POL00337569

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

Throughout the Period 1 April 2022 to 31 December 2022

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

POL00337569

Table of Contents

POL00337569

1. Fujitsu Services Limited's Management Statement

19 May 2023

The accompanying description has been prepared for Post Office Limited (POL), who have used Fujitsu Services Limited ("Fujitsu")'s IT Infrastructure services system, and their auditors who have a sufficient understanding to consider the Description, along with other information, including information about controls operated by POL themselves, when assessing the risks of material misstatements of POL's financial statements.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of Fujitsu's controls are suitably designed and operating effectively, along with related controls at the service organisation. The Description does not extend to controls of the user entity, POL.

Fujitsu confirms that:

a. The accompanying Description at pages 5-56 fairly presents the IT Infrastructure services system (System) supporting POL's HNG-X application throughout the period 1 April 2022 to 31 December 2022. The criteria used in making this statement were that the accompanying description:

(1) Presents how the System was designed and implemented, including, if applicable:

- The types of services provided.
- The procedures, within both information technology and manual systems, by which those services are provided for POL.
- The information used in the performance of the procedures and supporting information; this includes the correction of incorrect information and how information was transferred to the reports prepared for POL.
- How the System dealt with significant events and conditions.
- The process used to prepare reports for POL.
- Services performed by a subservice organisation, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
- Relevant control objectives and controls designed to achieve those objectives.
- Controls that we assumed in the design of the system, would be implemented by POL, and which, if necessary to achieve controls objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone.
- Other aspects of our control environment, risk assessment process, information systems (including the related business processes) and communication, control activities, and monitoring activities that were relevant to the services provided.

(2) Includes relevant details of changes to the service organisation's System during the period 1 April 2022 to 31 December 2022.

POL00337569

(3) Does not omit or distort information relevant to the scope of the System being described.

b. The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period 1 April 2022 to 31 December 2022**,** if POL applied the complementary user entity controls assumed in the design of Fujitsu's controls throughout the period 1 April 2022 to 31 December 2022. The criteria used in making this statement were that:

(1) The risks that threatened the achievement of the control objectives stated in the description were identified.

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

(3) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority throughout the period 1 April 2022 to 31 December 2022.

GRO

Dan Walton

Delivery Executive

POL00337569

Building a better working world

2. Independent Service Auditor's Assurance Report on the Description of Controls, their Design and Operating Effectiveness

To: Management of Fujitsu Services Limited.

Scope

We have been engaged to report on Fujitsu Services Limited ("Fujitsu")'s description at pages 5-56 of its IT Infrastructure services system supporting Post Office Limited ("POL")'s HNG-X application throughout the period 1 April 2022 to 31 December 2022 (the Description), and on the design and operation of controls related to the control objectives stated in the Description.

The Description indicates that certain Control Objectives can be achieved only if complementary user entity controls assumed in the design of Fujitsu's controls are suitably designed and operating effectively, along with related controls at the service organisation. Our engagement did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Fujitsu's responsibilities

Fujitsu is responsible for preparing the Description and accompanying statement at pages 1-2, including the completeness, accuracy, and method of presentation of the Description and statement; providing the services covered by the Description; stating the control objectives; identifying the risks that threaten the achievement of the Control Objectives; selecting the criteria presented in the statement; and designing, implementing, and effectively operating controls to achieve the stated control objectives.

Our independence and quality control

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

We apply International Standard on Quality Control I and accordingly maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Our responsibilities

Our responsibility is to express an opinion on Fujitsu's Description and on the design and operation of controls related to the Control Objectives stated in the Description, based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3402, *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of the risks that the description is not fairly presented and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the Control Objectives stated in the description were

POL00337569

Building a better working world

achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organisation and described on pages 1-2.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of controls at a service organisation

Because of their nature, controls at a service organisation may not prevent or detect all errors or omissions related to the provision of IT infrastructure services. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described at pages 1-2. In our opinion, in all material respects:

a. The Description fairly presents the IT infrastructure services system as designed and implemented throughout the period from 1 April 2022 to 31 December 2022.

b. The controls related to the control objectives stated in the Description were suitably designed throughout the period from 1 April 2022 to 31 December 2022 to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period 1 April 2022 to 31 December 2022 and if POL applied the complementary controls assumed in the design of Fujitsu's controls throughout the period 1 April 2022 to 31 December 2022.

c. The controls tested, which were those necessary to provide reasonable assurance that the Control Objectives stated in the Description were achieved, operated effectively throughout the period 1 April 2022 to 31 December 2022 if complementary user entity controls assumed in the design of Fujitsu's controls operated effectively throughout the period 1 April 2022 to 31 December 2022.

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed on pages 57-81.

Intended users and purpose

This report and the Description of tests of controls on pages 57-81 are intended only for POL, as user of Fujitsu's IT infrastructure services system, and POL's auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by POL themselves, when assessing the risks of material misstatements of POL's financial statements.

Ernst & Young LLP

19 May 2023
London
United Kingdom

POL00337569

3. Description of Fujitsu's system of IT infrastructure services supporting Post Office Limited's HNG-X application throughout the period 1 April 2022 to 31 December 2022

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 25 years.

A quick overview of FUJITSU Global key facts:

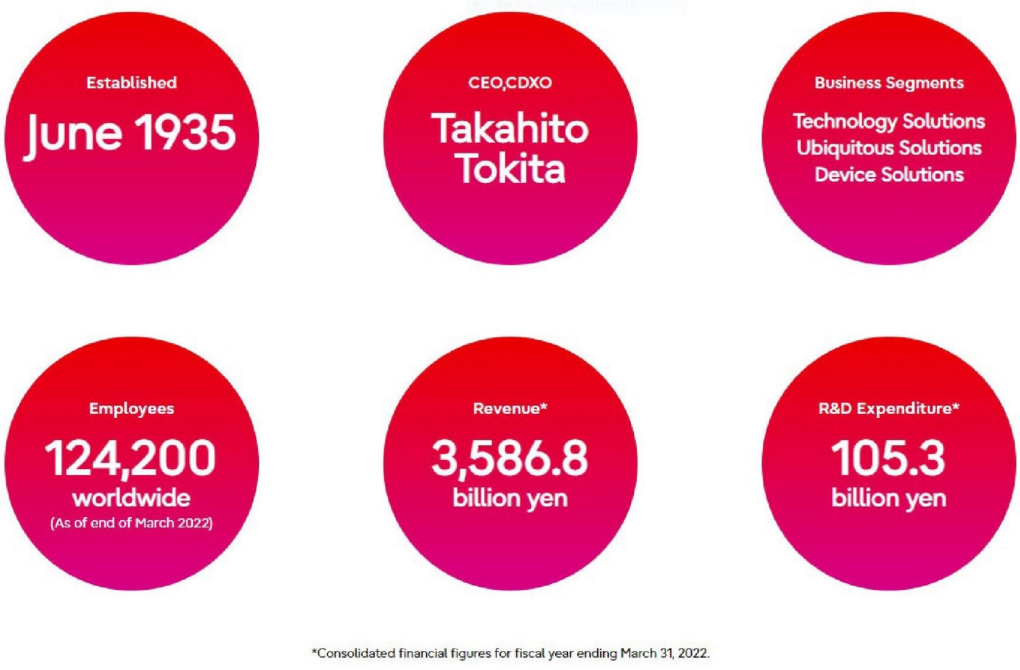

Figure 1. FUJITSU Global key facts

POL00337569

The Company milestones are on Fujitsu's website at Company milestones: Fujitsu Global and are summarised as follows:

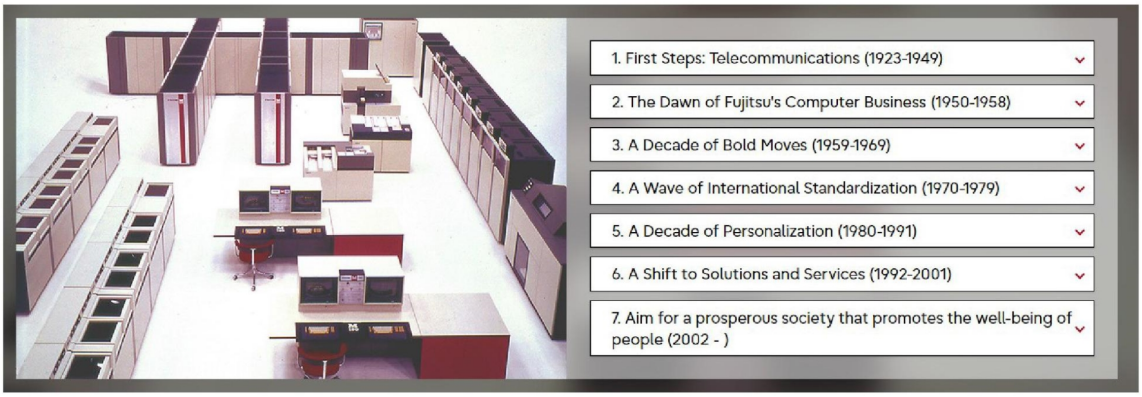

Figure 2. A long line of landmark achievements and product milestones for Fujitsu

3.1.2 Major Markets and Human Capital

Fujitsu is the leading Japanese information and communication technology (ICT) company, offering a full range of technology products, solutions, and services. Approximately 124,000 Fujitsu people support customers in more than 100 countries. Fujitsu use their experience and the power of ICT to shape the future of society with their customers. Fujitsu (TSE: 6702) reported consolidated revenues of 3.6 trillion yen (US $34 billion) for the fiscal year ended March 31, 2022.

