Document Title:	PAM RAM ASSURANCE REPORT
Document Reference:	COM/MGT/REP/4818
CP/CWO Reference:	N/A
Abstract:	Response to POL PAM RAM External Assurance questions
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	Fujitsu Responders (POA)	See Dimensions for record

Table of Contents

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	20-Apr-2023	Approved for release	N/A

0.2 Review Details

Mandatory Review	
Role	**Name**
Fujitsu Responders	Fujitsu

0.3 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/ION/0001 *(DO NOT REMOVE)*	168.0	13-Feb-2023	POA Document Reviewers/Approvers Role Matrix	Dimensions (internal)
PGM/DCM/PRO/0001	4.0	14-Apr-2023	POA Document Control Guidance Note	Dimensions (internal)
Europe Business Management System – Information standard	10.0	09-Feb-2023	Europe Business Management System – Information standard	EBMS (internal)
COM/MGT/REP/4165	1.0	12-Feb-2021	RA Report	Dimensions (external)
ISAE3402 Report	N/A	21-Mar-2022	Description of Fujitsu's System of IT Infrastructure Services supporting Post Office Limited's Horizon application	Shared
SVM/SDM/PRO/4293	1.0	01-Aug-2022	Horizon Data Changes Process Work Instruction	Dimensions (internal)
POL: POL/HNG/CIS/001 SVM/SEC/POL/0005	4.0	13-Oct-2011	Community Information Security Policy for Horizon & Horizon Online	Dimensions (external)
SVM/SDM/SD/0016	6.0	07-Jan-2022		Dimensions (external)
SVM/SEC/PRO/0012	17.0	17-Mar-2023	Post Office Account User Access Guide	Dimensions (internal)
SVM/SEC/POL/4538	2.0	23-Mar-2023	POA Privileged Account Policy	Dimensions (internal)
SVM/SEC/PRO/4537	1.0	28-Jul-2022	POA Privileged Account Release Procedure	Dimensions (internal)
Europe Business Management System – Privileged Access Management Process	2.0	07-Dec-2022	Europe Business Management System – Privileged Access Management Process	EBMS (internal)
Europe Business Management System – Privileged Access Management Work	2.0	07-Dec-2022	Europe Business Management System – Privileged Access Management Work Instruction	EBMS (internal)

Instruction				
REQ/SIR/SRS/2605	12.2	03-Mar-2023	End User Compute Towers Responsibilities and Requirements for Horizon Anywhere	Dimensions (external)
DEV/GEN/MAN/0015	15.0	26-Sep-2022	Audit Extraction Client User Manual	Dimensions (internal)
REQ/GEN/ACS/4252	1.0	10-Jun-2021	ACCEPTANCE REPORT FOR HNG-X - Release 21.51 - Transaction Correction Tool – Decommissioning	Dimensions (external)
DES/APP/HLD/0029	4.0	07-Sep-2016	Audit Data Retrieval High Level Design	Dimensions (internal)
LST SYS.AUD Log example 21.03.2023	N/A	21-Mar-2023	LST SYS.AUD Log example 21.03.2023	N/A

0.4 Abbreviations

Abbreviation	Definition
AD	Active Directory
ARQ	Audit Retrieval Query
BRDB	Branch Database
EBMS	Europe Business Management System (Fujitsu internal documents) – a Fujitsu internal system managed by Fujitsu corporate
ISMF	Post Office Information Security Management Forum
LST	Live System Test
MFA	Multi-Factor Authentication
PAM	Privileged Access Management
POA	Fujitsu Post Office Account
POL	Post Office Limited
RAM	Remote Access Management
SAN	Storage Area Network
SOD	Segregation Of Duties
TACACS	Terminal Access Controller Access Control System
VPN	Virtual Private Network

0.5 Glossary

Term	Definition
Dimensions	Fujitsu internal Document Management repository
HNG-A	The HNG-X Counter Business Application adapted to run on Windows operating systems other than NT4, providing all of the functionality of the HNG-X Counter Business Application.
HNG-X	HNG-X was a project that replaced the Horizon message-based branch network with the Horizon on-line branch service. Also known as Horizon Online. This was rolled out in 2010.

0.6 Changes Expected

Changes

0.7 Accuracy

Fujitsu has endeavoured to ensure that the information contained in this report is accurate. Fujitsu accepts no liability for any loss sustained (however caused), as a result of any information contained 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 . This report is also subject to the Information Distribution statements in Section 9.

1 Purpose & Introduction

The purpose of this report is to provide responses to the 22 questions presented by POL to Fujitsu on 06 March 2023. These responses are based on Fujitsu's understanding of the questions presented by POL. The responses relate to the current HNG-X environment for which Fujitsu is responsible for PAM and RAM and seek to describe the position as at the date of issue of this document.

Although every effort has been made to avoid confusing technical jargon in this document, the very nature 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.

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.

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 9 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 and looks forward to a constructive dialogue with POL.

