POL00030526

Document Title:	RA REPORT
Document Reference:	COM/MGT/REP/4165
CP/CWO Reference:	N/A
Abstract:	Explanation of the various current forms of Remote Access.
Document Status:	APPROVED
Author & Dept:	Fujitsu
External Distribution:	Restricted. See section titled Information Distribution.
Information Classification:	See section 0.8

Approval Authorities:

Name	Role	
Fujitsu	Horizon Audit Team (POA)	See Dimensions for record

POL00030526

Table of Contents

POL00030526

POL00030526

0 Document Control

0.1 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change CWO, CP, CCN or Peak Reference
1.0	12/02/2021	Approved for release	N/A

0.2 Review Details

Mandatory Review	
Role	**Name**
Horizon Audit Team	Fujitsu

0.3 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
COM/MGT/REP/4160	Latest	Latest	Expanded Table of Contents for the RA Report	Dimensions

0.4 Abbreviations

Abbreviation	Definition
AD	Active Directory
BRDB	Branch Database
CAB	Change Approval Board (POL)
CCTV	Close Circuit Television
EBMS	Europe Business Management System (Fujitsu internal documents)
FAD	Finance Accounting Division (unique identifier allocated by Post Office to branches)
FCN	Fujitsu Core Network
HTTPS	Hypertext Transfer Protocol Secure
LAN	Local Area Network
LST	Live System Test (Test environment)
MFA	Multi-Factor Authentication
MSSQL	Microsoft Structured Query Language (Microsoft database application)
NDM	Network Device Manager (platform code for TACACS server)
OEM	Oracle Enterprise Manager
PAM	Privileged Access Management
POA	Post Office Account
POL	Post Office Limited
RBAC	Role Based Access Control

POL00030526

Abbreviation	Definition
RCA	Remote Client Application
RDP	Remote Desktop Protocol
SAN	Storage Area Network
SFTP	Secure File Transfer Protocol
SIEM	Security Incident and Event Management
SMC	Systems Management Centre
SSC	Software Support Centre
SSH	Secure Shell
SSSD	System Security Services Daemon
SV&I	Systems Validation & Integration
TACACS	Terminal Access Controller Access Control System
VPN	Virtual Private Network

0.5 Glossary

Term	Definition
Assignment Manager	A Fujitsu user's designated manager on the POA
Change Control	POA Change Management Process
Data Centre	Fujitsu IRE11 and IRE19 Data Centres
Gemalto	Security company now owned by Thales
IRE11 and IRE19	Fujitsu Data Centres in Ireland
Peak	Fujitsu Incident and Release Management system
TfSNow	Fujitsu IT Service Management toolset

0.6 Changes Expected

Changes

0.7 Accuracy

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

0.8 Information Classification

The author has assessed the information in this document for risk of disclosure and has assigned an information classification of FUJITSU CONFIDENTIAL. This report is also subject to the Information Distribution statements in Section 11.

POL00030526

1 Executive Summary

The purpose and scope of this report is to explain how Fujitsu currently implements and manages Remote Access to the HNG-x environment. This report does not cover historic Remote Access capabilities. Remote Access can have many meanings and can be interpreted differently. Section 4 sets out Fujitsu's definition and explains how this report's content will be presented. This report provides POL with information to understand how Fujitsu provides this capability for the Production environment.

On 20 August 2020, POL requested an audit of the HNG-x services by sending a letter to Fujitsu titled "Horizon Audit". Following a number of discussions between POL and Fujitsu, it was agreed by POL that Fujitsu would prepare a set of reports on key topic areas identified by POL.

The spirit of the discussions between POL and Fujitsu in relation to these reports was to share content that would allow both organisations to confirm the efficiency of the current ways of working together, and to identify ways to make meaningful improvements that would enhance the working relationships and experience for the POL branches and their subpostmasters. Fujitsu believes in collaboration and welcomes constructive suggestions from POL.

This report explains Remote Access to the HNG-x environment ("RA Report"). It follows the "Expanded Table of Contents for the RA Report" (COM/MGT/REP/4160) which was shared with POL on 01 December 2020.

In this report, Fujitsu clarifies Remote Access and explains it in the context of Remote Connectivity and Privileged Access. Both of these capabilities are necessary for Fujitsu to deliver its contracted obligations.

Remote Connectivity enables specialist support staff to connect to the environment from remote locations. It has been designed to include multiple layers of authentication and control to ensure it is both effective and secure.

Privileged Access allows a restricted number of specialist support staff to make approved changes to the Production environment. The use of these elevated levels of access are documented as part of Change Control and require POL approval. In summary:

- the roles of Windows, Unix and Database Administrators are to keep the IT systems working as required so the HNG-x environment can function as needed;
- The APPSUP temporary role is used for non-balance impacting actions (such as stock unit associations, emergency branch opening, or monthly tidying of despatch reports). APPSUP is not used to correct branch balance discrepancies or to amend financial transactions made;
- The Transaction Correction Tool is the only way that Fujitsu can insert transactions.

It is important to note that the Transaction Correction Tool is not to be confused with the POL Transaction Correction Process. As described above, the Transaction Correction Tool (explained in Section 7.5) is a tool available exclusively to Fujitsu. The POL Transaction Correction Process refers to POL's exclusive ability to correct balance discrepancies.

Although there are no contractual requirements or processes in place with POL for Fujitsu to report on Privileged Access activities, the monthly Security Report that is provided to POL for the ISMF meeting includes information on all Privileged Access types mentioned in this report.

Fujitsu has endeavoured to ensure that the content of this report is correct as at the date of issue. This report has been prepared with the input of numerous Fujitsu individuals and attribution of any statements made in this report should be made to Fujitsu only. In preparing this report, the authors have collectively characterised and summarised many internal Fujitsu documents. They have also described processes and procedures which have been established over many years and may not be in written form. Many of the documents, processes and procedures described in this report are continuously updated and Fujitsu reserves the right to make changes to the way it works in the ordinary course of its operations and business without obligation to update this document. POL should verify the position with Fujitsu before relying upon any information or content from this document in the future, as well as bearing in mind the requirements set out in "Information Distribution" at Section 11 below.

POL00030526

The author has assessed the information in this report for risk of disclosure and has assigned an information classification of FUJITSU CONFIDENTIAL. This report is also subject to further Information Distribution statements at Section 11 in this report.

POL is invited to comment on this report to seek any additional clarifications it needs. Fujitsu will endeavour to respond to any comments or clarifications requested and may, if it deems necessary, provide an updated version of this report.

Fujitsu welcomes the opportunity to provide this report.

POL00030526

2 Purpose & Scope

The purpose and scope of this report is to explain how Fujitsu currently implements and manages Remote Access to the HNG-x environment. This report does not cover historic Remote Access capabilities. Remote Access can have many meanings and can be interpreted differently. Section 4 sets out Fujitsu's definition and explains how this report's content will be presented. This report provides POL with information to understand how Fujitsu provides this capability for the Production environment.

POL is invited to comment on this report to seek any additional clarifications it needs. Fujitsu will endeavour to respond to any comments or clarifications requested and may, if it deems necessary, provide an updated version of this report.

Fujitsu welcomes the opportunity to provide this report and looks forward to a constructive dialogue with POL.

3 Background & Introduction

On 20 August 2020, POL requested an audit of the HNG-x services by sending a letter to Fujitsu titled "Horizon Audit". Following a number of discussions between POL and Fujitsu, it was agreed by POL that Fujitsu would prepare a set of reports on key topic areas identified by POL.

The spirit of the discussions between POL and Fujitsu in relation to these reports was to share content that would allow both organisations to confirm the efficiency of the current ways of working together, and to identify ways to make meaningful improvements that would enhance the working relationships and experience for the POL branches and their subpostmasters. Fujitsu believes in collaboration and welcomes constructive suggestions from POL.

This report explains Remote Access to the HNG-x environment ("RA Report"). It follows the "Expanded Table of Contents for the RA Report" (COM/MGT/REP/4160) which was shared with POL on 01 December 2020.

Remote Access is a necessary part of an IT system. Remote Access is needed in a number of different ways to manage the HNG-x environment, for example, for retrieving log files from the branch counter, administering platforms and databases in the Data Centre and determining root causes of technical errors and taking remedial actions.

Remote Access is a current open and active topic that results in continued communications between POL and Fujitsu. This report aims to collate those interactions and communications in order to provide a common baseline for any future discussions. As POL is aware, Fujitsu is able to access local branch terminals, and is also able to access transactional data logs which are stored in central databases.

There are no contractual requirements or processes in place with POL for Fujitsu to report on Privileged Access activities.

POL decide the communication messages and involvement actions with subpostmasters.

It is also important to note that the Fujitsu Transaction Correction Tool is not to be confused with the POL Transaction Correction Process. The Transaction Correction Tool (explained in Section 7.5) is a tool available exclusively to Fujitsu. The POL Transaction Correction Process refers to POL's exclusive ability to correct balance discrepancies in POL Branches.

As a general comment, it should be noted that Fujitsu is one of many suppliers involved in the overall delivery of end-to-end services to POL in relation to HNG-x. HNG-x also relies on the working partnership between POL and its chosen partners – such as Verizon, Computacenter and Atos – as well as external service providers such as banks and affiliated organisations. This applies to both the IT systems and the operational processes in HNG-x.

Although every effort has been made to avoid confusing technical jargon in this document, the very nature of this aspect of the service delivered to POL necessitates the use of many acronyms and phrases that may need expanding upon to ensure the correct understanding. Fujitsu accepts that further explanation may be necessary and encourages POL to seek clarifications if anything is unclear.

POL00030526

Fujitsu has endeavoured to ensure that the content of this report is correct as at the date of issue. This report has been prepared with the input of numerous Fujitsu individuals and attribution of any statements made in this report should be made to Fujitsu only. In preparing this report, the authors have collectively characterised and summarised many internal Fujitsu documents. They have also described processes and procedures which have been established over many years and may not be in written form. Many of the documents, processes and procedures described in this report are continuously updated and Fujitsu reserves the right to make changes to the way it works in the ordinary course of its operations and business without obligation to update this document. POL should verify the position with Fujitsu before relying upon any information or content from this document in the future, as well as bearing in mind the requirements set out in "Information Distribution" at Section 11 below.