3.1.3 Organisational Structure, including Business Units

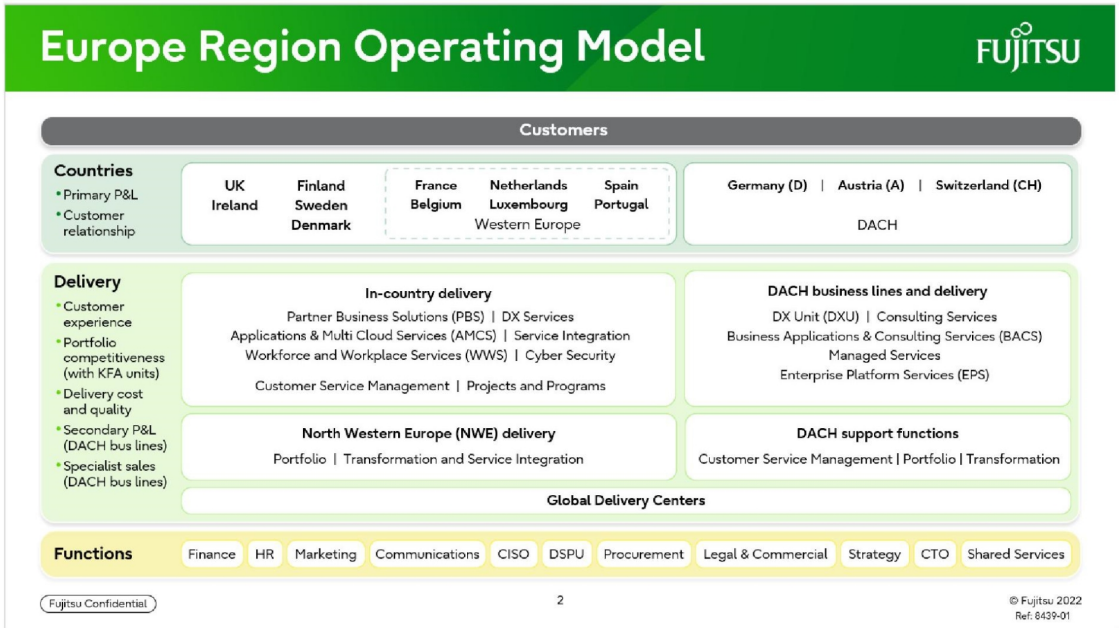

Figure 3. Fujitsu Europe Operating Model

POL00337569

3.1.4 Geographical Spread

As a global company, Fujitsu has offices in countries all around the world. Visit Fujitsu locations across the world: Fujitsu Global.

Figure 4. Fujitsu Global Locations

POL00337569

3.2 Overall Control Components

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

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

Fujitsu 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.

3.2.1 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.

3.2.2 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, which is understood by all employees of the organisation. All employees are required to maintain ongoing compliance training. Compliance checks are undertaken to help ensure that employees understand and comply with the Fujitsu Way.

3.2.3 Business Lines and Functions

The Business Lines and Functions that provide services or support the delivery of service to POL are as follows (as referenced on the Europe Region Operating Model):

- In-country delivery
    - Partner business Solutions (PBS) | DX Services
    - Applications & Multi Cloud Services (AMCS) | Service Integration
    - Workforce and Workplace Service (WWS) | Cyber Security
    - Customer Service Management | Projects and Programs
- North Western Europe (NWE) delivery

POL00337569

- Global Delivery Centres
- Functions
    - Finance
    - HR
    - Marketing
    - Communications
    - CISO
    - DSPU
    - Procurement
    - Legal & commercial
    - Strategy
    - CTO
- Shared Services

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.

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.

3.3 Control Activities

3.3.1 Governance and Oversight of Control Activities

Fujitsu has established the Risk Management Committee (RMC) as the body responsible to the Fujitsu Europe Board to promote risk management in accordance with the Fujitsu Way.

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. In addition, Fujitsu has a systematic approach to policy and process with a set of Master Policies approved by the RMC and sub-policies and processes determined by the relevant regional functions underneath. The framework, known as the Europe Business Management System (EBMS) is managed by Fujitsu's Governance and Assurance teams and comprises a set of mandatory Master Policies and Business

POL00337569

Processes. The Europe Master Policies cover the following under each of which is a set of specific business processes owned by Senior Management:

- Business Strategy Master Policy
- Compliance Master Policy
- Corporate Information Technology and Voice Master Policy
- Data Protection Master Policy
- Delegation of Authority Master Policy
- Europe Environmental Master Policy
- Europe Marketing Master Policy
- Europe Responsible Business Master Policy
- Finance Master Policy
- Occupational Health and Safety Master Policy
- Offerings Master Policy
- Procurement Master Policy
- Project and Program Management Master Policy
- Quality Master Policy
- Security Master Policy
- Service Delivery Management Master Policy
- Tax Master Policy
- Treasury Master Policy

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 an 'Exemption' from the Exemption Advisory Board where the Exemption Advisory Board authorises that local departure from the EBMS.

Human Resources

3.3.1.1 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.

3.3.1.2 Performance Management

Fujitsu has industry acknowledged good practice embedded in its approach to performance management.

POL00337569

Fujitsu call their approach Zinzai Career and Performance Management 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, Talent and Learning, 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 Zinzai Career and Performance Management IT recording system. Fujitsu's regional CEO is personally involved in filming communications and training material for all employees.

3.3.2 Information and Communication

Fujitsu UK and Ireland Business Lines and Functions have Europe 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:

- Virtual Road Shows.
- Virtual Staff Briefings.
- Virtual Team Meetings.
- Leadership and Management Cascades via Microsoft Teams.

Fujitsu also seeks the views of employees via representative groups and employee surveys 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.

POL00337569

3.3.3 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.

EBMS audits by various Fujitsu Subject Matter Expert (SME) 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.

3.3.4 Risk Assessment

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

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.

3.3.5 COVID-19 Global Pandemic

Fujitsu personnel have the technical capabilities and resource capacity to continue their relevant operations and services remotely. Service delivery includes the ability to perform processes, procedures, and controls related to Fujitsu's IT Infrastructure Services.

POL00337569

3.3.6 Description of Services provided

The Services that Fujitsu are contracted to provide are contractually referred to as HNG-X. HNG-X was a project that replaced the Horizon message-based branch network with the Horizon on-line branch service, also referred to by Post Office as Horizon Online and rolled out in 2010. The HNG-X Counter Business Application was later adapted to run on Windows operating systems other than NT4, providing all of the functionality of the HNG-X Counter Business Application. This adaptation is known as HNG-A.

In relation to the scope of Fujitsu services and assurance provided by this ISAE 3402 report for the examination throughout the period 1 April 2022 to 31 December 2022, noted below are the Fujitsu IT infrastructure services supporting POL's HNG-X application and the changes to the IT environment during the review period.

- The weekly incident reporting had been cancelled by POL in November 2021 but reinstated since October 2022. This has not impacted the fundamental end-to-end processes and controls in scope.
- As notified to POL, as of January 2022, McAfee Intrusion Detection system sensors have reached their end-of-life service. Signatures are still able to be downloaded but the vendor could change this at their entire discretion. A project to implement a supported solution has been commissioned by POL.
- As of July 2022, the test management tool changed from Quality Centre to Zephyr.

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.

Physical and Environmental Controls

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

#	Control
1.1	**Data centre access:** Data centre specific physical access security policies and procedures to control access to the data centre and other sensitive areas, including computer equipment and storage media, are implemented 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.

POL00337569

#	Control
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 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.

POL00337569

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)**.

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.

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 DC Support team) at the end of each day.

Persons issuing visitor access cards (reception/site security/DC Support 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.

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)**.

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, handheld 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.

POL00337569

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, ISS engineers) in the Phase I buildings within the data centre location, with repeater heads located in the Security office and the data centre support team's laptops. The BMS automatically alerts all three stations, if abnormal environmental conditions occur.

The ISS engineers and Security teams monitor the BMS system 24 hours a day, seven days a week; the DC Support team monitor the BMS Mon – Fri (08:00 – 17:00), 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.

Backup

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

#	Control
3.1	**Backup Definition:** The Backup High Level Design documents define the backup and recovery requirements for each platform.
3.2	**Backup Toolset:** Backups are performed either using NetBackup or RMAN (automated tools) for each platform.
3.3	**Backups are written to a secondary location:** Backups performed are written to a separate disk array and are 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 SMC 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. 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.

POL00337569

Note that in some circumstances, the recovery may by design be affected 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.

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 knowledge base) system to identify the appropriate team to respond to the backup failure and pass a Triole for Service (TfsNOW) call to their call stack with a voice prompt. Corrective action that is required beyond a simple rerun via the batch scheduler is planned TfsNOW 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**).

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 TfsNOW 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 ETERNUS CSHE.

Job Scheduling

4. ***Control Objective 4: Controls provide reasonable assurance that batch job 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.

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.

POL00337569

The platform architect will outline the required jobs needed for that platform as part of the High-Level Design (HLD) document. Changes to the required jobs would go to LST where the TWS schedule would be checked against the HLD by the test team. The Unix team then implements the changes. SMC 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 TfsNOW 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 Team (**4.1**). If changes are required to the job schedule, it will follow the standard TfsNOW process described in Control Objective 8.

Availability and Capacity Management

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

#	Control
5.1	**HNG-X 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.
5.2	**HNG-X 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.
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).

HNG-X Availability and Capacity 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. This includes the capture of availability information for the in scope platforms via the IBM Tivoli Monitoring (ITM) tool (**5.1**).

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.

POL00337569

Tool	Scope
Tivoli Provisioning Manager (TPM)	• Data Centre software provisioning.
Tivoli Endpoint Manager (TEM)	• Reference data delivery to 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.

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 operating system and application.

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 TfsNOW toolset and where appropriate Knowledge Base (KB) fixes, incidents or major incidents are applied.

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 POL Service Management Team (**5.3**).

POL00337569

Incident Management

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

#	Control
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).
6.1	**Incident policies and procedures:** Fujitsu has documented policies and procedures for managing incidents impacting the in scope applications which are available via SharePoint 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 weekly basis, the Fujitsu MAC Team reviews the number and severity of outstanding incidents in TfsNOW.
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.

Incident Management Process

Fujitsu Post Office Account (POA) applies its own implementation of Fujitsu's Corporate Incident management process as agreed with POL (**6.1**). It has documented procedures for managing incidents impacting the in scope applications which are available via the POA's SharePoint site 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 IT Digital Service Desk Team acts as the primary service desk function of Post Office Limited (user entity).

Fujitsu has defined an incident as "any perceived abnormal or undesirable occurrence relating to the Services" based on its contractual agreement with POL.

POL staff, e.g., Subpostmasters, either raise incidents with POL IT Digital Service Desk or POL's Network Business Support Centre (NBSC) and, where relevant, they are passed via POL's IT Digital Service Desk on to the Fujitsu POA MAC or SMC desks. Fujitsu raised incidents are logged and managed using the TfsNOW ticketing tool for incident management. The POL IT Digital Service Desk raise incident tickets in POL's ServiceNow tool which feed via an HDI link into Fujitsu's TfsNOW. Feedback and responses on the POL IT Digital Service Desk raised incidents can be sent back to POL's ServiceNow over the HDI link.