2 Background

On 06 March 2023, POL sent an email to Fujitsu titled "HIJ Remediation – PAM/RAM & Transaction Processing External Assurance". In this email POL stated, "please see below the areas that Post Offices wishes to cover in relation to PAM and RAM for which we need Fujitsu support and engagement." A table was included as follows – comprising 22 questions:

General Scope area	Specific Scope	Ref
Governance and Process	Documentation detailing processes to grant Privileged Access to system is in place (including processes for approvals, new joiner, changes in access and leavers	1.1
	Roles and responsibilities in the granting of Privileged Access are clearly identified and defined	1.2
	Management Information on the usage of Privileged Access is created and communicated appropriately	1.3
	Appropriate change management processes exist over any changes to this process	1.4
PAM General Controls	Process documentation exists for all known ways a user can be granted Privileged Access to the system	2.1
	Privileged access to each of the above categories is granted in accordance with the documented process, to appropriate users after appropriate approval	2.2
	Privileged access is only granted to authorised and appropriate personnel	2.3
	Privileged access is removed from leavers (by account disablement) in a timely manner following the user leaving	2.4
		2.5

	Where possible, privileged access is only granted for a set time, for a specifically documented task	
	Privileged access to each of the above identified systems, is via accounts with password settings in line with Post Office password policy	2.6
	There is a regular monthly review performed of all users with privileged access	2.7
	When privileged access is granted, there are logging & monitoring controls over what activity users perform; specifically § All transactional activity performed by privileged users is written to the audit log on the audit SAN § There is an adequate SOD between users with privileged access (as defined in the Fujitsu report [COM/MGT/REP/4165] & users access to audit log files (Audit SAN). § There are alerting controls over any changes to the audit log files and/or all access to the Audit SAN is read only	2.8
	The audit SAN has remote access disabled & only authorised individuals can access the Audit SAN locally	2.9
	Access to privileged generic or system accounts is appropriately restricted and monitored, specifically § All administrator accounts are individual where possible § Where generic or system accounts have to exist, access is restricted via an appropriately secured password § Where generic or system accounts are required to be used directly, this is appropriately approved via a 'break glass' approval	2.1o [sic]
	Any changes to Privileged access process and/or controls are subject to change management, including approval of changes by all required parties.	2.11
Remote Privileged Access	Remote access to the counter, does not allow a privileged user to create or amend basket transactions	3.1
	Remote access to BRDB, does not allow a privileged user to create or amend transactional records, except the functionality listed below by the APPSUP role: § File change § Change Counter data § Assisted roll over	3.2
	The Transactional Correction tool functionality has been deleted	3.3
	Remote Connectivity to HNG-A 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	3.4
Access Limitations and Reporting	Where Fujitsu staff with Privileged Remote Access are not UK based, appropriate security measures are in place to bring the access in line with UK based access practices	4.1
	No third parties / contractors have Remote Privileged Access	4.2
	A monthly security report is provided to POL by Fujitsu detailing information on all Privileged access in the month	4.3

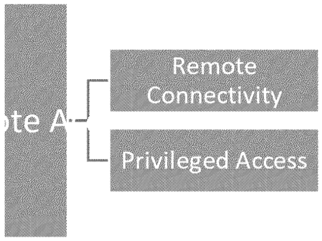
During a discussion with POL on 21 February 2023, where an early draft of the questions was shared with Fujitsu for discussion purposes, Fujitsu stated that it would prepare a report to respond to the questions identified by POL once they were formally submitted.

The spirit of the discussion between POL and Fujitsu in relation to this report was to share content that would allow both organisations to confirm the efficiency of the current ways of working together, and to identify any ways to make meaningful improvements. Fujitsu believes in collaboration and welcomes constructive suggestions from POL.

Terminology

In the “RA Report” [COM/MGT/REP/4165] Section 4 (extract here for ease of reference), Fujitsu provided clarity on terminology:

> “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.”



There are number of references within the questions POL has posed that Fujitsu wishes to map to these definitions so that its responses can be correctly interpreted.

Term used by POL	Fujitsu corresponding term
“Privileged Access”	Privileged Access
“privileged generic or system accounts”	Privileged Access
“Remote access”	Remote Connectivity
“privileged user”	Privileged Access
“Privileged Remote Access”	Remote Connectivity and Privileged Access
“Remote Privileged Access"	Remote Connectivity and Privileged Access

3 Types of Privileged Access

In the “RA Report” [COM/MGT/REP/4165] Section 7 (extract here for ease of reference), Fujitsu provided clarity on the types of Privileged Access required to support and maintain the systems that comprise the contracted responsibilities.

“In summary, it stated 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.”

Additionally, in Section 2 of the “Horizon Data Changes Process Work Instruction” [SVM/SDM/PRO/4293] Fujitsu explains the situations that mean it needs to make changes to data in the Live HNG-X System in Belfast.

4 Responses

Fujitsu has provided its response by appending a column to the table of questions provided by POL. Numerous references are made to the "RA Report" [COM/MGT/REP/4165] and ISAE3402 audit output titled "Description of Fujitsu's System of IT Infrastructure Services supporting Post Office Limited's Horizon application" (latest version dated March 2022). This report should therefore be read in conjunction with both these documents.