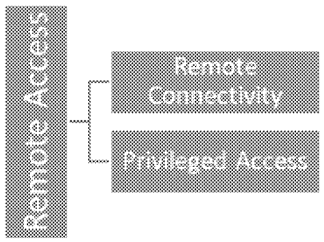
4 Terminology

The term "Remote Access" is used to describe a number of aspects of IT systems. The following section provides clarity on terminology to allow further detail in this report to be provided in a structured manner.

Remote Access relates to the following areas:

Remote Connectivity – The ability for specialist support staff to connect to an environment to access and provide support to a system from a location other than where it is physically located.

Privileged Access – The ability for specialist support staff to carry out operations on the system that they have accessed – whether such access is from a remote location or from the physical location where the system is located.



Remote Connectivity is a widely understood requirement in almost all IT systems to allow a service provider and/or an operator to connect to systems that they are responsible for supporting.

Most Fujitsu specialist support staff work from a location other than where the systems they need to support are located. They need Remote Connectivity in order to:

- Support the branch application on the branch counter
- View and retrieve logs held locally on the branch counters
- Administer platforms in the Data Centre
- Administer databases in the Data Centre
- Determine root causes and effect remediation actions

Remote Connectivity is further explained in Section 5 of this report.

Some specialist support staff also require Privileged Access to be able to perform some of their responsibilities. Again, this is a standard requirement in all IT systems to allow a service provider and/or an operator to keep systems working, investigate issues, and make necessary and required updates. Such access relies on Privileged Access Management processes.

Important note: Other parties may have Privileged Access capabilities that Fujitsu is neither responsible for nor aware of. For example, Computacenter, Verizon and Atos.

POL00030526

Privileged Access comprises three key elements:

A. The processes around Privileged Access user account creation, routine validation, and revocation; and

B. The tools and processes implemented to enable Privileged Access user activity monitoring; and

C. The level of visibility and impact for POL and subpostmasters when Privileged Access activities are undertaken.

Point A is explained in more detail in Section 6 of this report.

Points B and C are explained in more detail in Section 7 of this report.

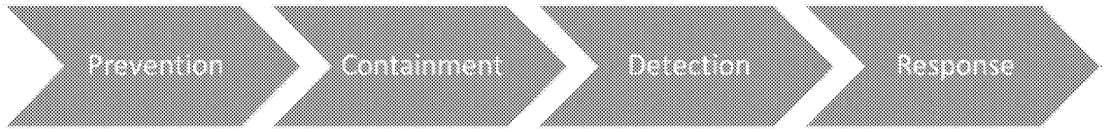
5 Remote Connectivity to Systems

Remote Connectivity is a widely understood requirement in almost all IT systems to allow a service provider and/or an operator to connect to systems that they are responsible for supporting.

Note: Other parties may have Remote Connectivity capabilities that Fujitsu is neither responsible for nor aware of. For example, Computacenter, Verizon, and Atos.

5.1 Overview of Environment/Architecture

The HNG-x security architecture is risk-based and uses the Prevention, Containment, Detection, Response model.



This strategy applies to both infrastructure and software development and provides defence in depth protection through the application of layered security controls.

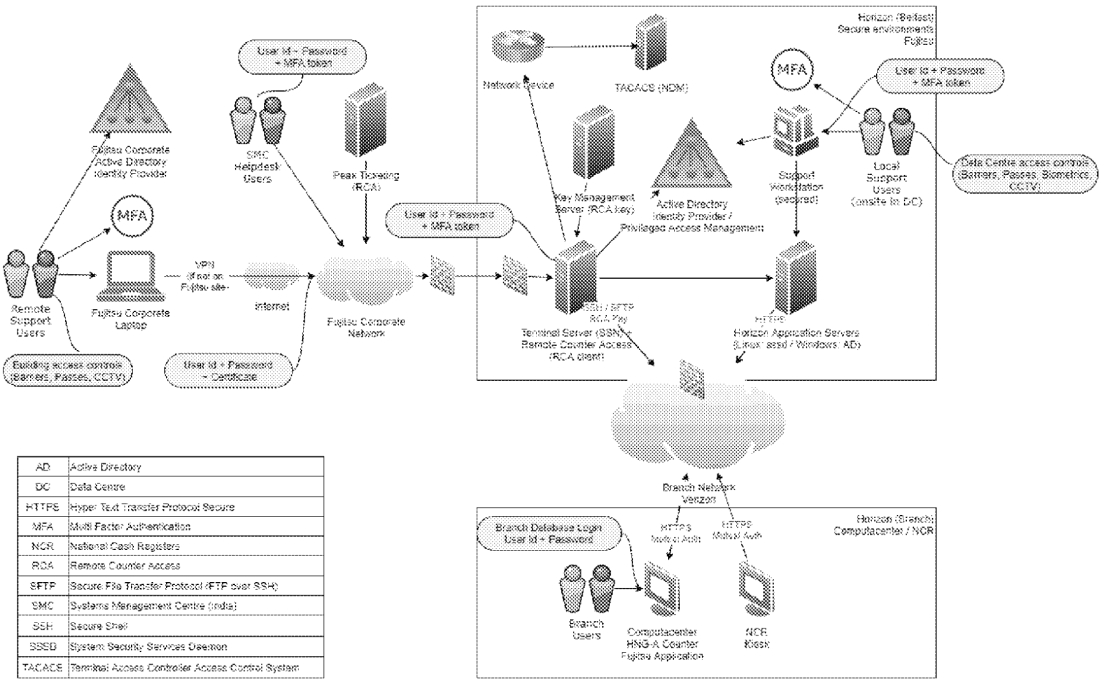
The HNG-x environment is required to connect with third parties on behalf of POL to satisfy business requirements, such as: branch counter and kiosk online transactions; real time services; and reconciliation. This is done over dedicated circuits (provided by Verizon and / or Fujitsu or other third parties) or in a limited number of cases, the Internet.

Fujitsu personnel have limited, role-based, local and / or remote connectivity to the HNG-x environment. Secure network protocols, authentication, anti-virus, anti-malware and logging contribute to assuring the system access, data integrity, confidentiality and auditability.

HNG-x environment access requires that users satisfy physical and / or logical and procedural access controls (see Section 6 later in this report). The controls include physical constraints (for example barriers, CCTV, security guards, door access controls, building zone access and proximity passes), logical controls (for example, user ID, password, multi factor tokens and Role Based Access Control (RBAC)) and procedural controls (for example financial background checks and separation of duties).

POL00030526

The diagram below depicts Fujitsu and branch user access to the HNG-x environment and the access controls implemented.



AD	Active Directory
DC	Data Centre
HTTPS	Hyper Text Transfer Protocol Secure
MFA	Multi Factor Authentication
NCR	National Cash Registers
RCA	Remote Counter Access
SFTP	Secure File Transfer Protocol (FTP over SSH)
SMC	Systems Management Centre (India)
SSH	Secure Shell
SSSD	System Security Services Daemon
TACACS	Terminal Access Controller Access Control System

Access to HNG-x environment for Fujitsu support users is via local workstations within IRE11, IRE19, Bracknell or Stevenage (that require physical access) and / or via the Fujitsu Core Network (FCN) that includes the Fujitsu corporate remote VPN solution (that requires a physical laptop, appropriately configured access software with key material, an authorised user ID with active password, and a Multi Factor Authentication physical device). The local workstations (ESET AV) and remote VPN devices (Symantec Endpoint Protection) include active vulnerability monitoring. The local workstations are built to a Fujitsu defined standard.

5.1.1 Systems & Tools

Remote Connectivity to HNG-x requires use of at least two of the following authentication systems:

- Local workstations
- Fujitsu corporate virtual private network (VPN)
- Active Directory (AD) + multi-factor authentication (MFA)
- Terminal Access Controller Access Control System (TACACS)
- Console servers

In general, Fujitsu prefers to integrate HNG-x platforms into the centralised Active Directory (AD) solution. Some third party devices (such as appliances) do not support AD integration and in these instances, local accounts are used. Similar RBAC controls apply and individuals typically use their own accounts.

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.

POL00030526

Each support user has a HNG-x AD user ID and password. The user is issued a Gemalto 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.

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 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 (i.e. making a connection) to branch counters (not kiosks, to which Fujitsu have no Remote Connectivity) requires the authorised support user to invoke the Remote Counter Access (RCA) client tool on the Windows Terminal Server. The command parameters for the RCA client require the specialist support staff to provide (at least) a FAD code, Node reference and Peak reference related to the reason for access. The RCA client obtains the counter access SSH private key from the key management service (see diagram 5.1.1.B below). The RCA client user accessing the SSH server on the branch counter is restricted to a limited set of actions and the user is further restricted by Computacenter defined Windows permissions. The branch counter SSH server only permits connections from the HNG-x Data Centre Windows Terminal Server IP addresses and using the HNG-x authorised SSH key. The RCA client logs the support activity to the Windows Terminal Server event log and the Tivoli agent harvests the log entries and writes them to the Audit Archive. The RCA command that is executed, and the result of the execution of the command, are stored in the Peak (see below). The data retrieved by the command executing may be attached to the Peak call by the specialist support staff if this is needed. Fujitsu can access branch counters, but it is not able to operate any of them.

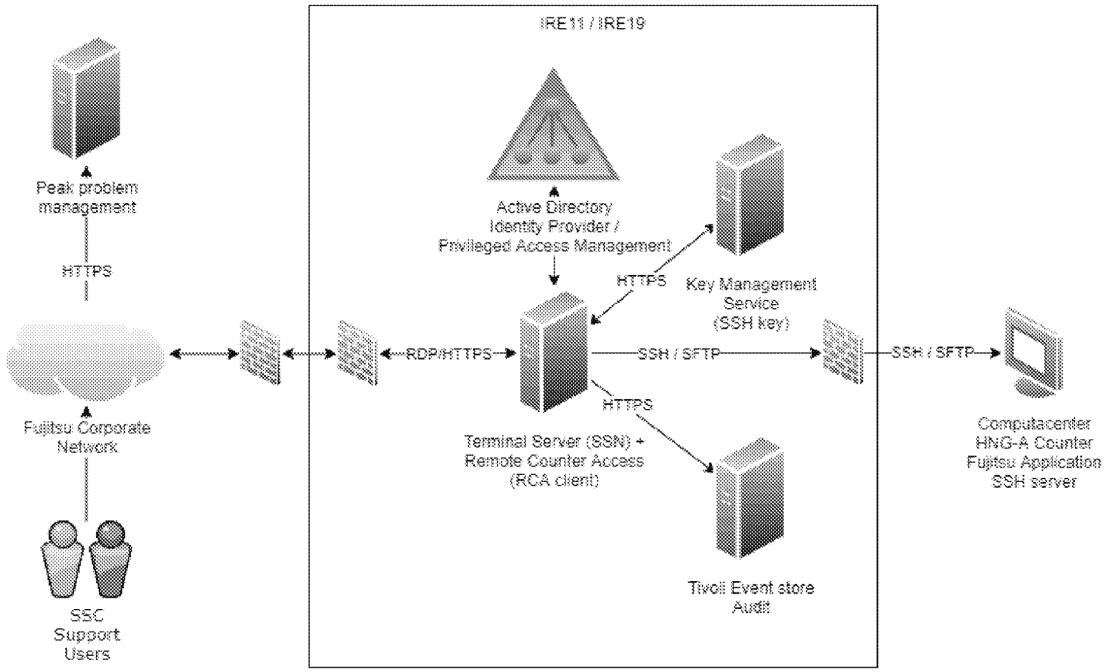
5.1.1.A – Example entry in a Peak following RCA use

Content has been obfuscated for privacy reasons.