Fujitsu POA incidents raised by the MAC/SMC teams are logged in Fujitsu's TfsNOW tool which are linked to POL's ServiceNow tool, as required. Fujitsu POA incidents raised that are for external third-party suppliers to POL, are picked up by POL IT Digital Service Desk for them to manage the POL suppliers.

POL00337569

On a weekly basis, the Fujitsu MAC team reviews the number and severity of outstanding incidents within TfsNOW. 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, the POL IT Digital Service Desk, can transfer incidents from POL's ServiceNow tool into TfsNOW. A Contact is defined as TfsNOW incident transfer from POL IT Digital 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.
- POL IT Digital Service Desk.

POL00337569

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.
- Major Account Controller - 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 TfsNOW the MAC/SMC team assigns a priority level to the incident (POL IT Digital Service Desk assign incident priority before transfer to TfsNOW). If the call is classed as a Security Incident or Major Incident, it follows a different route detailed in pages 24-27.

Incidents in TfsNOW 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 Base (KB).

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

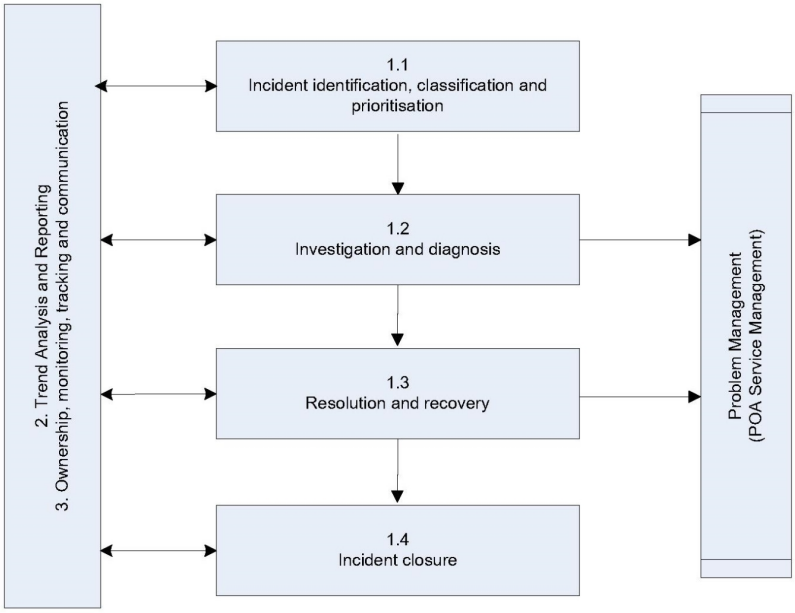

Figure 5. Incident Management Process

POL00337569

When a new TfsNOW incident is raised or received, the Knowledge Base is checked for KB 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 TfsNOW 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 are assigned a priority value (1 - 5) (**6.2**).

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 POL IT Digital Service Desk is advised of the status of the incident and the TfsNOW 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 TfsNOW, together with new information. The SDU also coordinates where Fujitsu sub-contract third parties are involved.

POL00337569

The SDU will produce a workaround or resolution for the incident. The SDU then either applies the workaround or resolution or passes it to the MAC/SMC to implement following appropriate testing. The parent incident record is the first incident for an issue in TfsNOW and is used as a tracking call for incidents with child 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 TfsNOW 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 POL IT Digital 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 (**6.3**). 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.

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/infrastructure failures or security issues.

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

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.

POL00337569

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, POL IT Digital Service Desk Team 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 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 Post Office Limited (and possibly their third suppliers).

The nature of the Major Incident determines which POA BU Service Team members 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.

POL00337569

A Draft Major Incident Report is distributed within 24hrs of resolution of Major Incident (**6.4**). 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 TfsNOWs.
- 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 arrange the conference calls, hold the formal closure review and produce the Major Incidents reports.

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 can be 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 Security and Fujitsu Central Security teams. In the case of Data Centre incidents, POA Security also informs the Data Centre Manager if this has not already been done.

POL00337569

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. POA SecOps team will work with POL Security Teams, as required.

When an investigation is closed, POA SecOps seek to ensure that details of the investigation have been recorded and can be made available for Root Cause Analysis, trending & lessons learned (**6.4**).

Security Incident Trends and Checks

POA SecOps carry out a monthly check of investigations and create a summary report of security incidents to the POL ISMF. This aims to inform POL of the security incidents raised for awareness and escalating any major incidents identified.

These security incidents are also reviewed by POA Senior Management at the monthly POA internal Information Security Management Reviews. Fujitsu Central Security team conducts trend analysis and check for weaknesses which may need to be raised at future POL Information Security Management Forums (ISMF).

Incident Reporting

The Fujitsu MAC/SMC Team reviews and reports the number and severity of all outstanding incidents in TfsNOW. A weekly meeting is held between POL and Fujitsu for the review (**6.5**). On November 2021, the weekly meeting has been cancelled by POL and reinstated since October 2022.

The Fujitsu MAC team reviews and reports the number and severity of all outstanding incidents in TfsNOW in a weekly internal report. All POL related incidents are reviewed weekly and chased via the TfsNOW incident management every 3 to 5 days. All outstanding incidents waiting for POL to progress have been added to the monthly SMR pack for review (**5.3**). Any incidents which require additional progression are chased via email into POL on an ad-hoc basis.

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 (**6.6**). Incidents are only logged in **TfsNOW** for alerts that trigger a status change, which then follow the incident management process described above.

Network Incident Management

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

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	**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).
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.

POL00337569

#	Control
7.2	**Network change management:** Network changes are managed using the standard Fujitsu TfsNOW 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 System Management Centre (SMC) 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.

Network Service Description

POL defines the network services it requires from Fujitsu in 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.

Provision of the Network Service

Fujitsu provides network services to POL using its Network teams. These teams provide technical support and implementation for the following products and platforms:

- The Post Office Account Network team based in UK (UK Networks Shared Services) and Pune 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 Gateway & Bluecoat Proxy SG).
- A centralised Network Toolset Specialist Services (NTSS) overviews and administers the network toolsets.

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

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

Network Change Management

Fujitsu follows the TfsNOW change management structure for all changes to network equipment as described below in Control Objective 8 for the review period (**7.2**).

Network Availability Monitoring

Fujitsu has its own dedicated SMC team to monitor the availability of Network Services to POL using TfsNOW 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 6 above (**7.4**).

POL00337569

Networks are monitored by POA SMC team for availability via the Spectrum and Netcool tools which send automated alerts (**7.3**). For these alerts, a corresponding incident ticket is raised by the SMC team for NTSS to resolve.

Network Service Monitoring

The Fujitsu Problem and Incident Management team report the central network availability against the agreed SLTs on a monthly basis to the POL Service Management Team (**5.3**).

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.
- Transit Networks.
- Wide Area Networks.

As shown in the diagram below. Note that branch networks is under Verizon's responsibility.

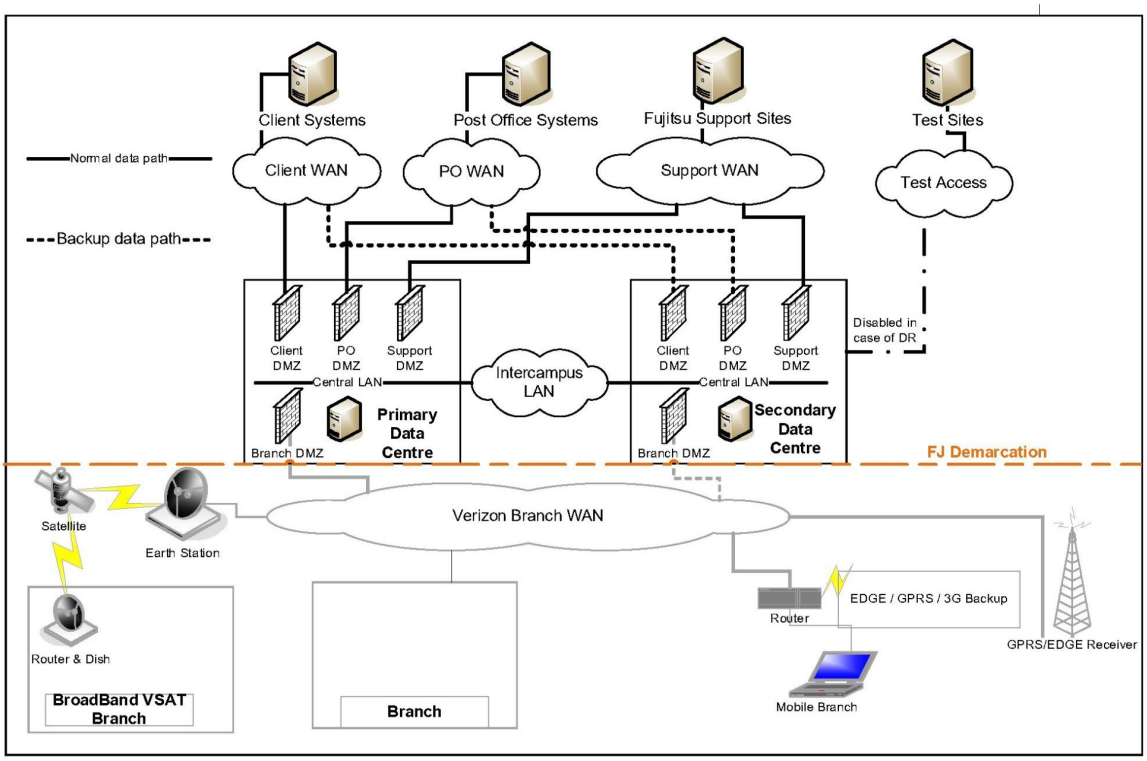

Figure 6. Network Design

Testing is provided through the standby data centre for Live System Test and Solution Validation and 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 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.

POL00337569

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 below illustrates how Network Domains fit within the Network tier model.