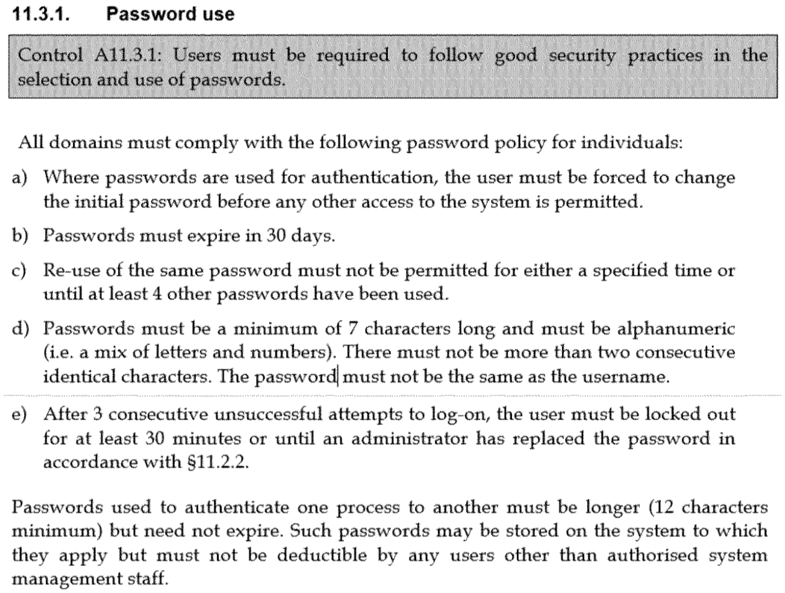
Fujitsu is currently being audited for ISAE3402 for the period 01 April 2022 to 31 December 2022 by Ernst & Young LLP for POL under CWO0703 with the report estimated for release in May 2023. Fujitsu understands that Deloitte is an ISAE3402 auditor and will be familiar with the depth and breadth of the control reviews needed to provide the responses for the ISAE3402 report.

General Scope area	Specific Scope	Ref	Fujitsu Response
Governance and Process	Documentation detailing processes to grant Privileged Access to system is in place (including processes for approvals, new joiner, changes in access and leavers	1.1	All access is granted as described in the "RA Report" [COM/MGT/REP/4165] Section 6.2. This was derived from the "Post Office Account User Access Guide" [SVM/SEC/PRO/0012] which provides more details on the steps taken and the alignment to the Fujitsu Europe Business Management Systems (EBMS) Privileged Access Management Process and Work Instruction. **This is within the scope of ISAE3402 (Control Objectives 10.1, 10.4, 10.5, 10.6 and 10.7).** Fujitsu also has a defined "Privileged Account Release Procedure" [SVM/SEC/PRO/4537] for providing access to Break Glass accounts. Usage of this procedure results in Break Glass account usage being reported on in the monthly Security Report (tab "Last Resort Password") that is provided to POL for the monthly ISMF meeting. The processes around the temporary granting of the APPSUP role are also defined in Fujitsu's "Horizon Data Changes Process Work Instruction" [SVM/SDM/PRO/4293] Section 5. POL has its own internal process document for Horizon Data Change which Fujitsu understands is titled "Horizon Support Approval Process vx.x" (latest version not known by Fujitsu).
	Roles and responsibilities in the granting of Privileged Access are clearly identified and defined	1.2	All access is granted as described in the "RA Report" [COM/MGT/REP/4165] Section 6.2. This was derived from the "Post Office Account User Access Guide" [SVM/SEC/PRO/0012] which provides more details on the steps taken. Section 3 of this document states all roles and the function they perform. **This is within the scope of ISAE3402 (Control Objective 10.4, 10.5 and 10.6).**

			Fujitsu also has a defined “Privileged Account Release Procedure” [SVM/SEC/PRO/4537] for providing access to Break Glass accounts which explains the roles applicable. The roles and responsibilities around the temporary granting of the APPSUP role are also defined in Fujitsu's “Horizon Data Changes Process Work Instruction” [SVM/SDM/PRO/4293]. POL has its own internal process document for Horizon Data Change which Fujitsu understands is titled "Horizon Support Approval Process vx.x" (latest version not known by Fujitsu).
	Management Information on the usage of Privileged Access is created and communicated appropriately	1.3	It is not clear what POL means by “Management Information on the usage of Privileged Access”. There is also no reference to this in the “Management Information Service: Service Description” [SVM/SDM/SD/0016]. Privileged Access is used by Fujitsu to perform its day-to-day obligations. Many of these obligations were described in the “RA Report” [COM/MGT/REP/4165] Sections 7.1.1, 7.2.1, 7.3.1, 7.4.1, and 7.5.1. The “RA Report” [COM/MGT/REP/4165] also described reporting in Sections 6.4, 7.1.4, 7.2.4, 7.3.4, 7.4.5, 7.5.5 and 8. This information is readily available to both Fujitsu and POL via the mutual service management toolsets. Question 4.3 below also seems related. Fujitsu provides POL with a weekly report of the users that have the Privileged Access as described in the “RA Report” [COM/MGT/REP/4165] Sections 7.1, 7.2 and 7.3. This is also provided as a monthly view as part of the monthly Security Report that is provided to POL for the monthly ISMF meeting (tab “PAM – Admins”). Fujitsu also provides a list of the occasions (with associated references) when POL permitted Fujitsu to temporarily grant the APPSUP role to stated Fujitsu specialist support staff. This is also shown in the monthly Security Report (tab “PAM – APPSUP”) that is provided to POL for the monthly ISMF meeting. Fujitsu also conducts an internal Team Access Review (see references in the “Post Office Account User Access Guide” [SVM/SEC/PRO/0012]) to ensure all access verifications have been received. It should be noted that there is no specific PAM tooling within the HNG-X solution.
	Appropriate change management processes exist over any changes	1.4	“This process” is understood to refer to those processes described in relation to question 1.1 above. Fujitsu's Europe Business Management System (EBMS) is subject to change control. The “Post Office