Date:22-Nov-2018 09:56:10 User:RCAClient Live PEAK [PC*******] Branch ID [******] Node ID [**] *** [**********] User [*******] Attempting command execution: get /cygdrive/c/ProgramData/Fujitsu/CounterBusinessApplication/log/PostOfficeCounter.log.2018-11-21.zip evidence/******/**_PostOfficeCounter.log.2018-11-21.zip
Date:22-Nov-2018 09:56:23 User:RCAClient Live PEAK [PC*******] Branch ID [******] Node ID [**] *** [**********] User [*******] Command execution completed successfully:get /cygdrive/c/ProgramData/Fujitsu/CounterBusinessApplication/log/PostOfficeCounter.log.2018-11-21.zip evidence/******/**_PostOfficeCounter.log.2018-11-21.zip

POL00030526

5.1.1.B – High-level overview diagram relating to branch counter access



5.2 Types of Remote Connectivity

Remote Connectivity is possible for the following IT systems:

- Data Centre platforms
- Data Centre Storage Area Network (SAN) devices
- Branch counters (not kiosks, to which Fujitsu has no Remote Connectivity)
- Data Centre network devices

Access to the above are either via dedicated workstations within the Data Centres, Bracknell or Stevenage, or via remotely accessible Windows Terminal Servers, as described previously.

5.3 Requirements to use Remote Connectivity

Remote Connectivity is required as part of the following example activities, including but not limited to:

- Normal operational activity:
  - performing cryptographic key renewals
  - issuing certificates
  - monitoring system performance
  - managing platforms
- An investigation:
  - an active Peak call / Incident
- Gathering information for development purposes:
  - troubleshooting system behaviour

POL00030526

5.4 Who has this type of Remote Connectivity

Remote Connectivity uses a role-based access model. Individual users are given the necessary permissions based on their role. The roles themselves restrict access to particular platforms and within platforms to particular functions (for example, read-write or read-only). Windows AD policy, groups and file system permissions, and TACACS limit access. The SSSD integrates Linux servers into AD authentication.

The user groups that may use certain levels of Remote Connectivity are:

- Software Support Centre (SSC)
- Systems Management Centre (SMC)
- Windows support
- UNIX support
- Network support
- Database support
- Security Operations
- Management System Support (MSS)
- Systems Management Group (SMG)
- Test teams
- Development teams
- Architects

The levels of Remote Connectivity access for members of each of the above teams is dependent on their role (as described earlier in Sections 5.2 and 5.3).

Examples of such access types and the user groups for each are set out below:

	Access requirements		
Resource	**Virtual**	**Physical**	**User group**
• Fujitsu corporate network	• Corporate laptop • Corporate issued VPN client certificate • Corporate AD credentials • Corporate VPN enabled	• Building pass • Building zone access • Corporate laptop • Corporate issued certificate • Corporate AD credentials	• All Fujitsu staff
• IRE11 / IRE19 Data Centres • Bracknell • Stevenage	• As above	• Pre-registered visit including vehicle registration plate • As above	• Designated site based personnel
• IRE11 / IRE19 Network device	• As above • POA AD user ID & password & MFA token • TACACS user ID and password	• As above • POA AD user ID & password & MFA token • TACACS user ID and password	• Network support
• IRE11 / IRE19 Application Server	• Corporate laptop • Corporate issued VPN client certificate • Corporate AD credentials • Corporate VPN enabled • POA AD user ID & password	• Building pass • Corporate laptop • Corporate issued certificate • Corporate AD credentials • POA AD user ID &	• Software Support Centre (SSC) • Systems Management Centre (SMC) • Windows Support

POL00030526

	& MFA token • Appropriate POA AD group membership	password & MFA token • Appropriate POA AD group membership	• UNIX support • Database support • Security Operations • Management System Support (MSS) • Systems Management Group (SMG) • Test teams • Development teams • Architects
• IRE11 / IRE19 Database Server	• Corporate laptop • Corporate issued VPN client certificate • Corporate AD credentials • Corporate VPN enabled • POA AD user ID & password & MFA token • Appropriate POA AD group membership	• Building pass • Corporate laptop • Corporate issued certificate • Corporate AD credentials • POA AD user ID & password & MFA token • Appropriate POA AD group membership	• Database support • Windows Support • UNIX support • Systems Management Centre (SMC) • Management System Support (MSS) • Systems Management Group (SMG)
• Branch counter	• As per IRE11 / IRE19 Application Server • RCA client group membership	• As per IRE11 / IRE19 Application Server • RCA client group membership	• Software Support Centre (SSC)
• Standalone devices (local login)	• As per IRE11 / IRE19 Application Server • Local user ID and password for the device stored in the user's KeePass safe	• As per IRE11 / IRE19 Application Server • Local user ID and password for the device stored in the user's KeePass safe	• Windows Support • UNIX support

5.5 Logging of Remote Connectivity

The following activities are logged to either the local Windows log, remote Syslog or Peak server:

- Windows Terminal Server access (success and failure to authenticate)
- Network device access
- Application server access
- Branch counter access (plus details of files transferred during the session)

POL00030526

6 Privileged Access Management (PAM)

Some specialist support staff require Privileged Access to be able to perform some of their support responsibilities. Again, this is a standard requirement in all IT systems to allow a service provider and/or an operator to keep systems working, investigate issues, and make necessary and required updates. Such access relies on PAM processes which are described below.

Important note: Other parties may have Privileged Access capabilities that Fujitsu is neither responsible for nor aware of. For example, Computacenter, Verizon, and Atos.

6.1 Overview of PAM

This section of the report will explain the PAM processes around Privileged Access user account creation, routine validation, and revocation.

Phrases such as root access, domain administrator, account operator, power user, database administrator, backup operator, super user, print operator or elevated access rights all fall within Fujitsu's definition of a privileged account (although this may vary throughout the industry).

A privileged account has additional abilities to a "standard" user account. Privileged accounts may be machine accounts or accounts allocated to individual development or support staff. Privileges may include access rights to operating systems or to application software and databases.

System privileges and levels of access required to perform management functions are higher than those assigned to standard users. Therefore, the allocation and use of privileges is restricted and controlled, and the principle of least privilege is used. The principle of least privilege refers to the concept and practice of restricting access rights to only those resources absolutely required to perform the authorised activities. Individuals are not granted unnecessary privileges.

Privileged Access is reviewed on a monthly basis as explained in Section 6.2.3 of this report below.

6.2 Processes, Procedures & Controls

6.2.1 Overall Process

The Fujitsu EBMS outlines the processes to be followed to create, amend and revoke Privileged Access for a given account. The following screenshots outline processes to be followed for each step in the PAM account process. The Fujitsu EBMS provides additional supporting content behind these screens that POA follows.

POL00030526

Figure 6.2.1.A: High Level over-arching End to End process

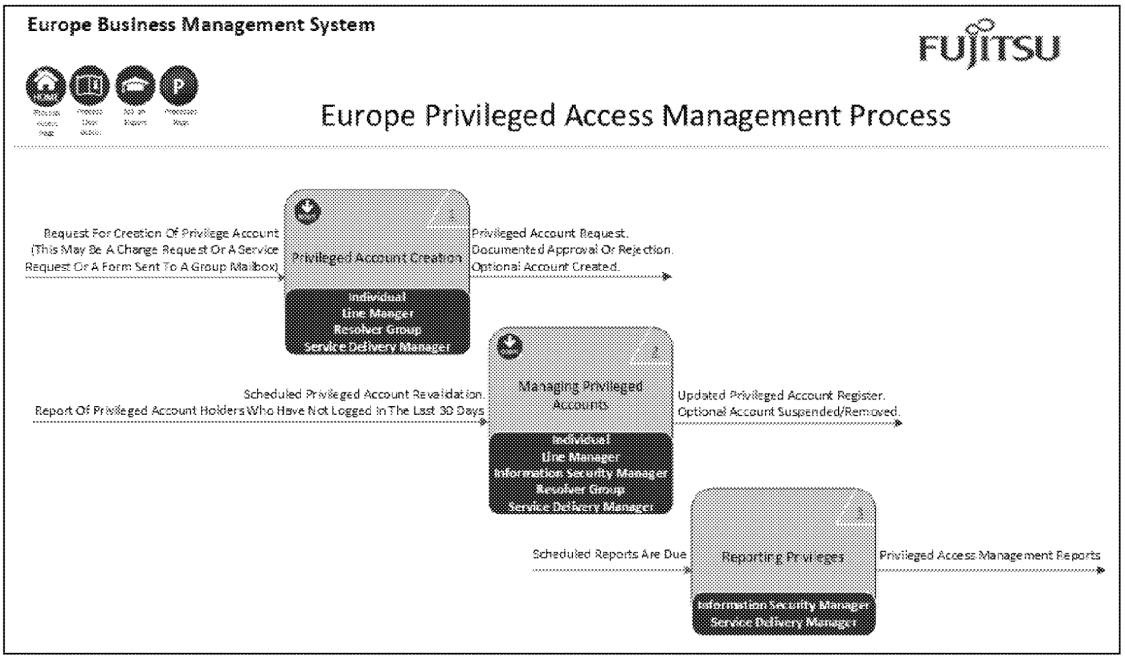
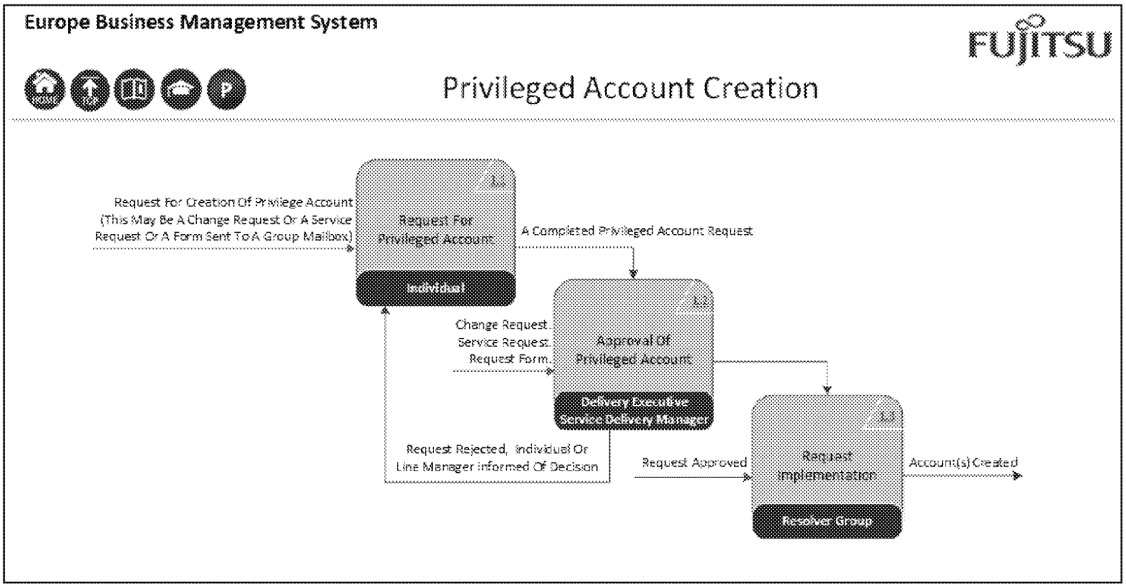


