POL00448344

Internal Audit Report

HNG-A: Privileged Access Management

Context

The Horizon IT system is used by Post Office Limited ("POL") to account for transactions in local Post Offices across the UK. Since the system was originally implemented in 1999, there have been several iterations of the Horizon system (the latest of which is known as "HNG-A"), provided and supported by vendor Fujitsu. In Figure 1 we outline the key HNG-A system components relevant for this internal audit. This report covers privileged access management for access managed by POL (Global IDs and Smart IDs) only and not Fujitsu managed access (see summary below for details).

Audit Objective

Internal Audit were asked by management to complete an independent review over the privileged access management (PAM) and Transactional Integrity (TI) for the system. This review was an in-year addition to the agreed FY23 internal audit plan and was delivered by an Internal Audit co-source partner who worked directly with management.

Audit Findings	
P1	5
P2	1
P3	0

Audit Rating

N/A

Not Rated

Conclusion

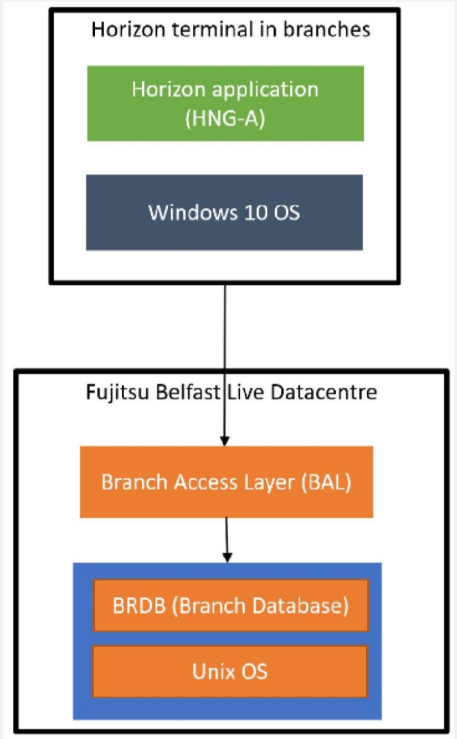
Due to a lack of cooperation provided to the fieldwork team by Fujitsu, who are responsible for managing privileged access to key components of HNG-A, several intended scope elements could not be completed. Specifically, Objective 1 of the audit (to assess the effectiveness of privileged access controls over the HNG-A system) could not be achieved. Further, whilst the scope included a set of analytics related to validating TI across a six-month dataset, this work could not be completed as a result (Objective 2: to understand and report on counter transaction success rates and reasons for transactional failure through analytical review of transaction metadata). Further, sampling of POL branches was limited at POL's request to a "friendly" branch list provided by POL's management team. **The overall audit rating is therefore "N/A – Not Rated"**.

As such, this report includes only findings related to privileged access controls over HNG-A operated by POL, specifically the management of Smart ID and Global IDs that provide sub-postmasters (PMs) and end user access to the HNG-A system. The table on Page 6 outlines the areas of scope that have, and have not, been tested with POL and Fujitsu.

POL00448344

This internal audit identified 6 key findings which relate to a lack of oversight and governance by POL over controls performed by third parties, lack of up-to-date policies & procedures, ineffective branch-level privileged access management, lack of robustness of user access review processes and an excessive number of Global IDs users with privileged access to account management and transactional activities across all branches.

Figure 1: HNG-A system: key components



Branch staff access HNG-A using a **Smart ID**. The branch PM has privileged access to manage users for their branch. Individuals at POL and third party strategic partners hold **Global IDs**, to allow them to perform activities across multiple branches, this includes setting up new branches and Smart IDs for new PMs.

The counter devices in the branch including the Windows 10 OS that the HNG-A application runs on is managed by third party DXC for Fujitsu's application and DB system.

The BAL is a middle-ware layer which sits between the HNG-A application and the database (BRDB). This component was agreed to be out of scope of the internal audit.

The HNG-A database server (BRDB) and the associated Unix OS is managed by Fujitsu.