	to this process		Account User Access Guide" [SVM/SEC/PRO/0012] is held in Dimensions and is also subject to change control – showing version history, reviewers and feedback, and approvals. It can be seen in the documents provided with this response that there are "Document History" and "Change Control" sections showing iterations of the versions. POA uses Dimensions as its document management repository. Documents are maintained following the "POA Document Control Guidance Note" [PGM/DCM/PRO/0001] supported by the "POA Document Reviewers/Approvers Role Matrix" [PGM/DCM/ION/0001]. Fujitsu's EBMS document management is also governed by "EBMS – Information standard".
PAM General Controls	Process documentation exists for all known ways a user can be granted Privileged Access to the system	2.1	All access is granted as described in the "RA Report" [COM/MGT/REP/4165] Section 6.2. This was derived from the "Post Office Account User Access Guide" [SVM/SEC/PRO/0012] which provides more details on the steps taken and the alignment to the Fujitsu "EBMS Privileged Access Management Process" and "EBMS Privileged Access Management Work Instruction". **This is within the scope of ISAE3402 (Control Objective 10.1, 10.4, 10.5, 10.6 and 10.7).** Fujitsu also has a defined "Privileged Account Release Procedure" [SVM/SEC/PRO/4537] for providing access to Break Glass accounts which explains the processes applicable. The processes around the temporary granting of the APPSUP role are also defined in Fujitsu's "Horizon Data Changes Process Work Instruction" [SVM/SDM/PRO/4293]. POL has its own internal process document for Horizon Data Change which Fujitsu understands is titled "Horizon Support Approval Process vx.x" (latest version not known by Fujitsu).
	Privileged access to each of the above categories is granted in accordance with the documented process, to appropriate users after appropriate approval	2.2	It is unclear what "the above categories" refers to. However, all access is granted as described in the "RA Report" [COM/MGT/REP/4165] Section 6.2. This was derived from the "Post Office Account User Access Guide" [SVM/SEC/PRO/0012] and the Fujitsu "EBMS Privileged Access Management Process" and "EBMS Privileged Access Management Work Instruction". **This is within the scope of ISAE3402 (Control Objective 10.1, 10.4, 10.5, 10.6, 10.7, 11.2, 11.3, 11.4, and 11.6).**
	Privileged access is only granted to authorised and appropriate personnel	2.3	This question seems to overlap with question 2.2 above. All access is granted as described in the "RA Report" [COM/MGT/REP/4165] Section 6.2. This was derived from the "Post Office Account User Access Guide" [SVM/SEC/PRO/0012] which provides more details on the steps taken and the alignment to the Fujitsu "EBMS Privileged Access Management

			Process" and "EBMS Privileged Access Management Work Instruction". **This is within the scope of ISAE3402 (Control Objective 10.1, 10.4, 10.5, 10.6, 10.7, 11.2, 11.3, 11.4, and 11.6).**
	Privileged access is removed from leavers (by account disablement) in a timely manner following the user leaving	2.4	All access is removed as described in the "RA Report" [COM/MGT/REP/4165] Section 6.2. This was derived from the "Post Office Account User Access Guide" [SVM/SEC/PRO/0012] which provides more details on the steps taken and the alignment to the Fujitsu "EBMS Privileged Access Management Process" and "EBMS Privileged Access Management Work Instruction". **This is within the scope of ISAE3402 (Control Objective 10.5 and 10.6).**
	Where possible, privileged access is only granted for a set time, for a specifically documented task	2.5	All access is granted as described in the "RA Report" [COM/MGT/REP/4165] Section 6.2. Where possible, it is only granted for a set time - such as in the granting of the temporary APPSUP role. The processes around the temporary granting of the APPSUP role in Fujitsu's "Horizon Data Changes Process Work Instruction" [SVM/SDM/PRO/4293] Section 5 (the latest version was shared with POL on 04 August 2022 along with a recommendation that a format of this be added to the contract). POL has its own internal process document for Horizon Data Change which Fujitsu understands is titled "Horizon Support Approval Process vx.x" (latest version not known by Fujitsu). **This is within the scope of ISAE3402 (Control Objective 10.1, 10.4, 10.5, 10.6, 10.7, 11.2, 11.3, 11.4, and 11.6).** Fujitsu also has a defined "Privileged Account Release Procedure" [SVM/SEC/PRO/4537] for providing access to Break Glass accounts. Usage of this procedure results in Break Glass account usage being reported on in the monthly Security Report (tab "Last Resort Password") that is provided to POL for the monthly ISMF meeting. Accounts released under this procedure are for a set time and for a specifically documented task.
	Privileged access to each of the above identified systems, is via accounts with password settings in line with Post Office password policy	2.6	It is unclear what "the above identified systems" refers to, or what the "Post Office password policy" document reference is. The POL owned "Community Information Security Policy for Horizon & Horizon Online" document [POL: POL/HNG/CIS/001, SVM/SEC/POL/0005] is the current Contract Reference Document. Section 11.3.1 provides a reference to "Password use" as shown below:



11.3.1. **Password use**

Control A11.3.1: Users must be required to follow good security practices in the selection and use of passwords.