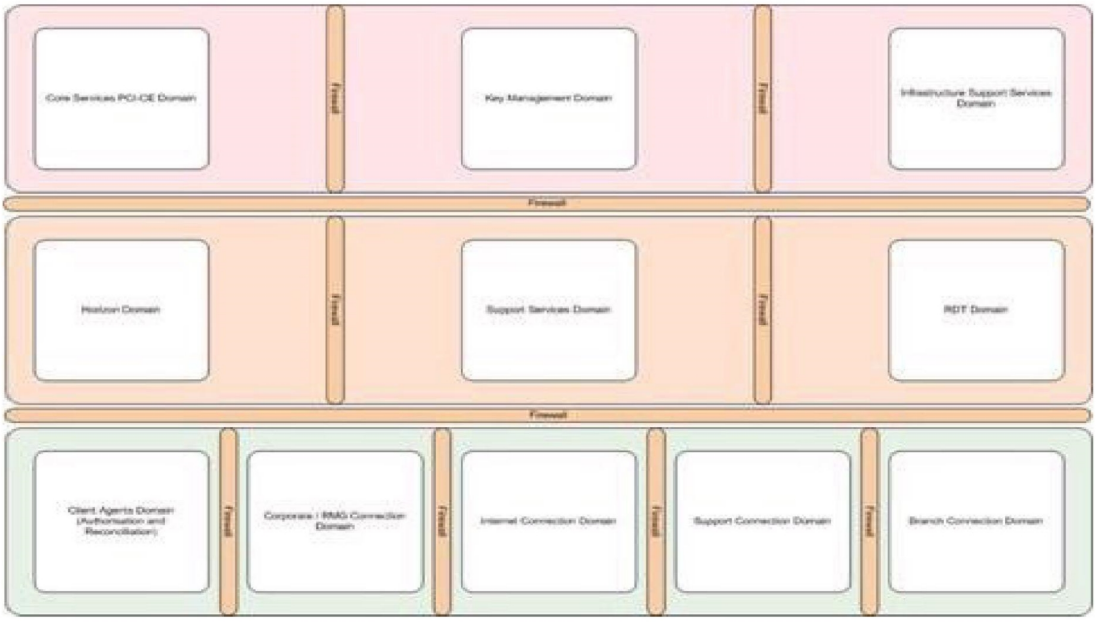

Figure 7. Network Tier

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.

Network Asset Management

Network Assets are managed through Cisco Prime 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.

POL00337569

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 TfsNOW 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 Change Owner, with the approval being documented in the TfsNOW toolset. Changes that cause major service interruption or are a significant risk must also be authorised by the Change Advisory Board (CAB), with approval being documented in the meeting minutes and within the TfsNOW change record.
8.3	**Emergency Changes:** A change deemed necessary in order to resume live service will be agreed, approved and documented on TfsNOW emergency change record. Updates are communicated to POL at an agreed timeframe dependent on the severity of the incident.

Types of Changes

All operational changes are raised via TfsNOW toolset and subject to the TfsNOW change process (**8.1**). Key change types that fall into scope for this process are listed below:

- Normal Change – Any change which is not classified as an emergency or standard change (e.g. large-scale change to the service or service infrastructure, catalogue service or administrative change of known low impact). This will include minor changes (minimum of 24 hrs prior to implementation) & significant changes (minimum 5 working days prior to implementation & in line with POL CAB).
- Standard Change – A standard change is a pre-defined and pre-approved change by POL Change Management following the initial standard change approval process, where authorisation is provided via CAB and changes added to the POL standard change catalogue. These are regular & predictable changes that have been proven to be successfully implemented a number of times with no history of unplanned impact.
- Emergency Change – Immediate action required in relation to a P1/P2 incident including changes that are required to prevent a major incident (MI). Where time doesn't allow a change to be raised & approval is granted on an MI Bridge, a retro emergency change would be logged retrospectively within 24 hours of the change taking place.

These changes include POL authorised project work with Fujitsu. Changes made by POL 3rd Party or POL Network Partners are supplied by POL and are then recorded in TfsNOW for visibility of these changes.

The change management TfsNOW operational change process uses the Fujitsu TfsNOW toolset to progress the change through control gates which are described below.

The TfsNOW toolsets are 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 TfsNOW 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 TfsNOW 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.

POL00337569

Once a change is ready to be implemented, it becomes subject to the TfsNOW change management 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 TfsNOW.

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).
- TfsNOW is used to record and authorise BAU changes also (Operational changes).
- TfsNOW systems record the assessment by other potentially impacted teams to determine risks associated with the change in their area (Operational Changes).
- TfsNOW systems contain a plan of the change (Operational Changes).
- The POL CAB's review helps to ensure (Operational Changes):
    - changes meet the governance requirements;
    - changes do not overlap with other changes;
    - that the change has considered any group or associated further risks and impacts by doing the change; and
    - the POL CAB follows the standard CAB process where it defines:
        - Attendees.
        - Sign off or rejection or associated actions.
        - Recording and issuing of minutes from the CAB.
        - Updating the TfsNOW toolsets with the CAB decision.
- The Change Manager is responsible for the following (Operational Changes):
    - Reviewing and ensuring process conformance.
- If the above are in place, the designated change owner approves the change within the TfsNOW system to proceed and implement the change (Operational Changes) (**8.2**). An approval note is added automatically in the notes of the change once the change owner approves the change.
- Output of the change is confirmed via the Post Implementation Review (PIR) task before the change is sent for closure.

In summary, TfsNOW 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 approved by the Change owner, are assessed 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.

Emergency Changes

Emergency changes are progressed if there is a service incident. This will be documented in a TfsNOW change record.

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. Any change deemed necessary in order to

POL00337569

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.

The TfsNOW change record will be sent to POL Change Management for approval as outlined above (**8.3**).

Project Changes

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 Governance:** 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 requirements are outlined in the Commercial Work Order (CWO) and if justified, within a (CSP) Customer Solution Proposal, (PSD) Project Solution Design documents or (FSR) Feasibility Study Reports, as applicable, that is stored in Dimensions 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 TfsNOW tool.

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**).

Project Changes for HNG-X

External requests for changes are raised by POL on a Request to Quote (RTQ) and provided electronically by Service Now to Business Change Management (ChM) and allocated to a Change Owner and converted into a Change Proposal (CP) by Fujitsu.

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

Once reviewed, CPs will be presented 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. For urgent CPs or those that meet certain criteria, CPs can be presented straight to the Change Control Board (CCB).

Once the PCCB has assessed and agreed the progression of a CP, it will be tabled for presentation to the CCB along with the associated Change Work Order (CWO). The CCB consists of the Account management team, with a recommendation from the PCCB as to whether the CCB should approve or reject it (**9.2**).

POL00337569

The CCB typically meets weekly. Change Owners are required to attend to be able to sponsor the change detailed in their CP/CWO. The CCB consists of members who represent the key functions within the Account to help ensure that if the CWO 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 to the required quality level.
- **Architects**
  - Be constrained within the overall architectural solution and is technically viable.
- **Quality and Compliance Management**
  - Not inhibit the Account in exploiting future business opportunities for the Account and its Customers.
  - Comply with applicable contractual obligations and legislative standards agreed with POL.

The Delivery Executive (or delegate) and a quorum of the CCB members 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 or agreement to progress to CWO are held in Dimensions (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 CWO will be submitted to the customer (electronically) and POL reviews the change and then once successfully approved (by both parties by electronically signing the CWO), the Programme team is advised, times codes and plan activities are set-up and work can commence.

Project Changes are allocated unique numbers and logged within a database (Dimensions) 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 for Contract Change Notifications (CCNs) and CWOs are documented in the relevant change history, as well as the artefacts being actioned to an approved state.

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.

POL00337569

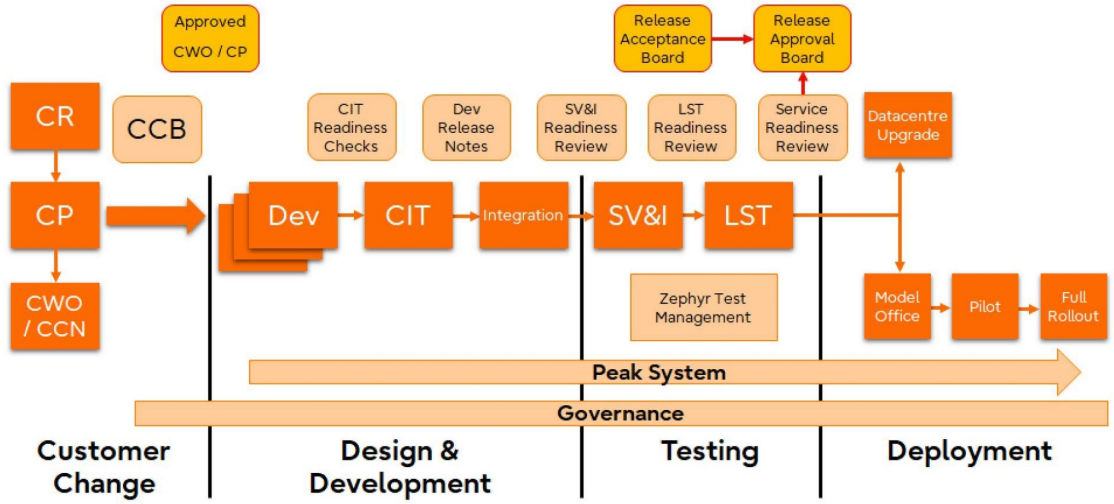

Figure 8. Project Lifecycle

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.

