.
11.3 Database Administrators Access to administer POL databases is restricted to appropriate Fujitsu personnel.	Obtained the PHIL listing of live POL platforms For HNG-X, selected a sample of in-scope databases and inspected system-generated lists of access rights to determine whether access to administer the databases was restricted to appropriate users based on their job responsibilities.	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.	Obtained the PHIL listing of live POL platforms For a sample of HNG-X and Credence platforms inspected system-generated lists of access rights to determine whether access to administration tools and system utilities was restricted to appropriate users based on their job responsibilities.	No deviations noted.

POL00401634

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 Unauthorised 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. *Changes to tool configuration follow the change management process in Control Objective 8.*	Obtained the PHIL listing of POL platforms. For a sample of application servers, inspected configuration settings to determine 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.	Obtained the PHIL listing of POL platforms. For a sample of platforms, inspected system-generated lists of access rights to determine whether access to significant production program and data files was appropriately restricted to users based on their job responsibilities.	No deviations noted.

POL00401634

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, a formal closure and review is performed, including, if applicable, a Root Cause Analysis.	Selected a sample of Major and Security Incidents from the incident tool (Information Direct) and inspected incident tickets to determine whether a formal closure and review was performed, including, if applicable, a Root Cause Analysis.	No deviations noted.
12.1 Firewall Configuration Access Access to set-up and configure firewalls is restricted to appropriate users from the Networks team.	Obtained the system list of network users from Active Directory with access to configure firewalls and inspected it to determine whether access was restricted to network team users based on their job responsibilities.	No deviations noted.
12.2 Configuration Changes Changes to firewall configuration follow the standard Fujitsu MSC process including authorisation, testing (where deemed appropriate) and approval of changes before they are implemented.	Obtained the PAB deployment list. Selected a sample change to firewall configuration and inspected change documentation to determine whether the change had been authorised, tested and approved prior to implementation as per the MSC process tested in Control Objective 8.	No deviations noted.
12.3 Anti-virus Software Anti-virus software is installed on critical Windows and Red Hat Linux network platforms as agreed with POL. Installed anti-virus software is up to date in line with agreed contractual requirements.	Selected a sample of servers from PHIL and inspected the Anti-Virus tool to determine that each server had Anti-Virus software installed which was up to date.	No deviations noted.

POL00401634

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.		
12.4 Intrusion Detection System (IDS) IDS is installed on critical network segments as per POL contractual requirements to detect threats and alert the networks team. *Changes to tool configuration follow the change management process in Control Objective 8.*	Inspected the IDS tool configuration to determine whether it is configured to monitor, detect and alert the networks team. Obtained an IDS alert and inspected documentation to determine whether it was managed in accordance with agreed contractual requirements.	No deviations noted.

POL00401634

7.2.13 Control Objective 13

Controls Specified by Fujitsu	*Testing Performed*	*Results of Tests*
Control Objective 13: Controls 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 POL systems are set up appropriately after approval by an appropriate Fujitsu line manager.	Obtained a system generated listing of users from the POL managed starters, transfers and leavers management tool, EMEIA Connect. Selected a sample of Fujitsu users and inspected documentation to determine 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 POL systems for Fujitsu users is controlled using two-factor authentication.	Observed a Fujitsu staff logging on to the POL systems network and determined whether it 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. *Changes to this configuration follow the change management process in Control Objective 8.*	Obtained the high level CHAP password documentation and inspected it to determine whether Radius Authentication and CHAP rules and procedures were established for validating Counters' remote access requests.	No deviations noted.