All domains must comply with the following password policy for individuals:

a) Where passwords are used for authentication, the user must be forced to change the initial password before any other access to the system is permitted.

b) Passwords must expire in 30 days.

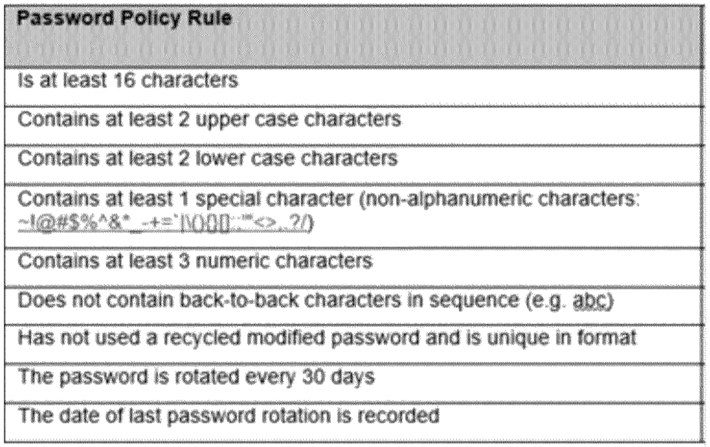
c) Re-use of the same password must not be permitted for either a specified time or until at least 4 other passwords have been used.

d) Passwords must be a minimum of 7 characters long and must be alphanumeric (i.e. a mix of letters and numbers). There must not be more than two consecutive identical characters. The password must not be the same as the username.

e) After 3 consecutive unsuccessful attempts to log-on, the user must be locked out for at least 30 minutes or until an administrator has replaced the password in accordance with §11.2.2.

Passwords used to authenticate one process to another must be longer (12 characters minimum) but need not expire. Such passwords may be stored on the system to which they apply but must not be deductible by any users other than authorised system management staff.

The following are the password rules POA implements for privileged accounts as documented in "POA Privileged Account Policy" [SVM/SEC/POL/4538]:

			 **Password Policy Rule** Is at least 16 characters Contains at least 2 upper case characters Contains at least 2 lower case characters Contains at least 1 special character (non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/) Contains at least 3 numeric characters Does not contain back-to-back characters in sequence (e.g. abc) Has not used a recycled modified password and is unique in format The password is rotated every 30 days The date of last password rotation is recorded
	There is a regular monthly review performed of all users with privileged access	2.7	This was described in the "RA Report" [COM/MGT/REP/4165] Section 6.2.3.2 "Privileged User Access Verification". All access is routinely validated monthly 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 **This is within the scope of ISAE3402 (Control Objective 10.6).** Fujitsu provides POL with a weekly report of the users that have the Privileged Access as described in the "RA Report" [COM/MGT/REP/4165] Sections 7.1, 7.2 and 7.3. This is also provided as a monthly view as part of the monthly Security Report that is provided to POL for the monthly ISMF meeting (tab "PAM - Admins"). Fujitsu also provides a list of the occasions (with associated references) when POL permitted Fujitsu to temporarily grant the APPSUP role to stated Fujitsu specialist support staff. This is also shown in the monthly Security Report (tab "PAM – APPSUP") that is provided to POL for the monthly ISMF meeting.

			Fujitsu also conducts an internal Team Access Review (see references in the "Post Office Account User Access Guide" [SVM/SEC/PRO/0012]) to ensure all access verifications have been received. It should be noted that there is no specific PAM tooling within the HNG-X solution.
	When privileged access is granted, there are logging & monitoring controls over what activity users perform; specifically § All transactional activity performed by privileged users is written to the audit log on the audit SAN § There is an adequate SOD between users with privileged access (as defined in the Fujitsu report [COM/MGT/REP/4165] & users access to audit log files (Audit SAN). § There are alerting controls over any changes to the audit log files and/or all access to the Audit SAN is read only	2.8	The "RA Report" [COM/MGT/REP/4165] described logging in Sections 7.1.2, 7.2.2, 7.3.2, 7.4.3, and 7.5.3. This question also appears to relate to: • Question 1.2 (roles & responsibilities and relationship to SOD) • Question 3.2 (transaction records) Fujitsu refers to the "audit log on the audit SAN" as the Audit Archive. Bullet 1 Fujitsu understands "transactional activity" to mean any actions taken on any Oracle production databases (not just BRDB) to amend branch transaction data by users with Privileged Access. All actions taken are logged to the SYS.AUD$ table which is then written to the Audit Archive. The actions that are logged are: LOGON; LOGOFF; SELECT; UPDATE; DELETE; INSERT; and EXECUTE (stored procedures). Using the LST system, each of these actions was taken on the BRDB IRRELEVANT), and the following was written to SYS.AUD$. LST was chosen to avoid unnecessary actions being taken on the Live system. The Live system would have recorded the same output. An example LST SYS.AUD$ log is shared with this response. The filename is "LST SYS.AUD Log example 21.03.2023.pdf". Please note that the user identity has been redacted and contains "XXXX". Bullet 2 Access to the Audit Archive is restricted to • Audit workstations (which have read only access to the Audit Archive and cannot be accessed remotely). This is described in "Audit Extraction Client User Manual" [DEV/GEN/MAN/0015] Section 7 – and is summarised here: ○ Audit workstations located at both the Bracknell and Stevenage Fujitsu offices. These machines are not connected to the Fujitsu network but have direct lines to the IRE11 and IRE19 Audit Servers. The Audit workstation implements the HDCR Windows 10 Secure Workstation build. Access to the Audit workstation is via two-factor authentication • Three groups exist for Audit workstation access: • Audit Users – the standard user account. Members of this group will be able to perform extraction and analysis of data held on the Audit system.