Figure 6.2.1.B: Privileged Account Creation



POL00030526

Figure 6.2.1.C: Managing Privileged Accounts

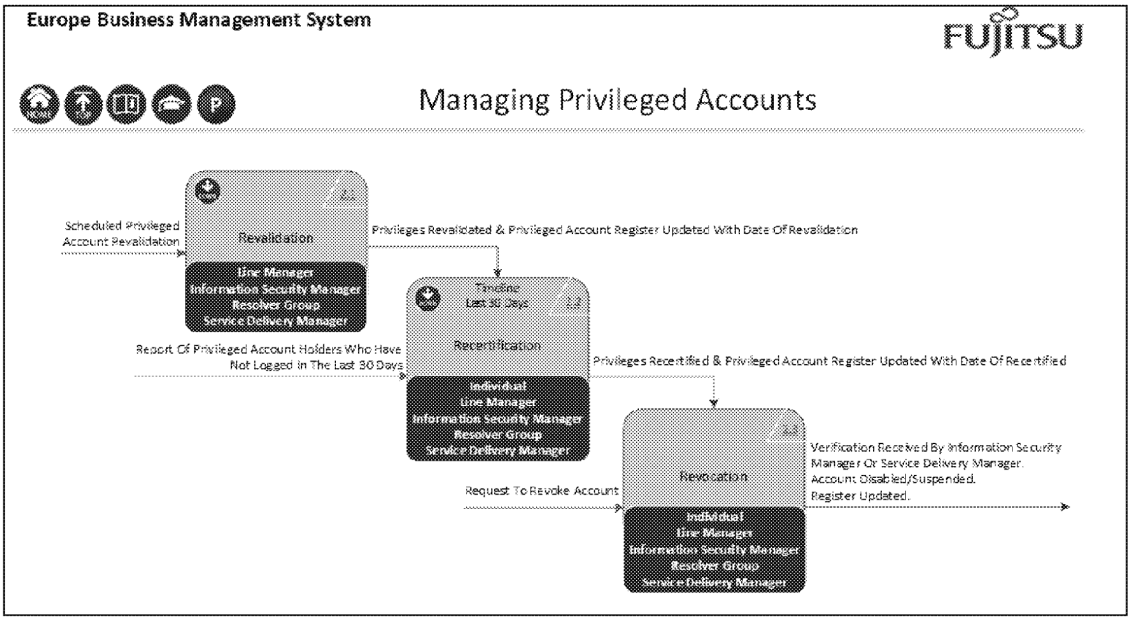
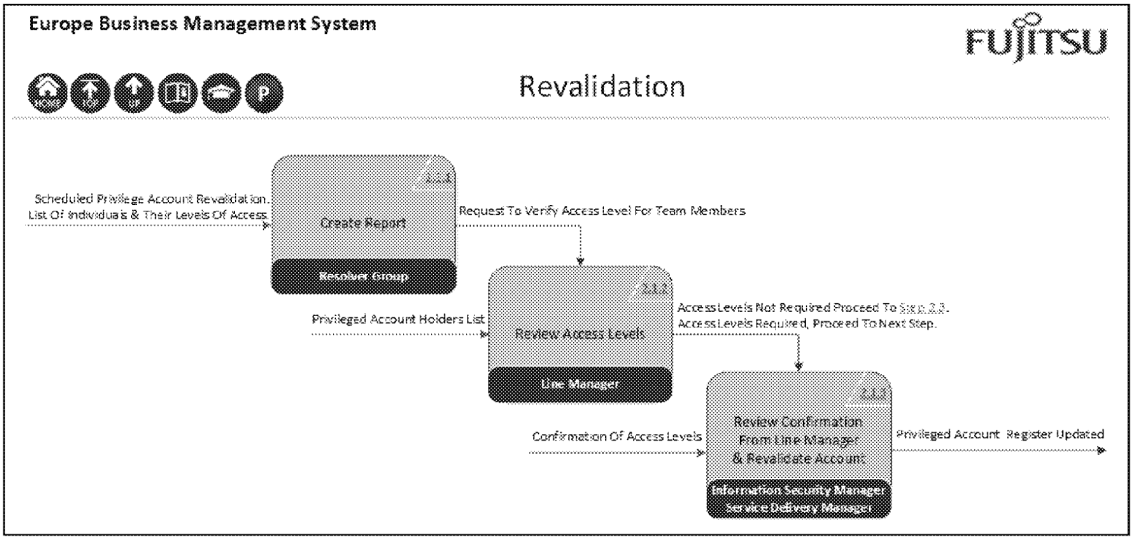
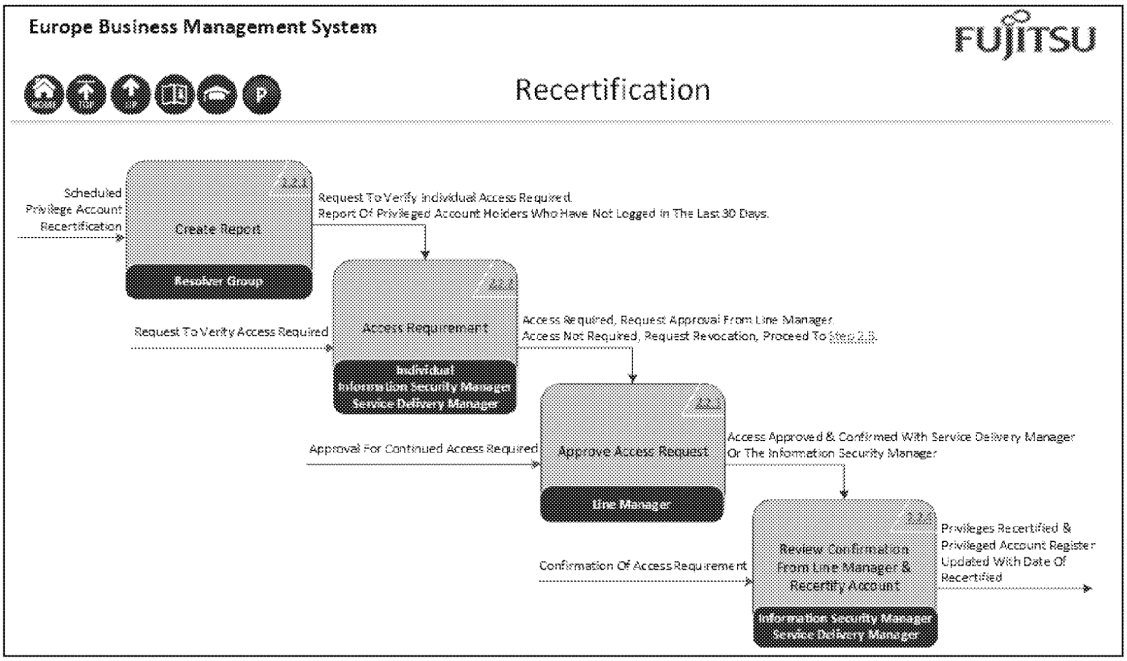


Figure 6.2.1.D: Revalidation



POL00030526

Figure 6.2.1.E: Recertification



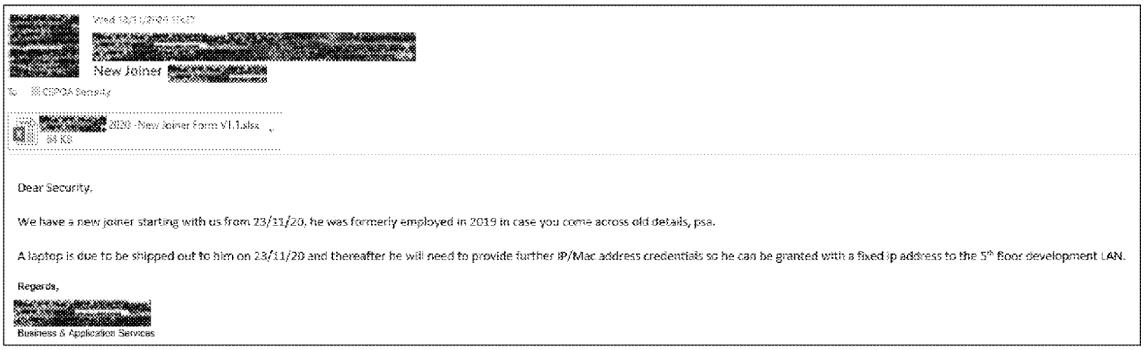
6.2.2 Access for Third Parties

The Fujitsu POA Security team also handle access requests for POL users accessing Fujitsu delivered applications within the Fujitsu environment. The PAM processes and principle of least privilege still apply.