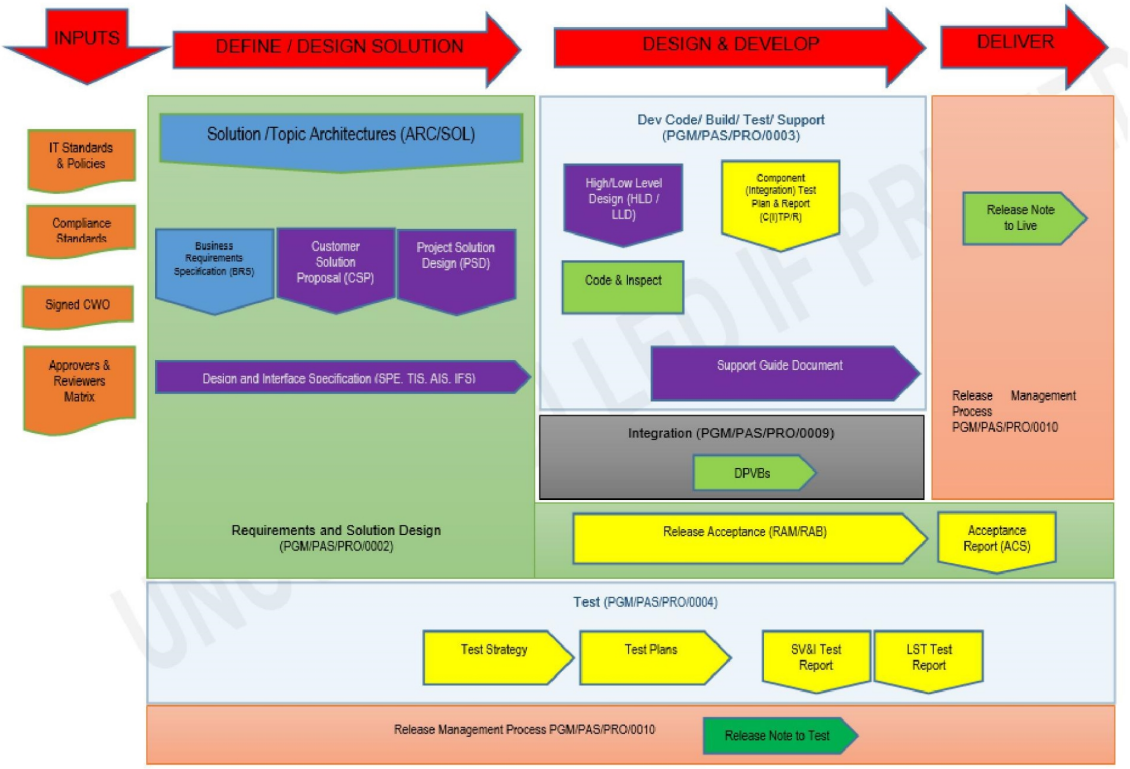

Figure 9. Design and Build Method

POL00337569

Definition

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

Requirements

Requirements are managed within Fujitsu by the Requirements manager.

POL defines a requirement baseline as a Business Requirements Specification (BRS) or as part of the Commercial Work Order (CWO). The BRS and/or CWO will contain the Acceptance Criteria.

Where applicable, a (CSP) Customer Solution Proposal, (PSD) Project Solution Design and (FSR) Feasibility Study Reports are written to show how these requirements will or can be implemented (**9.3**).

The CSP or PSD contains three key elements:

- The Work Packages that are built to deliver the project.
- The Monitoring Criteria for the project and stipulated service delivery requirements after go live.

The FSR describes the relevant alternatives to the proposed implementation including the relevant impact of each implementation.

Design

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

SDLC Methodology

HNGxDBM Design, Development and Build Method lifecycle was derived from the Fujitsu corporate Applications Design Methodology (ADM), Infrastructure Design Methodology (IDM) 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.

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

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

Code Build and Test

The Application Development Manager is responsible for the delivery of the code for the project or maintenance release. Code is developed and built in a segregated environment using appropriate source code repositories e.g. subversion for storage and then deployment from the Dimensions CM tool via Baselines containing checked in code content, and the management of changes associated with its delivery. Each project will have a Lead Developer or SME who will work with the Development manager to assign the packages of work and allocate these to developers. The Development manager will also produce their own project plan to track progress and development of code, its testing and any documentation that needs producing or updating. Code will then be produced within the context of this project plan.

A generic code review template or an automated code review tool, Crucible, is used to review the code and using this it is then peer reviewed by the Lead Developer or Subject Matter Expert until any outstanding issues are resolved. The resulting review document is stored in SharePoint or the Crucible tool itself.

POL00337569

Individual developers are responsible for producing unit tests which are then peer reviewed by a developer or subject matter expert where possible (in rare cases this maybe the same person). The developer will develop and execute the unit test, depending on the development methodology used (Waterfall/Agile/Blended) the unit test is then stored in Jira/SharePoint/Dimensions. The subsequent code (if applicable) is then tested on the Component Integration Test rig (CIT) for a few cycles until all defects raised are fixed and re-tested. A build of code is then produced at the end of this and uploaded into Dimensions to produce a Product Version Baseline for the application or its subcomponents.

Not all applications can be tested in CIT due to the rig's limitation or offshore security restrictions as this is not a formal test environment, as a result some applications can only be tested on the SVI/LST test environments.

Integration and Test

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

- Solution Validation and Integration (SV&I):
  - Testing against Requirements - Functional and Non-Functional covering business and infrastructure and based on testing the complete integrated solution.
  - Has End-to-End capability for testing with 3rd parties e.g., Merchant Acquirer.
- Live System Test (LST):
  - Final pre-production proving and release deployment validation.

The development-written test automation framework (documented in DEV/APP/SPG/1208) 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 (1 April 2022 to 30 June 2022) as the test management tool and Peaks 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.

As of July 2022, Quality Centre was replaced by Zephyr as the test management tool, however, it does not interface with Peaks.

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

- Progressive, incremental development, testing and acceptance.

Each test cycle is subject to entry criteria acceptance. Quality Centre or Zephyr 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.

SV&I Testing Process

Test Analysis is based on requirements and high level designs. Test cases are documented in Quality Centre (QC) or Zephyr 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 or Zephyr and defects are recorded within Peak.

POL00337569

Daily and Weekly reports are produced using QC or Zephyr to produce statistics e.g., test coverage. After the last cycle of testing (pre LST) a report is produced covering the full release.

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.

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/CWO (**9.6**).

The results of testing are summarised in the Release Acceptance Meeting (RAM) presentation.

This is then reviewed and discussed internally to assess the status of Acceptance, including Acceptance Incidents. An acceptance incident is where the acceptance criteria has been tested and is either not met or partially met.

The Release Acceptance Meeting (RAM) held jointly with POL will then review the results of Testing and agree on how to progress the Acceptance Incidents and overall whether the project as stand-alone entity is ready to be implemented.

Subsequent to the Release Acceptance Meeting (RAM) is the Release Authorisation Board (RAB) where POL are asked to confirm that everything is ready to enact deployment plans for the Release.

The Release Acceptance Meeting (RAM) and Release Authorisation Board (RAB) meetings are typically held as one joint meeting.

The RAB considers approving deployment based on whether:

- The Release has passed the Release Acceptance Meeting (RAM).
- 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., Subpostmasters, POL's partners (such as Verizon, Accenture, DXC) and Fujitsu's third parties

The decisions around Acceptance (RAM) and Authorisation to deploy (RAB) are documented in the minutes of the RAM/RAB meeting and held in Dimensions in the form of the Release Acceptance Report (ACS document).

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

Deploy and Support

Release management is based around the use of three documentation tools, Dimensions, Peak and TfsNOW change management process, and three delivery tools, Dimensions and Tivoli Provisioning

POL00337569

Manager (TPM) and BigFix End Point Manager (**9.5**). TPM is used for operating system deployments whereas BigFix is used for application software deployments. 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 Product Version Baseline (PVB) to group software at a component level 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 creates a Deployable Product Version Baseline (DPVB) from the PVB and 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, the DPVB is made available to Release Management. Release Management control the deployment of the packaged software (DPVBs) to SV&I for project functional testing with POL and other third parties, 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 System Test) and Live by using a combination of Release Notes generated in Peak and TfsNOW for change control.

The Release note (RN) will be passed to Software Configuration Management (SCM) to move the software onto a staging server and then passed to the Deployment teams in Ireland (Unix and NT) to upload to the deployment servers (TPM and TEM). TfsNOW is used to authorise deployment to the servers in the Data Centres. SCM is the only team with access rights to move software from Dimensions to staging server and the implementation teams are the only teams with access rights to upload the software to the deployment servers and then deploy to the Data Centres (**9.5**).

The approvals to move the change through the various stages (both Fujitsu and POL approvals) are logged in TfsNOW tickets and are typically copies of emails pasted into the TfsNOW ticket and does not use formal workflow-based sign offs (**9.6**). The authority and ability to move the change into production is given to the deployment team when Release Management assigns the TfsNOW and the release note ticket to the deployment team.

Once the deployment is complete, the Release Note Peak ticket and the TfsNOW Change ticket will be closed by the Change Manager.

Post Implementation

Monitoring and Review

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

Weekly Project report to Post Office Project Managers

A collated reporting pack issued to the Post Office Project Managers showing the delivery RAG (Red, Amber, and Green) status, Executive summary, key milestones, dependencies, risks and issues for each of the Project deliverables and/or Releases, as applicable. In addition, financial spend is also reported on, with the report offering a view of Project Actuals and Forecast to completion.

Steering Committee Reporting (with Post Office)

For key programmes, presentation of a collated reporting pack to Post Office showing the RAG status, Executive summary, key milestones, dependencies risks and issues for each of the key Releases that are currently in Delivery. The Steering Committee consists of key stakeholders from Fujitsu, POL and POL's third parties.

Internal Weekly POA Transformation Steering Board

POL00337569

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.

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 TfsNOW 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.

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 which is designed and managed by POL.

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 reviews user access to systems on a monthly 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.

Policies and Procedures

Fujitsu employees adhere to the over-arching Europe Security Policy Manual (ESMP001/A) 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

POL00337569

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.

The Community Information Security Policy (CISP), SVM/SEC/POL/0005, is a contract reference document which provides guidance from POL regarding 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 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 (**10.1**). The ARC/SEC/ARC/0003 is reviewed in line with customer requested changes in the contract.

General System Security Settings

Each Operating System and Database in use by Fujitsu to support HNG-X (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**).

The HLDs and LLDs are established based on the security hardening guidelines provided from the manufacturers of their products in line with industry standards.

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. Any changes to configurations must be reviewed, risk assessed and approved by POL prior to the 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

POL00337569

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.

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.

There is an 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.

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.

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 and application 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 turn 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 TfsNOW records 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.

POL00337569

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.

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).

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.

Password Settings

Password configuration requirements are defined in Fujitsu Systems Access and Passwords (EBMS Security Toolkit) supplemented by the POA password policy rules defined within the POA Privileged Account Policy, and/or the relevant baselines for infrastructure components. Any exceptions are recorded and authorised by POA SecOps Passwords on relevant platforms and directory servers are stored in a one-way encrypted form and are protected against substitution or dictionary attack.

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 (SecOps).

New Joiners/Transfers

Detailed below are the steps that must be followed when an individual joins Fujitsu and POA, or joins the POA from another area within Fujitsu which are shown in the Figure 10 below (**10.4**).