  - Audit Admin – grants access from the Audit workstation, to the operational area of the Audit servers to allow investigative and maintenance tasks to be performed.
  - Audit User Administrator – users in this group have administrator rights on the Audit workstations and in particular can run the card reconciliation tooling – see Section 11 “Card Reconciliation tool”.
- Audit Server – which writes to the Audit Archive – applying the delete protection attributes
- System administrators

Users with Privileged Access who perform “transactional activity” do not have the ability to amend the SYS.AUD$ table. The 07_DICTIONARY_ACCESSIBILITY is set to FALSE on Live databases:

```
SQL> show parameter O7_DICTIONARY_ACCESSIBILITY

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
O7_DICTIONARY_ACCESSIBILITY          boolean     FALSE
```

Refer to IRRELEVANT for additional information (Oracle website content shown below too).

“O7_DICTIONARY_ACCESSIBILITY:

Property	Description
Parameter type	Boolean
Default value	false
Modifiable	No
Range of values	true | false

O7_DICTIONARY_ACCESSIBILITY controls restrictions on SYSTEM privileges. If the parameter is set to true, access to objects in the SYS schema is allowed

> (Oracle7 behavior). The default setting of false ensures that system privileges that allow access to objects in "any schema" do not allow access to objects in the SYS schema.
>
> For example, if O7_DICTIONARY_ACCESSIBILITY is set to false, then the SELECT ANY TABLE privilege allows access to views or tables in any schema except the SYS schema (data dictionary tables cannot be accessed). The system privilege EXECUTE ANY PROCEDURE allows access on the procedures in any schema except the SYS schema.
>
> If this parameter is set to false and you need to access objects in the SYS schema, then you must be granted explicit object privileges. The following roles, which can be granted to the database administrator, also allow access to dictionary objects:
>
> SELECT_CATALOG_ROLE
>
> EXECUTE_CATALOG_ROLE
>
> DELETE_CATALOG_ROLE”

The APPSUP role does have "ANY TABLE" privileges (e.g. DELETE ANY TABLE/SELECT ANY TABLE etc) - but the role is only applicable to BRDB, and the role cannot DELETE from the SYS.AUD$ table due to Oracle parameter O7_DICTIONARY_ACCESSIBILITY being set to FALSE.

Bullet 3

To assure the integrity of the audit data while on the Audit Archive, the checksum seal for the file is re-calculated by the audit file sealer and compared to the value calculated when the file was originally written to the Audit Archive. The result is maintained in a check seal table. (as documented in the “Audit Extraction Client User Manual” [DEV/GEN/MAN/0015] Section 6.1.3).

Any discrepancies – which would indicate tampering or omission – are automatically detected and alerts are generated. This is described in “Audit Extraction Client User Manual” [DEV/GEN/MAN/0015] Section 8.

			Also, for branch transaction data queries, the data integrity checks are described as follows: *“The following integrity checks will be applied to the data* • *Completeness of data – contiguous message sequence numbers* • *Integrity of individual messages* ○ *…* ○ *For HNG-X data the message signature will be verified* *Separate Riposte & HNG-X summaries of the results of the integrity checks are generated. They should detail:* • *Summary of the message sequence runs broken down by counter Id. This should include start & end date/times and start & end message sequence numbers. Any gaps in the message sequence runs must be highlighted.* • *Summary of messages that have failed individual message integrity checks* *Any failure of the data integrity checks will not prevent subsequent execution of the query. The audit workstation user will be warned of the failure via the server process status notification mechanism.”* (As documented in the “Audit Data Retrieval High Level Design” [DES/APP/HLD/0029] Section 6.1.6).
	The audit SAN has remote access disabled & only authorised individuals can access the Audit SAN locally	2.9	It is not clear what POL means by "remote access disabled" and "can access…locally". Fujitsu use Remote Connectivity (as described in the “RA Report” [COM/MGT/REP/4165] Section 5) to gain access to systems - including the Audit Archive. The Audit Archive is not part of the HNG-X domain and access is via local logon once the user has remotely connected into the environment. Local logon to the Audit Archive is only available to the UNIX support specialists. Direct logon as “root” is part of the break glass process as the “root” account is centrally managed by SecOps. See question “2.1o” [sic] below for more detail on the break glass process and the reporting it generates. Access to the Audit Archive is restricted to