6.2.3 Access Requests, Approval, Routine Validation, Revocation

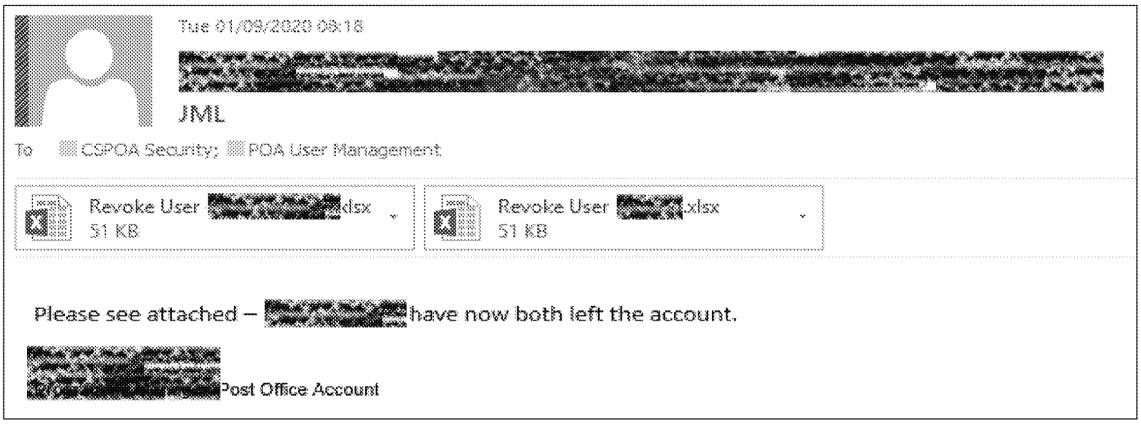
All Privileged Access requests are received into a group mailbox which can only be accessed by the POA Security team. Requests for Privileged Access/change/revocation are received on a form, or by email for access changes and revocation. Access requests, changes or revocations are not accepted verbally. All access follows least privilege and role-based principles as outlined in Fujitsu EBMS. Privileged Access requests must come from either a Fujitsu or POL email address.

Figure 6.2.3.A: New User Example (with redactions as necessary)



POL00030526

Figure 6.2.3.B: Revoke Example (with redactions as necessary)



All Privileged Access requests and changes must be approved by the user's designated manager on the POA (their Assignment Manager) who must verify that the change is appropriate to the job role.

All access is routinely validated on a monthly basis to ensure that the access supplied is still required and appropriate, including standard user access for all POA systems and privileged user access for the Production environment. Access is revoked if verification is not possible, for instance:

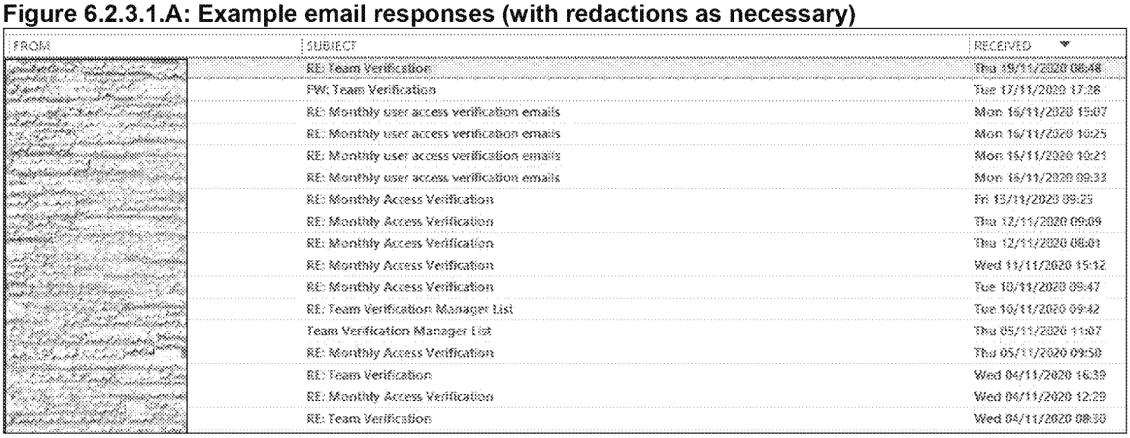
- When requested, and within a short timeframe, or on a date specified
- When verification of the continued need for access is not received
- Where roles change and access is no longer appropriate or required
- Where a user account has not been used for more than 90 days

The local POA User Access Request work instruction (Fujitsu internal document) outlines the low-level process to be followed to request access. This is aligned to Fujitsu EBMS.

6.2.3.1 Standard User Access Verification

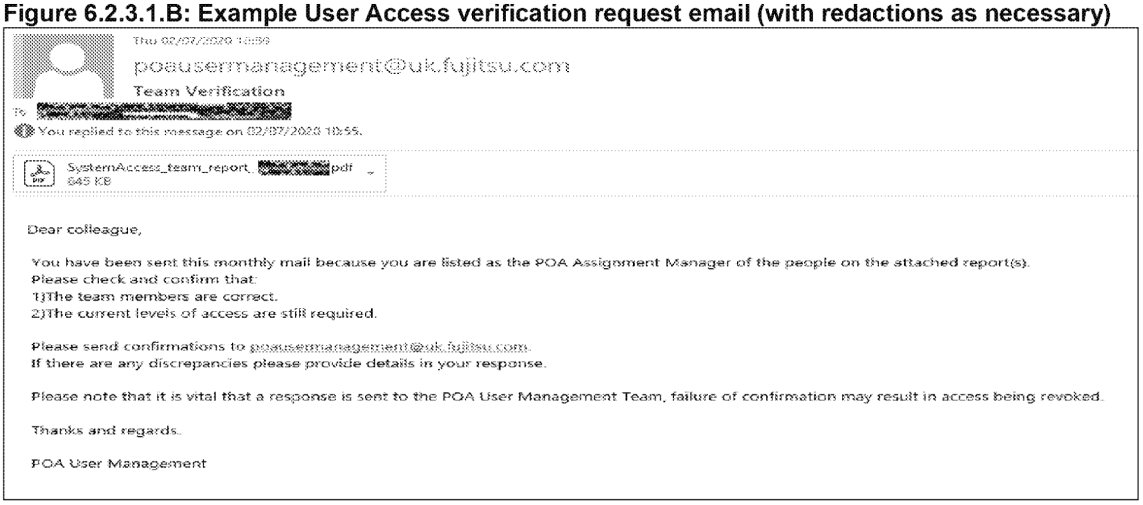
Every month, emails are sent to all Assignment Managers asking them to verify that, for those people for which they are Assignment Manager, the access held is still required and still appropriate.

Figure 6.2.3.1.A: Example email responses (with redactions as necessary)



POL00030526

Figure 6.2.3.1.B: Example User Access verification request email (with redactions as necessary)


Thu 02/07/2020 10:59
poausermanagement@uk.fujitsu.com
Team Verification
To: [redacted]
You replied to this message on 02/07/2020 10:55.
SystemAccess_team_report_[redacted].pdf
645 KB

Dear colleague,

You have been sent this monthly mail because you are listed as the POA Assignment Manager of the people on the attached report(s).
Please check and confirm that:
1)The team members are correct.
2)The current levels of access are still required.

Please send confirmations to poausermanagement@uk.fujitsu.com.
If there are any discrepancies please provide details in your response.

Please note that it is vital that a response is sent to the POA User Management Team, failure of confirmation may result in access being revoked.

Thanks and regards.

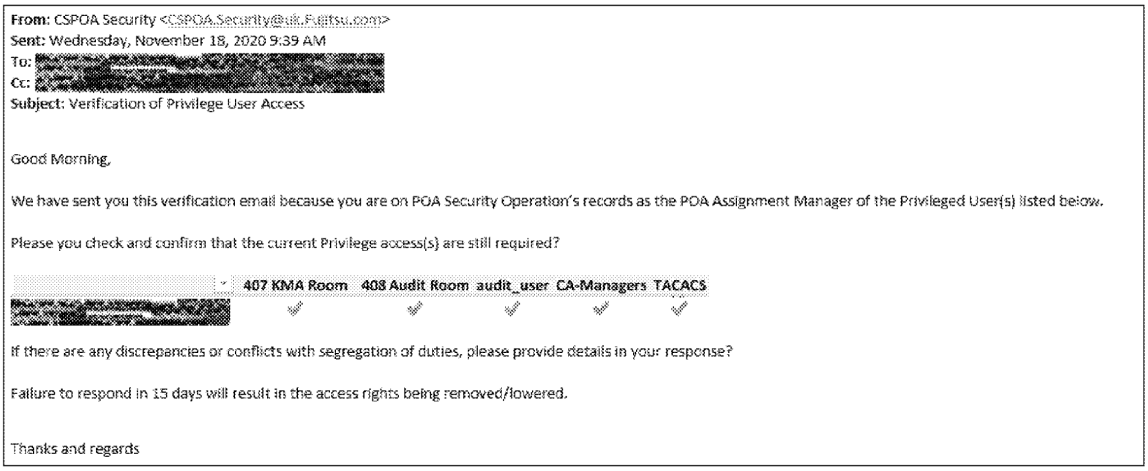
POA User Management

6.2.3.2 Privileged User Access Verification

A second, more detailed access verification check is conducted monthly, specifically for Production Privileged Access. Examples can be seen below which show the check and subsequent actions taken.

As part of this monthly verification process, segregation of duties is also checked to ensure there are no segregation issues – for example, due to changes to a user's role or responsibilities.

Figure 6.2.3.2.A: Example Privileged User Access verification request email (with redactions as necessary)


From: CSPOA Security <CSPOA.Security@uk.Fujitsu.com>
Sent: Wednesday, November 18, 2020 9:39 AM
To: [redacted]
Cc: [redacted]
Subject: Verification of Privilege User Access

Good Morning,

We have sent you this verification email because you are on POA Security Operation's records as the POA Assignment Manager of the Privileged User(s) listed below.

Please you check and confirm that the current Privilege access(s) are still required?