POL00337569

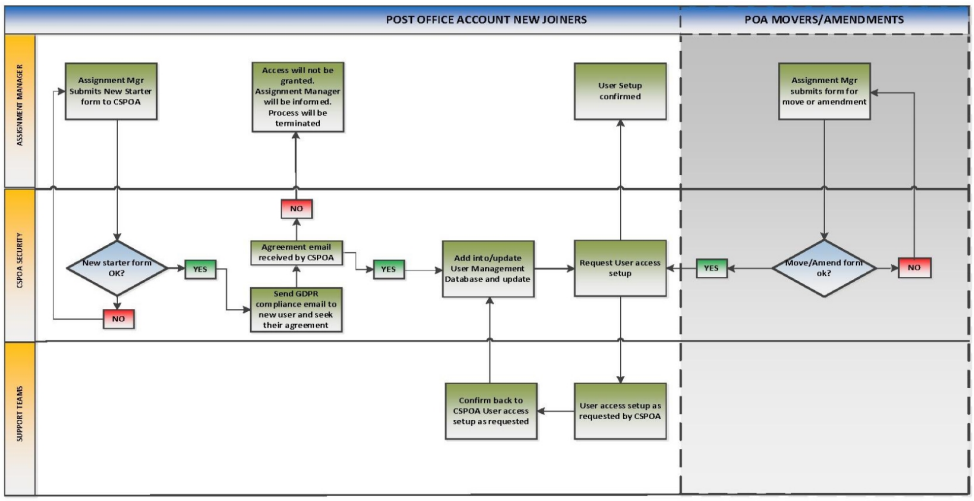

Figure 10. User System Access Process Flow for New Joiners, Movers, Transfers and Access Amendments

The Assignment Manager will complete the latest New User Access form from the POA Security Operations (SecOps) with all required information. The completed form is returned to CSPOA via email.

POA SecOps will check the form to ensure it has been completed correctly, and in line with Fujitsu Security Policy. Once both the correct New User Access Form and the GDPR agreement have been received, POA SecOps will arrange all relevant access to be set up for the user by e-mailing the relevant system owners (e.g., Windows NT Team, Unix Team, etc.) and requesting user access to be set up. A TfSNOW call will be raised for back-end system requirements and a copy of the completed request form will be attached to the TfSNOW call, where required.

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

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**).

Assignment managers must submit a Leaver form as soon as possible prior to user leaving Fujitsu and/or the POA. The Assignment Manager must complete the latest Leaver Form from the POA SecOps Portal with all information required and return to CSPOA via email.

POA SecOps check the form is completed correctly, and in line with Fujitsu Security Policy. POA SecOps notify the relevant system owners (e.g. Windows NT Team, Unix Team, etc.) via email, and where backend system access is held, a TfSNOW call will be raised and progressed to the system owners requesting revocation of access.

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

User Access Review

The POA User Management and CSPOA Teams undertake a monthly review of the access granted to individuals and its continued appropriateness (**10.6**). POA User Management Team produce details of all users contained in the register and their access levels and communicate these via email to the relevant

POL00337569

Line/Assignment Managers. Line/Assignment Managers review the listing and consider whether any users require their access to be amended by providing the details to POA User Management Team within 15 working days of receipt of the original e-mail. CSPOA performs an audit of access rights and roles with each functional area; the results of which is presented at the monthly Team Access Review meeting with POA User Management.

A more detailed access verification check is conducted monthly, specifically for Production Privileged Access. CSPOA produce details of all users with Privileged Access and email these to the relevant Line/Assignment Managers. As part of this monthly verification process, segregation of duties is also checked to ensure there are no segregation of duties issues e.g., due to changes to a user's role or responsibilities.

Information Security Management Forum

The Information Security Management Forum (ISMF), as organised by POL, is a formalised monthly forum where Post Office and Fujitsu Security operations discuss governance matters and issues/risks 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 etc. as agreed between Fujitsu and Post Office.

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

- Monthly summary
- Security Incidents raised in reporting period
- Operational security
- Security Event Analysis (in reporting period)
- Systems end of life status
- Privileged user access accounts
- Other matters.

User Authentication Technologies

A separate Active Directory (AD) forest is deployed for each of the environments: Systems Validation & Integration (SV&I); Live System Test (LST); and Production. The SV&I, LST (collectively described as Test) and Production environments are deployed on common infrastructure but are logically separated by virtual LANs, virtualised services, access controls and firewalls.

Fujitsu employees have a corporate laptop that includes VPN software and cryptographic keys. The laptop permits access to the Fujitsu corporate network and authenticates the user with a corporate user ID, password and VPN key tuple.

Each support user has an HNG-X AD user ID and password. The user is issued an iKey hardware token by POA Security Operations. The token contains a client certificate used to identify and authenticate the user to the HNG-X Production or Test environment. The client certificates are issued by the HNG-X Production or Test certification authority (CA). The combination of local physical access or remote VPN access, user ID, password and a multi-factor authentication (MFA) token provides the support user access to the Windows Terminal Server within the HNG-X environment (**10.7**).

The Windows Terminal Servers provide a virtual desktop environment and support a limited number of applications the user may execute. The applications may themselves require further authentication. The

POL00337569

support user's role (defined by AD groups and access permissions) restricts the user's access to platforms and applications. The Windows Terminal Servers do not run core business applications; they only provide the ability to connect the support user to other servers.

User logins to Linux servers are unprivileged. To gain additional privileges, the user must, if authorised, use the Sudo command. AD incorporates the permitted Sudo privileges and distributes them via the System Security Services Daemon (SSSD) process. Sudo use is logged.

TACACS supports the authentication, authorisation and accounting for support access to network (primarily Cisco) devices. TACACS is not integrated with AD so user accounts are stored locally within the TACACS servers. A designated team manages the network equipment and in order to access a network device, a user must have already authenticated to a Windows Terminal Server as described above. The network devices are further restricted to accept interactive support connections from the terminal and network management servers. TACACS also limits the commands users can run on the network device according to their role.

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 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 Fujitsu managed 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.

Patch Management

Fujitsu's POA SecOps 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 a secured SharePoint site only accessible by authorised individuals.

The Deployment Spreadsheet is reviewed by the SDTs and Application Support teams on a regular basis (minimum monthly or as required for critical vulnerabilities); 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 Patch Approval Board (PAB (**11.1**)).

The PAB consists of members of the Applications and Multi Cloud Services division, Application Delivery and Support 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).

POL00337569

System Administrators & Database Administrators

System or Database Administrator user management controls are only implemented once appropriate approval has been obtained for access to various sites and systems. The user management database utilised by the POA SecOps holds details of all the support teams and the system access the team resources have (**11.2** and **11.3**). This database 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 SecOps provides a monthly report for privileged users and presents at the monthly ISMF with POL.

Throughout Fujitsu managed 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 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.

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 to POA SecOps who monitor the console.

On a monthly basis, the POA SecOps reviews alerts that have been raised from Tripwire. Monthly reports are produced detailing alert statuses and a root cause analysis for each alert. 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.

POL00337569

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 Fujitsu Security Delivery team.
12.2	**Configuration Changes:** Changes to firewall configuration follow the standard Fujitsu TfsNOW 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 Fujitsu ATC Team.

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, proxy servers and Stateful Inspection Firewalls, ACLs, AES Encryption and physical separation.

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.

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 and PAT technologies.

POL00337569

Access to set-up and configure firewalls is restricted to appropriate Fujitsu Security Delivery personnel (**12.1**). TfsNOW 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 TfsNOW 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.

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 monthly.

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 TfsNOWs. 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 month to keep it up to date.

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.

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.

POL00337569

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 SecOps.
4. If the cleaning is not successful, an alert event is logged and an incident is raised in TfsNOW, with alerts going through to SMC to 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 KBs 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.

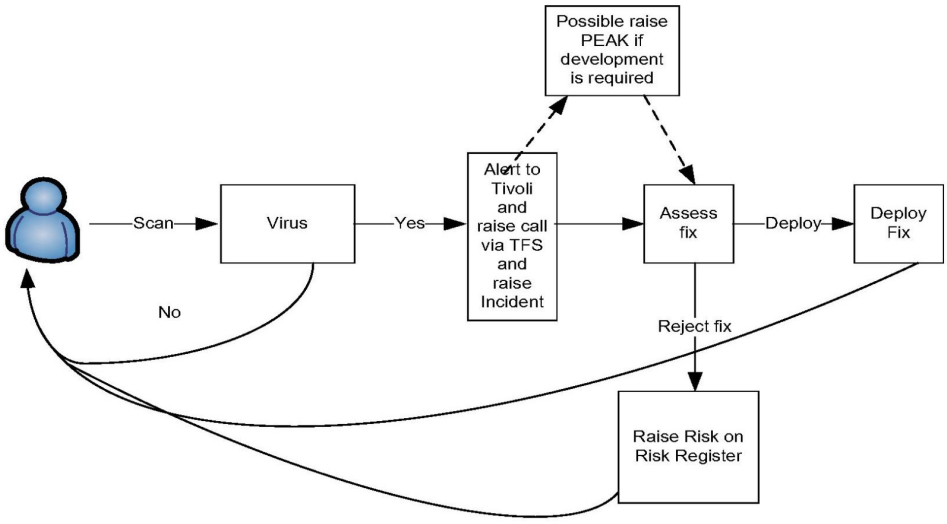

Figure 11. AV Scanning Process

Intrusion Detection System (IDS)

Network-based intrusion detection is deployed as part of the HNG-X Data Centre and infrastructure. This provides notification of an attempted compromise of systems within the Data Centre, through malicious activity or malicious code (**12.4**).

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 (DEV/INF/LLD/0051). 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.

POL00337569

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 HIDS 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 intrusion detection system ensures that any false positives and false negatives are reduced to a minimum. Additionally, intrusion attempts are investigated by the ATC (Advanced Threat Centre) Team and alerts raised as a result of failed attempts to logon or to access data with invalid permissions. The Incident Management Procedure and Security Incident Management Work Instruction documents are updated accordingly.

Distributed denial of service (DDOS) attacks are considered to be a low risk for the HNG-X system as it operates as a closed network system and therefore the possibilities of attack from the Internet (the most significant threat source), although present, are very low. However, to ensure that such attacks do not originate from within the HNG-X 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 HNG-X 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.