			• Audit workstations (which have read only access to the Audit Archive and cannot be accessed remotely). This is described in “Audit Extraction Client User Manual” [DEV/GEN/MAN/0015] Section 7 – and is summarised here: ○ Audit workstations located at both the Bracknell and Stevenage Fujitsu offices. These machines are not connected to the Fujitsu network but have direct lines to the IRE11 and IRE19 Audit Servers. The Audit workstation implements the HDCR Windows 10 Secure Workstation build. Access to the Audit workstation is via two-factor authentication • Three groups exist for Audit workstation access: • Audit Users – the standard user account. Members of this group will be able to perform extraction and analysis of data held on the Audit system. • Audit Admin – grants access from the Audit workstation, to the operational area of the Audit servers to allow investigative and maintenance tasks to be performed. • Audit User Administrator – users in this group have administrator rights on the Audit workstations and in particular can run the card reconciliation tooling – see section 11 “Card Reconciliation tool”. • Audit Server – which writes to the Audit Archive – applying the delete protection attributes • System administrators
	Access to privileged generic or system accounts is appropriately restricted and monitored, specifically § All administrator accounts are individual where possible § Where generic or system accounts have to exist, access is restricted via an appropriately secured password § Where generic or system accounts are required to be used directly, this is appropriately	2.1o [sic]	The “POA Privileged Account Policy” [SVM/SEC/POL/4538] states the policy that applies to all Privileged Access accounts. This is routinely validated to ensure that policy compliance is recorded. <u>Bullet 1</u> All administrator accounts are individual where possible. <u>Bullet 2</u> Generic and system accounts, and break glass are described in the “RA Report” [COM/MGT/REP/4165] Section 6.3. <u>Bullet 3</u> Fujitsu has a defined “Privileged Account Release Procedure” [SVM/SEC/PRO/4537] for providing access to Break Glass accounts. Usage of this procedure results in Break Glass account usage being

	approved via a 'break glass' approval		reported on in the monthly Security Report (tab "Last Resort Password") that is provided to POL for the monthly ISMF meeting.
	Any changes to Privileged access process and/or controls are subject to change management, including approval of changes by all required parties.	2.11	Fujitsu's Europe Business Management System (EBMS) is subject to change control. The "Post Office Account User Access Guide" [SVM/SEC/PRO/0012] is held in Dimensions and is also subject to change control – showing version history, reviewers and feedback, and approvals. The "POA Privileged Account Policy" [SVM/SEC/POL/4538] is also held in Dimensions and is also subject to change control – showing version history, reviewers and feedback, and approvals. It can be seen in the documents provided with this response that there are "Document History" and "Change Control" sections showing iterations of the versions. POA uses Dimensions as its document management repository. Documents are maintained following the "POA Document Control Guidance Note" [PGM/DCM/PRO/0001] supported by the "POA Document Reviewers/Approvers Role Matrix" [PGM/DCM/ION/0001]. Fujitsu's EBMS document management is also governed by "EBMS – Information standard".
Remote Privileged Access	Remote access to the counter, does not allow a privileged user to create or amend basket transactions	3.1	Fujitsu is not in control of live counter access permission: access permission to live counters is managed by POL's End User Computing (EUC) provider, DXC. Fujitsu's requirements for remote counter access are described in "End User Compute Towers Responsibilities and Requirements for Horizon Anywhere" [REQ/SIR/SRS/2605]. Fujitsu provides POL with a weekly report on Post Office Branch counter access made by its support specialists. This was delivered under CWO0574 – New Counter Access Report. The production of this report was incorporated into the Management Information Service (MIS), added into Section 2.1.6 'Reporting for Information Only' of the "Management Information Service: Service Description" [SVM/SDM/SD/0016]. "CCN1718 – Changes in Respect of Ongoing Provision of the Counter Access Report" was produced to formalise the update to the CCD. By way of further background, Fujitsu is aware that POL recently conducted a piece of work in this area as Fujitsu contributed under a Change Work Order (CWO0623 – Testing of branch counter Fujitsu Services remote support least privilege changes).