	407 KMA Room	408 Audit Room	audit_user	CA-Managers	TACACS
[redacted]					

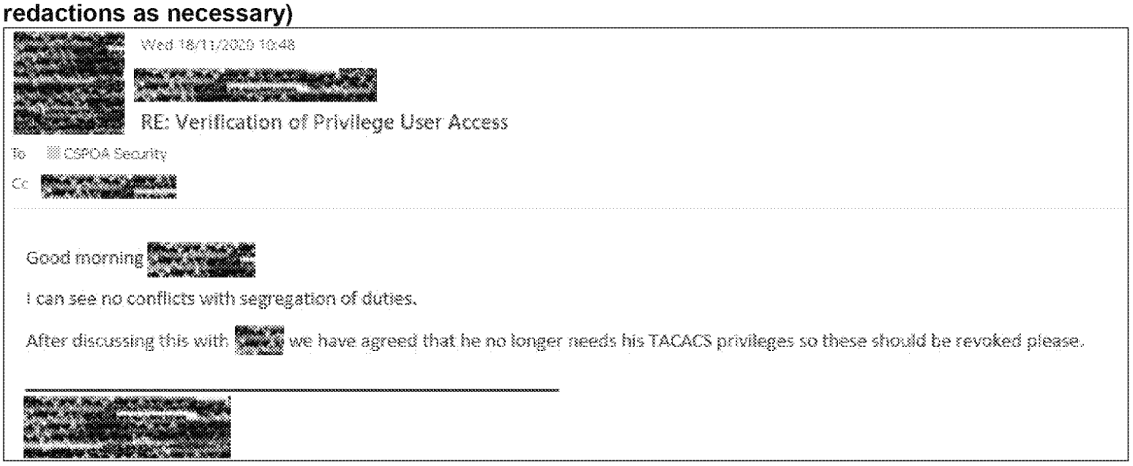
If there are any discrepancies or conflicts with segregation of duties, please provide details in your response?

Failure to respond in 15 days will result in the access rights being removed/lowered.

Thanks and regards

POL00030526

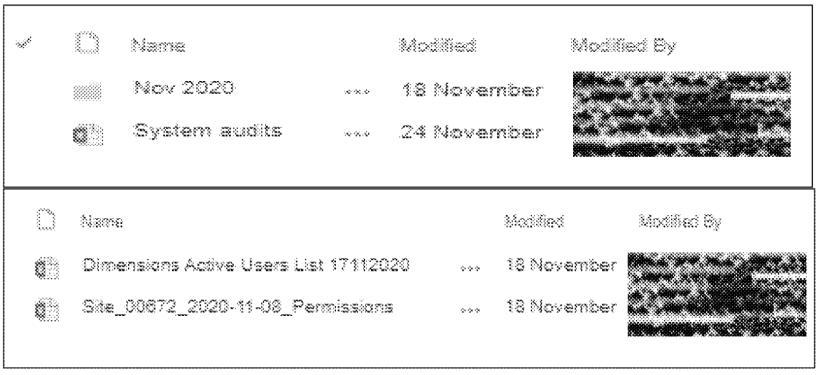
Figure 6.2.3.2.B: Example Privileged User Access verification request email response (with redactions as necessary)



6.2.3.3 POA Security Spot Checks

Over and above the Assignment Manager and PAM access monthly verifications, the POA Security team conduct occasional spot checks of systems. The spot check is performed on a randomly selected system. The current active user account list is obtained and then compared to the central records held. Inconsistencies are investigated and appropriate action taken. A record is kept of which system has been spot checked and when, and the outcome.

Figure 6.2.3.3.A: Example spreadsheets for the tracking of access spot checks (with redactions as necessary)

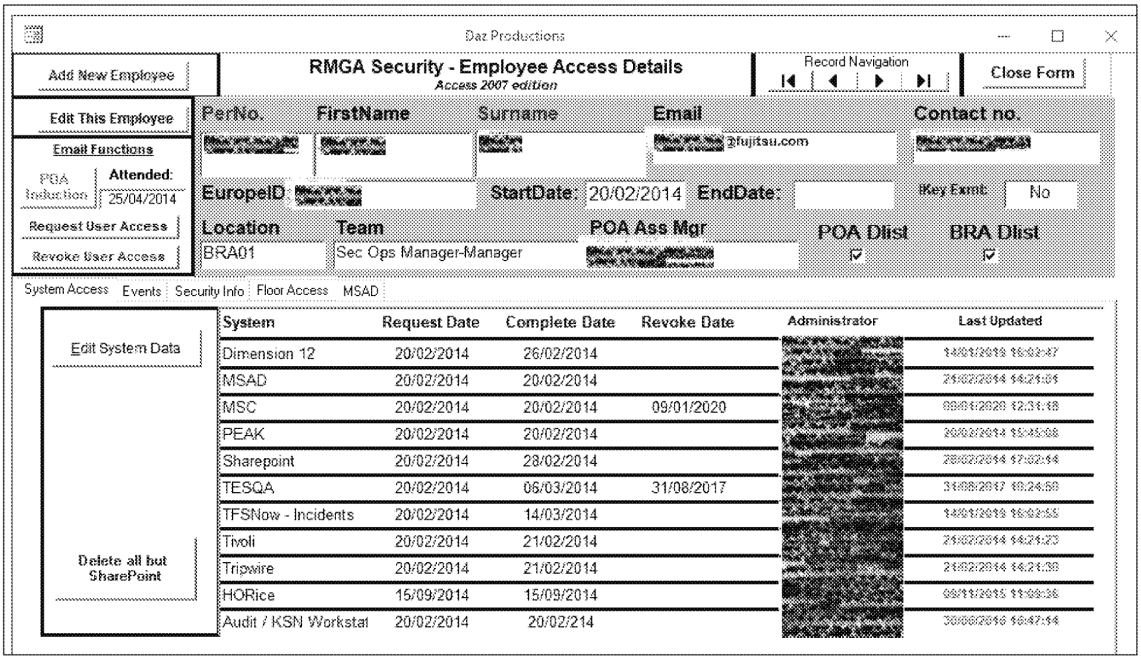


POL00030526

6.3 Systems & Tools

The management of PAM accounts is completed using a variety of tools such as an Access database, Excel spreadsheets, email and SharePoint. A central database is held which records all access across all environments.

Figure 6.3.A: Screen Shot of the User Access Database (with redactions as necessary)



Note: the dates shown are when the redacted user joined the account

A weekly spreadsheet is supplied to the POA Security team which details all Production AD accounts, the last login date/time stamp as well as AD groups applied to the accounts. POA Security team review the spreadsheets monthly to challenge requirements to retain accounts not used in the last 90 days, and to check appropriateness of AD groups based on RBAC (not an exhaustive list). An example can be seen below:

POL00030526

Figure 6.3.B: Screen shot of weekly AD user list report (with redactions as necessary)

Logon	Full Name	OU (Team)	Account Status	Last Logon Date/Time	Age (days)	Password Never Expires	Groups
[redacted]		Admin Users\UNIX Team	ENABLED	05/01/2021 17:06:48	3	NO	is-nt
		Admin Users\UNIX Team	ENABLED	05/01/2021 17:06:48	3	NO	tsadmin
		Admin Users\UNIX Team	ENABLED	05/01/2021 17:06:48	3	NO	est administrators
		Admin Users\UNIX Team	ENABLED	05/01/2021 17:06:48	3	NO	is-backup
		Admin Users\UNIX Team	ENABLED	05/01/2021 17:06:48	3	NO	Backup Operators
		Admin Users\UNIX Team	ENABLED	05/01/2021 17:06:48	3	NO	virtualserveradmins
		Admin Users\UNIX Team	ENABLED	05/01/2021 17:06:48	3	NO	isd
		Admin Users\UNIX Team	ENABLED	05/01/2021 17:06:48	3	NO	Domain Admins
		Admin Users\UNIX Team	ENABLED	05/01/2021 17:06:48	3	NO	SophosAdministrator
		Admin Users\UNIX Team	ENABLED	05/01/2021 17:06:48	3	NO	Administrators
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	Domain Users
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	Cacti Users
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	cacops
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	cacadmins
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	ikey-exemptou-users
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	aurora-users
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	Terminal Service Users
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	Remote Desktop Users
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	is-network
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	is-dba
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	dxcadmins
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	is-unix
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	is-nt
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	tsadmin
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	est administrators
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	is-backup
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	Backup Operators
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	virtualserveradmins
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	isd
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	Domain Admins
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	SophosAdministrator
		Admin Users\UNIX Team	ENABLED	24/12/2020 10:17:18	15	NO	Administrators
		Admin Users\NT Team	ENABLED	08/01/2021 07:54:26	0	NO	Domain Users
		Admin Users\NT Team	ENABLED	08/01/2021 07:54:26	0	NO	nrp_ro
		Admin Users\NT Team	ENABLED	08/01/2021 07:54:26	0	NO	Cacti Users
		Admin Users\NT Team	ENABLED	08/01/2021 07:54:26	0	NO	cacops
		Admin Users\NT Team	ENABLED	08/01/2021 07:54:26	0	NO	cacadmins
		Admin Users\NT Team	ENABLED	08/01/2021 07:54:26	0	NO	aurora-users
		Admin Users\NT Team	ENABLED	08/01/2021 07:54:26	0	NO	Terminal Service Users
		Admin Users\NT Team	ENABLED	08/01/2021 07:54:26	0	NO	Remote Desktop Users
		Admin Users\NT Team	ENABLED	08/01/2021 07:54:26	0	NO	is-network
		Admin Users\NT Team	ENABLED	08/01/2021 07:54:26	0	NO	is-dba
		Admin Users\NT Team	ENABLED	08/01/2021 07:54:26	0	NO	dxcadmins
		Admin Users\NT Team	ENABLED	08/01/2021 07:54:26	0	NO	is-unix

A number of 'Break Glass' or Generic accounts (such as Local Administrative Accounts) are held by the Belfast admin support teams in a KeePass software safe. Access to the KeePass software safe to retrieve a password for an account requires the Belfast admin support team to provide both their allocated certificate and their password.

Some accounts which allow Privileged Access are also held by the POA Security team. These accounts are for use in emergency scenarios (perhaps where a network device has hung and is not accessible using standard access methods). The supply and use of the passwords for those accounts is documented and passwords are changed after use, i.e. they are single use passwords.

6.4 Reporting

The POA Security team supply a monthly Security Report to the POL Security team which provides POL with information on privileged accounts. The report is reviewed with POL Security at the monthly POL Information Security Management Forum (ISMF), which is the main mechanism by which key security points are discussed with POL.

The monthly Security Report contains tabs with the following PAM-related information:

- Number of New User, Change User and Revoke User requests
- Number of login failures
- Number of Privileged Access Accounts per system location or environment
- Last Login date/time for Active Directory PAM accounts
- Log on/off for some non-AD integrated systems
- Access to secure locations, floors and rooms
- Granting of APPSUP role and Transaction Correction Tool permissions

POL00030526

7 Types of Privileged Access

There are different types of Privileged Access required to support and maintain the systems that comprise the contracted responsibilities.