As notified to POL, as of January 2022, McAfee Intrusion Detection system sensors have reached their end-of-life service. Signatures are still able to be downloaded but the vendor could change this at their entire discretion. A project to implement a supported solution has been commissioned by POL.

POL00337569

3.4 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 delivery of particular services relating to the ISAE 3402 controls. These additional third parties are not considered subservice organisations for the purposes of ISAE 3402 audit opinion since Fujitsu do not outsource any controls and each third party POL agent works independent of each other with separate contractual outsourcing arrangements with POL.

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.	DXC Verizon	As part of the Tower Model service delivery model, DXC manages the End User Computing (EUC) Tower unit. Fujitsu is not responsible for EUC support but can be called upon to support incident investigation if required. POL's IT Digital Service Desk hosts the front desk operations for POL's branches and head office users and has taken ownership for 1st level support calls. Verizon are responsible for hosting POL's network.
8.1 Change management The TfsNOW 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.	POL DXC Verizon	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 other POL agents and third parties.

POL00337569

3.5 Complementary User Entity Controls

In designing its system, Fujitsu has expected 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 POL 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.

- **Physical Access**

  Controls should be established to:

  - Appropriately restrict access to terminals, workstations, and other computing equipment at POL sites or other locations (e.g. staff homes or POL 3rd party suppliers), 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.

- **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.
  - Ensure that POL agents with TIS interfaces provide the correct requirements and controls for secure connectivity.

POL00337569

- **Change Control**

  Controls should be established to:

  - Ensure that application changes follow a formal change process and are approved by relevant parties involved for the change (e.g. POL's clients, other third party suppliers, etc.) on a timely basis.
  - 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.

- **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 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 monthly meeting with Fujitsu are appropriate.

- **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.
  - 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.
  - POL and /or other vendors provide minimum data sets for incident reporting.

POL00337569

- **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.
  - Identify and prioritise data and its respective criticality as required by the applicable legislative and industry standards which POL are subject to comply with.
  - Ensure that where POL or its other suppliers administer POL infrastructure, the application's developers have appropriate access.
  - Ensure that POL agents with TIS interfaces provide the correct requirements and controls for secure connectivity via API's.

- **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.
  - Ensure that 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.
  - Ensure with Fujitsu that adequate funding and resources are in place to enable design and testing to meet modern best practice.

- **Business Change**

  Controls should be established to:

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

- **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 Meeting (RAM) and Release Authorisation Board (RAB) meetings.
  - Identify and document all joint policies, processes, work instructions and guidelines that are required between relevant POL partners and third parties that are interfaced with each other as part of providing the POL solution.

POL00337569

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.

POL00337569

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

4.1 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.

4.2 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 HNG-X application. 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.

POL00337569

4.2.1 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 policies outline the physical access security protocols for controlling access to the data centre, including other sensitive areas, and 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 virtually that access doors are equipped with a key-card system to restrict individual access to specific data processing areas. Inquired with management to determine that users were granted access levels in order to restrict individual access to specific data processing areas based on the access level assigned. Obtained and inspected the system generated data centre user listing to determine the population of new users granted access to the data centre.	No deviations noted. *Based on inspection of the data centre system access listing, we determined there were no new users that were granted access to the Fujitsu data centre in the review period and therefore no operation of the control within the review period.*
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 virtually that CCTV video cameras are placed at key locations around the data centre to monitor user activity. Observed virtually that the CCTV video footage is monitored by the security staff at the data centre.	No deviations noted.

POL00337569

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.	Virtually 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 observed that the data centre can only be accessed through a central point (security desk), which has security guards 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 virtually 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 virtually from inspection of the visitor log that visitors are escorted by a Fujitsu staff at approved dates and times per the visitor logbook and time 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 to determine whether these were reviewed for suspicious activity and proactively followed up. Please refer to Control Objective 6 for our test procedures performed for the incident management process.	No deviations noted. *Based on inspection of the failed login alerts and list of incidents logged, we determined there were no unauthorised failed logins that were identified that required access to the data centre to be removed.*
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 centre 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.

POL00337569

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.	Inquired of management to determine that access to the data centre is removed on the users' HR leave date. Obtained the system generated HR leavers list and determined the complete and accurate population of leavers. We observed that there were no leavers with access to the data centre in the review period.	No deviations noted. *Based on inspection of the data centre system access listing and revocation requests logged, we determined there were no identified leavers from the data centre that required their access to the data centre to be removed and therefore no operation of the control within the review period.*

POL00337569

4.2.2 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 virtually 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 fireproof wall) 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 (for 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 to determine 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 virtually 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 virtually 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.

POL00337569

4.2.3 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 those platforms.	No deviations noted.
3.2 Backup Toolset Backups are performed either using NetBackup or RMAN (automated tools) for each platform.	Obtained the PHIL listing and selected a sample of platforms. Inspected the backup tool configuration and backup logs to determine whether NetBackup or RMAN were installed on those platforms to perform automated backups and backups are completed successfully.	No deviations noted.
3.3 Backups are Written to a Secondary Location Backups performed are written to a separate disk array and are written to a disk array at the disaster recovery site.	Obtained the PHIL listing and selected a sample of platforms. Inspected the backup tool configuration for the platforms to determine whether backups performed are written to a separate disk array and are 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 TfsNOW ticket was logged and resolved appropriately by the SMC Team. Please refer to control 4.2 for the TWS configuration for detecting job failures and control objective 6 for the testing procedures over incidents.	No deviations noted.

POL00337569

4.2.4 Control Objective 4

Controls Specified by Fujitsu	*Testing Performed*	*Results of Tests*
Control Objective 4: Controls provide reasonable assurance that batch job 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 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 the batch jobs for HNG-X infrastructure to determine whether it is configured to raise an alert if a batch job fails and to then pass this alert to the TBSM tool. Please refer to control 6.6 for our testing procedures over the handling of alerts.	No deviations noted.

POL00337569

4.2.5 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 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 platform to determine whether they are configured to monitor the CPU, memory, disk utilisation and the capacity of internal services on the servers. Inspected a system generated listing of users with administrator access to the tools used to monitor the environment and ascertained that it is restricted to authorised users based on their job responsibilities. Please refer to control 6.6 for our testing procedures over the handling of alerts.	No deviations noted.
5.2 HNG-X 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 to determine whether: • These showed that the tools monitor and manage availability and capacity of servers; and • Thresholds were defined which, if breached, would send alerts to TBSM for SMC review. Please refer to control 6.6 for our testing procedures over the handling of alerts. Inspected a system generated listing of users with access to administer Netcool Omnibus and ascertained that it is restricted to authorised users based on their job responsibilities.	No deviations noted.

POL00337569

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 and corresponding communications between Fujitsu and POL to determine whether the: • Analysis was provided to POL to review its agreed SLTs; and • Book contained details of capacity, availability and incident management performance.	No deviations noted.

POL00337569

4.2.6 Control Objective 6

Controls Specified by Fujitsu	*Testing Performed*	*Results of Tests*
Control Objective 6: Controls provide reasonable assurance that significant incidents are adequately reported, tracked, monitored through resolution and resolved timely.		
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).	Refer to control 5.3 within Control Objective 5 for the testing procedures performed.	No deviations noted.
6.1 Incident Policies and Procedures Fujitsu has documented policies and procedures for managing incidents impacting the in scope applications which are available via SharePoint 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 outline the incident management process and were made available to relevant Fujitsu employees via SharePoint.	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, TfsNOW. 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, TfsNOW, inspected the incident tickets to determine whether they had been escalated and monitored for timely resolution, as per the assigned priority.	No deviations noted.

POL00337569

Controls Specified by Fujitsu	Testing Performed	Results of Tests
Control Objective 6: Controls provide reasonable assurance that significant incidents are adequately reported, tracked, monitored through resolution and resolved timely.		
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.	For a sample of Major and Security Incidents selected from the Fujitsu SharePoint - Security Occurrence Reports (Security Incidents) and incident tool, TfsNOW (Major Incidents), 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 *27 October 2022 – 31 December 2022* On a weekly basis, the Fujitsu MAC Team reviews and reports the number and severity of outstanding incidents in TfsNOW.	For a sample of weeks inspected the incident reports to determine whether the Fujitsu MAC Team had reviewed the number and severity of outstanding incidents in TfsNOW. Please refer to control 5.3 for the test procedures performed for monthly incident reporting for the period prior to the weekly incident reporting control operating.	No deviations noted.
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 key event, inspected the alert and TfsNOW ticket to determine whether the alert was flagged to the SMC for resolution and that the event was resolved in a timely manner through Fujitsu's incident management procedures. Please refer to controls 6.2–6.4 for test procedures performed for incident management process.	No deviations noted.

POL00337569

4.2.7 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).	Refer to control 5.3 within Control Objective 5 for the testing procedures performed.	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 to determine whether these are available to Fujitsu employees via Dimensions 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 TfsNOW 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 TfsNOW. Selected a network change and inspected the TfsNOW ticket and related approvals to determine whether this change was managed using the standard Fujitsu TfsNOW process including authorisation, testing and approval prior to deployment. Please refer to Control Objective 8 for test procedures performed on network change management.	No deviations noted.

POL00337569

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 System Management Centre (SMC) 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 Spectrum and Tivoli Netcool tools monitoring network availability, to determine whether they are configured to send automated alerts to the SMC Team.	No deviations noted.
7.4 Network Incident Management Incidents relating to network availability are managed using standard incident management procedures.	Selected a network incident from the incident management tool, TfsNOW, and inspected the TfsNOW ticket and history log of the incident to determine whether it was managed using the standard POL incident management procedures, and is included in the standard incident management reporting to POL. Please refer to Control Objective 6 for our test procedures performed for the incident management process.	No deviations noted.

POL00337569

4.2.8 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 TfsNOW 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 network changes from the change management tool, TfsNOW. Selected a sample of changes and inspected the supporting TfsNOW change tickets and related change review discussions between Fujitsu and POL to determine whether the TfsNOW 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 Change Owner, with the approval being documented in the TfsNOW toolset. Changes that cause major service interruption or are a significant risk must also be authorised by the Change Advisory Board (CAB), with the approval documented in the meeting minutes and within the TfsNOW change record.	Obtained a system generated listing of system software and network changes from TfsNOW. For a sample of changes, inspected the supporting TfsNOW tickets and related approval confirmations to determine whether these changes were authorised by the Change Owner and the approval was documented in meeting minutes (including CAB approval for major service interruption changes or significant risks) and within TfsNOW.	No deviations noted.
8.3 Emergency Changes A change deemed necessary in order to resume live service will be agreed, approved and documented on TfsNOW emergency change record. Updates are communicated 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 TfsNOW. For a sample of emergency changes, inspected the supporting TfsNOW tickets, approval confirmations and corresponding communications between Fujitsu and POL to determine whether: • They had been agreed, approved and documented during the incident; and • Updates to POL had been sent as per the agreed timeframes dependent on the severity of the incident.	No deviations noted.