			Fujitsu also understands that POL is intending to “arrange, manage and carry out a PEN test” - as stated in the Post Office Responsibilities section of CWO0699 – Cygwin Counter Software Upgrade. Fujitsu is already assisting POL with this work.
	Remote access to BRDB, does not allow a privileged user to create or amend transactional records, except the functionality listed below by the APPSUP role: § File change § Change Counter data § Assisted roll over	3.2	The question seems to relate to Privileged Access and Fujitsu users that have been temporarily granted the elevated APPSUP role. It is not clear what POL means by “File change” or “Change Counter data”. To create or amend records in BRDB requires the temporary granting of the APPSUP Privileged Access role to the Fujitsu user. POL must approve the granting of the APPSUP Privileged Access. Fujitsu has a defined process for the use of the APPSUP role which has been agreed with POL and is documented in the “Horizon Data Changes Process Work Instruction” [SVM/SDM/PRO/4293]. The APPSUP role was described in the “RA Report” [COM/MGT/REP/4165] Section 7.4 and is further explained in Fujitsu's “Horizon Data Changes Process Work Instruction” [SVM/SDM/PRO/4293] Section 5 (the latest version was shared with POL on 04 August 2022 along with a recommendation that a format of this be added to the contract). POL has its own internal process document for Horizon Data Change which Fujitsu understands is titled "Horizon Support Approval Process vx.x" (latest version not known by Fujitsu).
	The Transactional Correction tool functionality has been deleted	3.3	The Transaction Correction Tool was decommissioned under release 21.51 on 13 May 2021 (CWO0425). POL was involved and provided sign off for the release on 11 May 2021. The “Acceptance Report For HNG-X - Release 21.51 - Transaction Correction Tool – Decommissioning” [REQ/GEN/ACS/4252] was issued 10 June 2021. Fujitsu confirmed to POL via email on 17 May 2021 that the Transaction Correction Tool was decommissioned, and POL HM Horizon IT Director responded to acknowledge this on the same day.
	Remote Connectivity to HNG-A 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	3.4	Please note the Glossary definition of HNG-A and HNG-X. Remote Connectivity meets the stated criteria and is performed as described in the “RA Report” [COM/MGT/REP/4165] Section 5.

	Access Control System (TACACS) § Console servers		
Access Limitations and Reporting	Where Fujitsu staff with Privileged Remote Access are not UK based, appropriate security measures are in place to bring the access in line with UK based access practices	4.1	Remote Connectivity is performed as described in the "RA Report" [COM/MGT/REP/4165] Section 5. This applies irrespective of the location of the user or whether they have Privileged Access or not.
	No third parties / contractors have Remote Privileged Access	4.2	Fujitsu uses contract staff (contractors) in addition to its full-time employees. Contractors are considered Fujitsu staff. They are granted the levels of access needed to perform their roles and are required to adhere to all applicable obligations and restrictions as full-time employees. Contractors, therefore, may have Remote Connectivity and Privileged Access to the HNG-X systems as applicable to their role. Fujitsu does not use any external third-party organisations to manage the HNG-X systems. Fujitsu does not control who POL grants access to in respect of its Post Office Cloud environment – where that comprises part of the Live HNG-X solution. Fujitsu does not control who Ingenico/Worldline grants access to in relation to their solution – where that comprises part of the Live HNG-X solution.
	A monthly security report is provided to POL by Fujitsu detailing information on all Privileged access in the month	4.3	There is no definition of "all Privileged access". In May 2021, POL requested a weekly report of the users that have the Privileged Access as described in the "RA Report" [COM/MGT/REP/4165] Sections 7.1, 7.2 and 7.3. Fujitsu continues to provide this on a weekly basis. This is also provided as a monthly view as part of the monthly Security Report that is provided to POL for the monthly ISMF meeting (tab "PAM - Admins"). POA also provides a list of the occasions (with associated references) when POL authorised Fujitsu to temporarily grant the APPSUP role to stated Fujitsu specialist support staff. This is also shown in the monthly Security Report (tab "PAM – APPSUP") that is provided to POL for the monthly ISMF meeting. Outside of these 2 reported areas, POL has not yet provided any specific requirements to Fujitsu for a formal response.

5 Formal Audit Reports

POL commissions annual ISAE3402 audits which cover several of the areas of interest in this report. References to the applicable Control Objectives within ISAE3402 have been made where possible. 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.

6 Conclusions

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 the Privileged Access types mentioned in the “RA Report” [COM/MGT/REP/4165]. Fujitsu also provides that information weekly as described in the response to question 4.3 above. Fujitsu also provides a list of the occasions (with associated references) when POL permitted Fujitsu to temporarily grant the APPSUP role to stated Fujitsu specialist support staff. This is also shown in the monthly Security Report that is provided to POL for the ISMF meeting.

7 Recommendations

POL and Fujitsu have discussed the topics of Remote Connectivity and Privileged Access on many occasions over the years and during recent meetings. A compilation of recommendations was provided in Appendix A of the “RA Report” [COM/MGT/REP/4165]. Progress has been made on all of the recommendations.

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.

8 Information Distribution

This report and any enclosed materials (the “External Assurance Materials”) are being provided to POL pursuant to POL’s request “HIJ Remediation – PAM/RAM & Transaction Processing External Assurance” (the “External Assurance Request”) – received by email on 06 March 2023 from POL. The External Assurance Materials comprise work product prepared by Fujitsu pursuant to questions from POL. Fujitsu has confined this report to the specific requests from POL and does not seek to address any other matters. The External Assurance Materials relate to the current HNG-X environment as at the date of the release of this document.

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

(i) the External Assurance 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 live HNG-X environment;

(ii) the External Assurance 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 External Assurance 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.

The External Assurance 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 External Assurance Materials (or any part thereof). Attribution of any External Assurance 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 External Assurance Materials, any related enquiries, advice, or other work. Any person who receives a draft or copy of this External Assurance Materials (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 the External Assurance Materials or any related information given by Fujitsu for any other purpose. Fujitsu accepts no liability for any loss sustained (however caused) as a result of any information contained herein.