In this section of the report, each type of Privileged Access discussed will be presented in a consistent format, which may result in the repetition of text where a response applies to multiple types of Privileged Access.

In summary, this section will explain the following types of Fujitsu Privileged Access:

- Windows Domain (NT) Administrators – who administer the Windows platforms
- Unix Domain Administrators – who administer the Unix platforms
- Database Administrators – who administer the Oracle and MSSQL databases
- APPSUP Role – used for non-balance impacting actions (such as stock unit associations, emergency branch opening, or monthly tidying of despatch reports). APPSUP is not used to correct branch balance discrepancies or to amend financial transactions
- Transaction Correction Tool – used to insert transactions

The first three administrator types are used on a regular basis as required to keep the HNG-x systems working as required.

APPSUP is used infrequently (on average twice a month throughout 2020) and is a temporary privilege subject to multiple levels of authorisation from POL and Fujitsu.

The Transaction Correction Tool is subject to multiple levels of authorisation from POL and Fujitsu.

Privileged Access that affects branch transaction data is necessary in some circumstances. For example, it may be required to help resolve Incidents raised by subpostmasters, or to complete actions that the HNG-x service was unable to complete for some reason. This could be a bug, error or defect, or it may be a specific scenario that HNG-x has not been designed to cater for.

Fujitsu can access branch counters, but it is not able to operate any of them.

The logs collected relating to Privileged Account activity are extremely large and interspersed with other activity logging. Analysis of the logs would require specialist tools as to do so manually would be practically unworkable. The deployment of Security Incident and Event Management (SIEM) tooling (which would augment Privileged Account activity monitoring and analysis) has been discussed numerous times over the years between Fujitsu and POL but has never been taken forward. The absence of a SIEM tool limits Fujitsu's abilities in relation to some security events. This includes Privileged Account activity monitoring and reporting.

POL00030526

7.1 Windows Domain (NT) Administrators

There are a number of versions of the Microsoft Windows operating system deployed that need administering. This role is used to administer the Windows platforms when required.

7.1.1 Scope of Privileged Access

This level of Privileged Access is required to perform the following main tasks:

- System maintenance
- Patching & Upgrades
- Fault investigation
- Fault remediation
- Enabling & disabling logging settings
- Maintain operational availability
- Granting, amending and revoking user privileges
- Perform agreed Change Control activities
- Perform agreed Project Change activities
- Provide security & user reports to POA Security team

7.1.2 Logging of actions

The Windows server writes to the local Application, System & Security logs, which are sent to the IBM Tivoli Netcool server and the Audit Archive.

7.1.3 Visibility for POL

Any use of Privileged Access to make changes to the Production environment is done under Change Control and only with prior approval from POL. POL have visibility of Change Control documents for the Production environment.

7.1.4 Reporting – internal & external

The use of this type of Privileged Access to make changes to the Production environment will be linked to Change Control documents that are produced and shared as part of the POL-led Change Control process. This information sharing is automated between the Fujitsu and POL service management toolsets.

In addition, the number of Windows Domain (NT) Administrators is also included in the monthly Security Report which is provided to the POL Security team. The report is reviewed with POL Security at the monthly POL Information Security Management Forum (ISMF).

POL00030526

7.2 Unix Domain Administrators

There are a number of versions of Red Hat Linux and Solaris operating systems deployed that need administering. This role is used to administer the Unix platforms when required.

7.2.1 Scope of Privileged Access

This level of Privileged Access is required to perform the following main tasks:

- System maintenance
- Patching & Upgrades – operating system
- Fault investigation
- Fault remediation
- Enabling & disabling database logging settings (but not the data)
- Maintain operational availability
- Supporting the DBA Administrators with platform related activities
- Granting, amending and revoking user privileges
- Perform agreed Change Control activities
- Perform agreed Project Change activities

7.2.2 Logging of actions

The following is logged locally and also sent to the IBM Tivoli Netcool server and the Audit Archive:

- All commands executed as Root user against BRDB, NPS, DAT (Scheduling server)
- All events the Unix server writes to Syslog Messages and Syslog Secure (includes user login and Sudo commands used)

7.2.3 Visibility for POL

Any use of Privileged Access to make changes to the Production environment is done under Change Control and only with prior approval from POL. POL have visibility of Change Control documents for the Production environment.

7.2.4 Reporting – internal & external

The use of this type of Privileged Access to make changes to the Production environment will be linked to Change Control documents that are produced and shared as part of the POL-led Change Control process. This information sharing is automated between the Fujitsu and POL service management toolsets.

In addition, the number of Unix Domain Administrators is also shared in the monthly Security Report which feeds in to the monthly POL Information Security Management Forum (ISMF).

POL00030526

7.3 Database Administrators

The role is used to administer the numerous Oracle and MSSQL databases and keep them in the required operational state to hold the system data.

7.3.1 Scope of Privileged Access

This level of Privileged Access is required to perform the following main tasks:

- System maintenance
- Patching & Upgrades – Oracle database e.g. quarterly updates from Oracle, which have to be packaged by the team to be applied to the databases
- Fault investigation & remediation e.g. space, efficient usage of volumes, system errors and warnings
- Enabling & disabling database logging settings (but not the data)
- Maintain operational availability
- Supporting the Unix or Windows Domain Administrators with database related activities
- Granting, amending and revoking user privileges
- Perform agreed Change Control activities
- Perform agreed Project Change activities
- Provide diagnostic information (e.g. to Oracle)

7.3.2 Logging of actions

Oracle events are written to the local Oracle system event logs. These are also sent to the Audit Archive.

SQL events are written to the relevant Windows Application, System & Security log files. These are also sent to the IBM Tivoli Netcool server and the Audit Archive.

7.3.3 Visibility for POL

Any use of Privileged Access to make changes to the Production environment is done under Change Control and only with prior approval from POL. POL have visibility of Change Control documents for the Production environment.

7.3.4 Reporting – internal & external

The use of this type of Privileged Access to make changes to the Production environment will be linked to Change Control documents that are produced and shared as part of the POL-led Change Control process. This information sharing is automated between the Fujitsu and POL service management toolsets.

In addition, the number of Database Administrators is also included in the monthly Security Report which feeds in to the monthly POL Information Security Management Forum (ISMF).

POL00030526

7.4 APPSUP Role

The APPSUP role allows the Privileged Access user to make changes to data within Oracle databases. The APPSUP role has to be granted to a specialist support user when needed. They do not have this role by default.

7.4.1 Scope of Privileged Access

The APPSUP role provides the assigned user with full data read/write privileges on all Oracle databases. The role is only granted to a specific member of the specialist support team for a specific period of time as necessary to perform actions which have been specifically authorised by both POL and Fujitsu.

APPSUP is not used to correct branch balance discrepancies or to amend financial transactions. Corrections relating to branch balance discrepancies are performed by POL using the POL Transaction Correction Process.

APPSUP is used for non-balance impacting actions (such as stock unit associations, emergency branch opening, or monthly tidying of despatch reports). Some APPSUP actions can indirectly lead to a balance impact (such as deleting a corrupt recovery message that is causing a logon loop). Where an action being taken by Fujitsu using APPSUP could lead to a balance impact, it is POL that decide if any balance discrepancy correction is required with the branch and it is POL that take any corrective action required.

7.4.2 Assignment of the APPSUP role

Granting of the APPSUP privilege requires approval from three POL entities (POL Service, POL Security and POL Financial Service Centre). POL selected these entities and POL is responsible for the internal approval processes prior to Fujitsu receiving each of the 3 POL approvals. Further approval is then needed from Fujitsu POA Service Operations after which the Fujitsu POA Security team additionally verify that APPSUP is needed based on the defined action to be taken. Fujitsu POA Security then provide the final approval and notify the Unix Administrator team to grant the specified user the temporary elevated privilege. When the actions are complete, Fujitsu POA Security team notifies the Unix Administrator team to revoke the privilege.

Approvals and actions are recorded in TfSNow, change tasks, and Peak.

7.4.3 Logging of APPSUP actions

Actions taken when using the APPSUP role are witnessed by a second member of the SSC support team and this is documented in the Peak. Within the SSC, one member of the SSC will perform the data correction while a second member of the SSC (with appropriate skills and expertise) will witness the change being made. Both names must be recorded on the Peak and the change task.

Note: If the APPSUP role is used out of hours, this is less likely to be witnessed by a second member of the SSC support team. There would be consultation with other working on-call support staff at the time and the recorded actions are also likely to be checked by the SSC Duty Manager. Use of the APPSUP role out of hours is extremely rare.

The applicable logging is as described in Section 7.3.2 on the logging of Database Administrator actions.

7.4.4 Visibility for POL

POL have full visibility relating to the APPSUP role. POL see the Incidents and approve the granting of the APPSUP role for the temporary period. For potentially balance impacting actions, POL decide whether a balance discrepancy correction is required and, if so, enact the required corrective actions.

7.4.5 Reporting – internal & external

In addition to the explanations in the sections above, there are a number of ways in which the assignment and use of the APPSUP role use can be monitored by both Fujitsu and POL:

POL00030526

- From the related TfSNow Incident which is visible to POL via the integration of the Fujitsu and POL service management tools.
- From the three required emails sent by POL to Fujitsu to grant authorisation.
- From the Peaks created and updated to record activity.
- From the monthly Security Report which feeds in to the monthly POL Information Security Management Forum (ISMF). This shows each assignment of the APPSUP role as well as any associated Incident, Change or Peak references.