POL00337569

4.2.9 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.	Inspected SDLC policies and procedures on Europe Connect to determine whether these were available to relevant Fujitsu employees, and whether phases included: • Initiation; • Requirements; • Definition; • Design; • Development; • Deployment; and • Maintenance.	No deviations noted.
9.2 Change Governance 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 TfsNOW. For a sample of changes, inspected the supporting TfsNOW tickets and related change approval confirmations to determine whether these changes were 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.

POL00337569

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 requirements are outlined in the Commercial Work Order (CWO) and if justified, within a (CSP) Customer Solution Proposal, (PSD) Project Solution Design documents or (FSR) Feasibility Study Reports, as applicable, that is stored in Dimensions and is reviewed and approved by POL and Fujitsu management.	Obtained a system generated listing of new or modified application software changes from TfsNOW. Selected a sample of changes and inspected the supporting CWO and CSPs/PSDs/FSRs, approvals and Dimensions to determine whether projects were reviewed and approved by POL as well as Fujitsu management and stored in Dimensions.	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 TfsNOW. For a sample of changes, inspected the supporting TfsNOW tickets, test plans completed and approvals documented to determine whether, where applicable, for these changes: • Testing had been performed by the relevant Fujitsu team and POL team; • Test plans had been placed in the Quality Centre (1 April 2022 – 30 June 2022) or in the Zephyr (1 July 2022 to 31 December 2022) application; and • The POL Testing Manager had emailed to indicate their approval that testing has been successfully completed.	No deviations noted.

POL00337569

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.		
9.5 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 a system generated list of users with deployment privileges from the TPM and BigFix systems to determine whether it was restricted to authorised users based on their job responsibilities. Obtained a system generated list of users from the Dimensions tool server and inspected the users with access to develop changes to determine whether segregation of duties was enforced between users able to develop and implement changes.	Deviation noted. We inspected the list of users with development access and compared against users with access to implement changes, and noted one user who has access to both develop and implement changes. We performed additional testing to inspect the delivered baselines within Dimensions and noted that the user had not delivered a baseline (i.e. did not perform any development activity) from 1 April 2022 to 31 December 2022. **Management response:** There are compensating controls in place that mitigate this finding. From a substantive review of the user who had access to both development and implementation, our risk assessment shows that the user did not access the development account during the audit period, as validated by EY. The finding has highlighted that having both types of access is not required and is as a result of role changes. This will be addressed in conjunction with the applicable Assignment Managers to clarify the specific access required, removing any unnecessary access.

POL00337569

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 TfsNOW tool.	Obtained a system generated listing of new or modified application software changes from TfsNOW. For a sample of changes, inspected the supporting TfsNOW tickets and change deployment approval confirmations to determine whether POL approval to implement the change was obtained and documented within the tool.	No deviations noted.

POL00337569

4.2.10 Control Objective 10

Controls Specified by Fujitsu	*Testing Performed*	*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.	Inspected Fujitsu's Post Office HNG-X Account Information Security Policy on Europe Connect to determine whether this policy was available to relevant Fujitsu employees, and whether these had been reviewed and agreed by both POL and Fujitsu.	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 Dimensions system which details the listing of platforms and servers in operational use within the account estate. For a sample of POL platforms in operational use, inspected the High-Level Design, Low-Level Design, and Physical Platform Design documents to determine whether baseline standards had been defined and agreed with POL.	No deviations noted.
10.3 Baseline Operating System Standards Implementation Platforms in operational use are set up and configured in line with documented and agreed baseline standards. Variances from the baseline standard are fully documented and appropriately approved.	Obtained the Platform Hardware Instance List (PHIL), selected the POL 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 the POL platform baseline standard documents to determine whether these variances had been documented and approved in accordance with defined procedures.	No deviations noted.
10.4 User (Fujitsu) Set-up and Amendment Fujitsu users requiring new or modified access to POL systems are set up appropriately after approval by an appropriate Fujitsu line manager.	Obtained a system generated listing of users from the POL starters, transfers and leavers management tool, EMEIA Connect. For a sample of new or modified Fujitsu users, inspected the supporting user access request tickets and user access listings to determine whether the users had been set up in	No deviations noted.

POL00337569

Controls Specified by Fujitsu	Testing Performed	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.		
	accordance with the approved access request and after the 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.	Obtained a system generated Europe Connect report of leavers. For a sample of leavers, inspected the supporting access revocation requests and user access lists to determine whether access had been removed within five working days of the user's leave date.	Deviations noted. We selected a sample of 10 Fujitsu staff with access to the in-scope POL infrastructure who had left during the examination period. We noted that for six of these leavers, their access to certain Fujitsu systems and tools used to support in-scope POL infrastructure was not removed within five working days of their last day with Fujitsu or the POL account. We confirmed that access to the MSAD AD domain (which is the first level authentication after which Fujitsu staff gain privileged access to the in-scope POL infrastructure through two-factor authentication) for the sampled leavers had not been used since they had either left Fujitsu or the POL account. We performed additional testing to compare all leavers during the period against active and disabled accounts on the MSAD AD domain. We determined that none of the active MSAD accounts belonged to staff who had left Fujitsu or the POL account and that last log on dates for leavers who had MSAD access were before or on the leavers' actual leave dates. **Management response:** The systems for which access had not been revoked in a timely manner do not provide any access to data. All the systems identified are call

POL00337569

Controls Specified by Fujitsu	Testing Performed	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.		
		handling systems and development areas. However, we appreciate that timely revocation of all user access is good practice. To ensure we tighten up on this process, we have re-educated the administrators of the various systems that they must action revoke requests within 5 days and report back on any issues preventing them from doing so. We will also ensure that we monitor more closely and follow up when we do not obtain positive confirmation of revocation of a user's access within a short timeframe. We have also re-stated that leavers forms should be submitted by Assignment Managers in good time to allow for the scheduling of access revocation on the leave date.
10.6 Periodic User Reviews Fujitsu reviews user access to systems on a monthly basis to determine the appropriateness of access, and changes performed as deemed necessary.	For a sample of monthly reviews inspected the ISMF report 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.	Inspected the configuration settings in the Active Directory Domain to determine whether two factor authentication was required to access POL systems. Observed a Fujitsu staff log on to the POL systems network to determine whether it required two factor authentication.	No deviations noted.

POL00337569

4.2.11 Control Objective 11

Controls Specified by Fujitsu	*Testing Performed*	*Results of Tests*
Control Objective 11: Controls provide reasonable assurance that access to databases, data files and programs is restricted to 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 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 the TfsNOW change tickets, patch review and approvals to determine whether the most recent patches had been applied as per the TfsNOW change process. Please refer to Control Objective 8 for patch management test procedures performed.	No deviations noted.
11.2 System Administrators Access to perform system administrator functions is restricted to appropriate Fujitsu personnel.	Obtained the Platform Hardware Instance List (PHIL) 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 Fujitsu 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 Platform Hardware Instance List (PHIL) of live POL platforms. For a sample of in-scope databases, inspected system-generated lists of users with database administrator access rights to determine whether access to administer the databases was restricted to appropriate Fujitsu users based on their job responsibilities.	No deviations noted.

POL00337569

Controls Specified by Fujitsu	Testing Performed	Results of Tests
Control Objective 11: Controls provide reasonable assurance that access to databases, data files and programs is restricted to authorised individuals.		
11.4 Administration Tools and System Utilities Access to administration tools and system utilities on Fujitsu managed infrastructure is restricted to appropriate Fujitsu personnel.	Obtained the Platform Hardware Instance List (PHIL) of live POL platforms For a sample of 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.
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 Platform Hardware Instance List (PHIL) of POL platforms. Inspected the configuration settings of Fujitsu's Tripwire system to determine whether automated alerts are configured to alert the Security Operations Team for changes applied to Fujitsu-managed HNG-X infrastructure. For a sample alert from the Tripwire system, inspected the supporting alert and TfsNOW ticket to determine whether changes to Fujitsu-managed infrastructure followed the formal incident management process. Please refer to Control Objective 6 for test procedures performed for the incident management process.	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 Platform Hardware Instance List (PHIL) 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.

POL00337569

4.2.12 Control Objective 12

Controls Specified by Fujitsu	*Testing Performed*	*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.	Refer to control 6.4 within Control Objective 6 for the testing procedures performed.	No deviations noted.
12.1 Firewall Configuration Access Access to set-up and configure firewalls is restricted to appropriate users from the Fujitsu Security Delivery team.	Obtained the system generated list of network users from Active Directory, with access to set-up and configure firewalls, and inspected the listing to determine whether access was restricted to Fujitsu Security Delivery team users based on their job responsibilities.	No deviations noted.
12.2 Configuration Changes Changes to firewall configuration follow the standard Fujitsu TfsNOW process including authorisation, testing (where deemed appropriate) and approval of changes before they are implemented.	Obtained the Patch Approval Board (PAB) deployment list. Selected a sample change to firewall configurations and inspected change documentation to determine whether the change had been authorised, tested and approved prior to implementation as per the TfsNOW process tested in Control Objective 8. Please refer to Control Objective 8 for configuration change test procedures performed.	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.	Obtained the list of in-scope servers from Platform Hardware Instance List (PHIL) and inspected the Anti-Virus tool to determine whether each server had Anti-Virus software installed and updated based on POL's contractual requirements.	No deviations noted.

POL00337569

Controls Specified by Fujitsu	Testing Performed	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 Fujitsu ATC 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 and detect threats and alert the Fujitsu ATC team. For a sample alert from IDS, inspected the supporting TfsNOW incident ticket and resolution activities performed to determine whether the alert was handled by the Fujitsu ATC team and managed through Fujitsu's formal security incident management process. Please refer to Control Objective 6 for our test procedures performed for the incident management process.	No deviations noted.