Example extract from the January 2021 Security Report:

TFSNow ref	*Date APPSUP requested*	*Date APPSUP was Granted*	*Time APPSUP was Granted*	*Date APPSUP revoked*	*Time APPSUP revoked*	*Who APPSUP was granted to ie user*	*INC & Peak/CHG Ref*
INC4391361	06/01/20	06/01/20	10:16	06/01/20	10:29	**obfuscated**	INC4329285/PC0281742
INC4424596	09/01/20	09/01/20	16:46	10/01/20	14:43	**obfuscated**	PC0281946/INC4421666
INC4578838	29/01/20	29/01/20	11:07	29/01/20	11:48	**obfuscated**	PC0282246
INC4739526	17/02/20	17/02/20	16:52	18/02/20	12:20	**obfuscated**	PC0286327
INC4823722	28/02/20	28/02/20	11:07	02/03/20	12:48	**obfuscated**	PC0286463
INC4824263	28/02/20	28/02/20	11:39	03/03/20	10:23	**obfuscated**	PC0286452
INC4810249	28/02/20	28/02/20	16:55	28/02/20	17:04	**obfuscated**	PC0286452
INC4879692	06/03/20	06/03/20	12:23	06/03/20	12:42	**obfuscated**	INC4873126
INC5069711	01/04/20	01/04/20	11:56	01/04/20	15:38	**obfuscated**	PC0287391
INC5112767	07/04/20	07/04/20	10:38	07/04/20	11:58	**obfuscated**	PC0287206/INC5003813
INC5908612	06/08/20	06/08/20	18:00	06/08/20	18:52	**obfuscated**	CHG0185028
INC5938493	11/08/20	11/08/20	09:36	11/08/20	10:37	**obfuscated**	PC0289598
INC5948682	12/08/20	12/08/20	18:00	12/08/20	18:06	**obfuscated**	CHG0185649
INC5960310	13/08/20	13/08/20	15:26	13/08/20	15:59	**obfuscated**	PC0289870
INC5999291	19/08/20	19/08/20	10:35	19/08/20	12:01	**obfuscated**	PC0289934
INC6103727	02/09/20	02/09/20	10:34	02/09/20	15:55	**obfuscated**	PC0290155
INC6605309	05/11/20	05/11/20	13:36	05/11/20	15:43	**obfuscated**	PC0291360/PC0291321
INC6639576	10/11/20	11/11/20	08:14	11/11/20	15:51	**obfuscated**	PC0291513
INC6795573	01/12/20	01/12/20	17:03	01/12/20	18:12	**obfuscated**	PC0291816
INC6802704	02/12/20	02/12/20	12:44	02/12/20	16:37	**obfuscated**	PC0291160

POL00030526

7.5 Transaction Correction Tool

Important note: Please note that the Transaction Correction Tool is not to be confused with the POL Transaction Correction Process. As described above, the Transaction Correction Tool is a tool available exclusively to Fujitsu. The POL Transaction Correction Process refers to POL's exclusive ability to correct balance discrepancies.

The Transaction Correction Tool (also known as BRDBX015) provides a packaged and audited interface to run defined data correction scripts. This tool allows the Fujitsu SSC to insert balancing records to transactional, accounting, or stock tables in the BRDB. The tool was created as making data amendments is highly complex, requiring many parts of the system to be amended concurrently to ensure data integrity and avoid errors.

7.5.1 Scope of Privileged Access

This tool allows the Fujitsu SSC to insert balancing records to transactional, accounting, or stock tables in the BRDB.

7.5.2 Assignment of permission to use the Transaction Correction Tool

Use of the Transaction Correction Tool by Fujitsu requires granting of permission to use it following the same process as is used for granting the APPSUP role. This would include multiple (both POL and Fujitsu) approvals and permission being temporary. See APPSUP Section 7.4.2.

7.5.3 Logging of Transaction Correction Tool usage

Every correction that is completed using the Transaction Correction Tool generates an audit record in the BRDB which is then extracted on a nightly basis via process BRDBC033 and made available to the Audit Archive system.

In addition to the audit records in the BRDB and Audit Archive systems, logging would be the same as is described for the APPSUP role. See APPSUP Section 7.4.3.

7.5.4 Visibility for POL

Visibility for POL would be the same as is described for the APPSUP role. See APPSUP Section 7.4.4.

7.5.5 Reporting – internal & external

Reporting would be the same as is described for the APPSUP role. See APPSUP Section 7.4.5.

Note – the monthly Security Report shows the uses of the Transaction Correction Tool.

POL00030526

8 Formal Audit Reports

POL has commissioned an ISAE3402 audit as well as quarterly PCI Prioritised Approach audits on POA. Both audits examine PAM from slightly different perspectives and to varying degrees of detail. For example, the ISAE3402 audit report for the period 1 April 2019 to 31 December 2019 has a specific section on Remote Access in section 4.8.14 where all 3 required controls are reported as "No deviations noted." Furthermore, POA are periodically requested to contribute to internal Fujitsu corporate audits to support Fujitsu UK in attaining and maintaining a variety of certifications such as ISO27001, ISO9001 and ISO22301.

9 Conclusions

Remote Access is a term that can be used to describe a number of processes within HNG-x and the usage of the term varies.

In this report, Fujitsu has provided clarity and explained Remote Access in the context of Remote Connectivity and Privileged Access. Both of these capabilities are necessary for Fujitsu to deliver its contracted obligations.

Remote Connectivity enables specialist support staff to connect to the environment from remote locations. It has been designed to include multiple layers of authentication and control to ensure it is both effective and secure.

Privileged Access allows a restricted number of specialist support staff to make approved changes to the Production environment. The use of these elevated levels of access are documented as part of Change Control and require POL approval. In summary:

- the roles of Windows, Unix and Database Administrators are to keep the IT systems working as required so the HNG-x environment can function as needed;
- The APPSUP temporary role is used for non-balance impacting actions (such as stock unit associations, emergency branch opening, or monthly tidying of despatch reports). APPSUP is not used to correct branch balance discrepancies or to amend financial transactions;
- The Transaction Correction Tool is the only way that Fujitsu can insert transactions.

Important note: Please note that the Transaction Correction Tool is not to be confused with the POL Transaction Correction Process. As described above, the Transaction Correction Tool is a tool available exclusively to Fujitsu. The POL Transaction Correction Process refers to POL's exclusive ability to correct balance discrepancies.

Although there are no contractual requirements or processes in place with POL for Fujitsu to report on Privileged Access activities, the monthly Security Report that is provided to POL for the ISMF meeting includes information on all Privileged Access types mentioned in this report.

10 Recommendations

POL and Fujitsu have discussed the topics of Remote Access over the years and during recent meetings. A compilation of recommendations for improvement options arising out of these discussions is contained in Appendix A. This list in Appendix A collates the various action items into a single list so that POL and Fujitsu can work jointly to improve the Remote Access capabilities. The recommendations should be prioritised and the most relevant ones actioned as promptly as possible.

Fujitsu strives for continual improvement and is committed to having an open dialogue with POL on additional recommendations that could be further implemented where appropriate.

POL00030526

11 Information Distribution

This report and any enclosed materials (the "Audit Materials") are being provided to Post Office Limited ("POL") pursuant to POL's request for an audit of the HNG-x services Fujitsu provides (the "Audit"). The Audit Materials comprise work product prepared by Fujitsu pursuant to requests from POL. Fujitsu has confined this report to the specific requests from POL and accepts no responsibility for any other matters. The Audit Materials relate to the current HNG-x environment.

The Audit Materials are confidential and provided to POL for the sole purpose of the Audit. The Audit Materials may only be shared by POL with KPMG, the external auditors appointed by POL in connection with the Audit. POL shall take all necessary precautions to ensure that any Audit Materials are: (i) not used for any purpose other than the Audit and; (ii) not disclosed to any third party (apart from KPMG), without Fujitsu's express consent in writing. In particular, it should be noted that:

(i) the Audit Materials may contain highly confidential and sensitive information which, if disclosed, is likely to significantly increase the risk of cyber and engineering attacks on the HNG-x environment ;

(ii) the Audit Materials may contain personal data within the meaning of the General Data Protection Regulation ("GDPR"); and

(iii) any system architectural content may be subject to copyright and/or other intellectual property rights and cannot be shared or disseminated.

Prior to making any permitted disclosure of the Audit Materials (or any part thereof), POL shall provide Fujitsu with reasonable advance notice of such intended disclosure and shall permit Fujitsu the opportunity to redact information including but not limited to any privileged information, personal data and/or other commercially sensitive or proprietary content.

This report refers to various documents that are confidential and internal to Fujitsu. Such confidential documents are proprietary to Fujitsu and are not intended for sharing outside of Fujitsu. Fujitsu in no way waives or intends to waive confidentiality in these documents by describing, referring to, reproducing extracts of, or in any way referencing these documents in this report. Where extracts of such documents are reproduced in this report, redactions have been applied to protect personal and sensitive information.

The Audit Materials, or any part thereof, may not be altered or amended without Fujitsu's express consent in writing. Under no circumstances shall any Fujitsu personnel be named or identified in any reports or other documents created by POL based on information from the Audit Materials (or any part thereof). Attribution of any Audit Materials shall be to Fujitsu only.

Unless agreed specifically in writing to the contrary Fujitsu does not accept any duty of care or any other legal responsibility whatsoever to any person or entity in relation to this Report, any related enquiries, advice or other work. Any person who receives a draft or copy of this Report (or any part of it) or discusses it (or any part of it) or any related matter with Fujitsu, does so on the basis that he or she acknowledges and accepts that he or she may not rely on this Report or any related information given by Fujitsu for any other purpose.

POL00030526

Appendix A – Recommendations

POL and Fujitsu have discussed the component topics of Remote Access over the years and during recent meetings. A compilation of recommendations for improvement options arising out of these discussions is contained below. This list collates the various action items into a single list so that POL and Fujitsu can work jointly to improve the Remote Access capabilities. The recommendations should be prioritised and the most relevant ones actioned as promptly as possible.

Fujitsu strives for continual improvement and is committed to having an open dialogue with POL on additional recommendations that could be further implemented where appropriate.

Ref	Recommendation	Additional Notes
1	Fujitsu and POL should revisit the discussion on the deployment of SIEM	• Fujitsu and POL should revisit the discussion on the deployment of SIEM to determine if it would be a valuable technology to deploy to augment how Privileged Access is managed and monitored by Fujitsu • SIEM tools have many other potential benefits too • Any review of options will need to be mindful of the various change projects already underway between Fujitsu and POL
2	POL should decide if it requires any Privileged Access Management reporting	• POL should initially review the content already shared in the monthly Security Report • New requirements should be stated by POL and reviewed by Fujitsu • Recommendation 1 may be required to meet some requirements • Any review of options will need to be mindful of the various change projects already underway between Fujitsu and POL

3	Ways of working should be formalised where appropriate	• A number of the ways of working have evolved over time and are understood and agreed on the basis of emails and discussions
		• Important processes and procedures agreed in this way should be formally documented and any relevant contractual clauses or documents updated as needed
		• This should include:
		  ○ The POL and Fujitsu approval processes necessary to authorise the use of the APPSUP privilege or the use of the Fujitsu Transaction Correction Tool
		  ○ The SSC second person review process