Key:

Scope covered by this report	Scope element could not be suitably assured due to lack of third party cooperation	Out of scope

POL00448344

Executive Summary

Background

The HNG-A IT system is used by POL to account for transactions in local Post Offices across the UK. Since the system was originally implemented in 1999, there have been several iterations of the HNG-A system (the latest of which is known as "HNG-A"), provided and supported by vendor Fujitsu.

The HNG-A system is underpinned by a database ("BRDB"), and a number of UNIX-like servers. Branch counter terminals using HNG-A software are used to interface with the BRDB to write transactions to the database. All of these can be collectively considered to make up the broader HNG-A "system" ("the system") which is used by POL to capture branch transactions driving the company's accounting and finance data.

Objectives & scope

The table below sets out the objectives of the overall internal audit and the coverage provided by this report. These objectives are underpinned by scope areas described in the Summary of Findings on Page 6).

Objective	Coverage by this report
Objectives of this internal audit	
Objective 1 - To assess the effectiveness of privileged access management controls over the system. The system is comprised of the BRDB (including associated UNIX servers and Oracle DB instances), Branch Counter Terminals (including associated Windows Servers) and the HNG-A application running on the counter terminals. These controls should prevent the ability of non-privileged individuals to tamper with or erroneously modify transactional data. Remote access controls for these privileged users, including controls over remote access from the UK and the rest of the world, has also be included in the scope of the work.	Scope partially completed (see table overview on Page 6) - This report includes findings related to privileged access management controls operated by POL, specifically management of access to the HNG-A application layer. Due to a lack of cooperation provided to the fieldwork team by third parties responsible for managing privileged access to key components of HNG-A, internal audit has been unable to perform any work regarding controls operated by, or reliant on, Fujitsu.
Objective 2 - To understand and report on counter transaction success rates (i.e., transaction integrity) and reasons for transactional failure through analytical review of transaction metadata.	Scope not completed - This piece of work did not map to a specific contractual obligation between FJ & POL and was not pursued owing to FJ lack of willingness to engage in anything which wasn't explicitly mapped to the contract.
Objective 3 - To understand and report on the impacts on transaction integrity in the system given certain unique complications (specifically lack of receipt printing, power failure mid-transaction, and network failure mid-transaction).	Scope completed - This objective has been covered and observations related to this are included in this report.
Objective 4 - To understand and report on the effectiveness of specific Branch Reconciliation Team ("BRT") processes and controls as detailed in the scope. These controls should prevent inappropriate users from approving reconciliations and associated balancing transactions.	Scope completed - This objective has been covered and findings related to this are included in this report.

POL00448344

Executive Summary

Approach

Testing of identified controls was performed on a non-statistical sample basis. It is important to note that sample testing of the identified controls will not provide a definitive answer as to whether the data flowing through the system, or at rest in the system, is complete and accurate.

To complete this internal audit, the following steps were taken:

- Meetings were held with relevant stakeholders.
- We read and understood policy and process information provided by these stakeholders, relevant to the scope areas.
- Performed testing of controls, on a non-statistical sample basis as required.
- Consolidated and discussed findings emerging from the audit with relevant stakeholders.
- Produced a draft internal audit report.
- Completed walkthroughs on the model branch counter at POL HQ in London, to understand the impact on a test transaction for each scenario (lack of receipt printing, power failure mid-transaction, and network failure mid-transaction).

Conclusion

There are multiple access routes to the HNG-A system, with a range of individuals involved in the access control process. With multiple parties involved, it is vital to have a suite of up-to-date process and control documentation. During this internal audit it was observed that process and control documentation was not current and did not include key details such as what access POL deem to be privileged. Another key challenge identified for POL to address is to provide robust training on privileged access management, its importance, and the role of Post Masters (PMs) in managing access, to ensure PMs are suitably supported to operate effective privileged access management controls.

The impact of a lack of understanding of access control at a branch level was evidenced through multiple issues being identified in the six branches sampled, with individuals having access to branch HNG-A terminals and associated transactional processing privileges despite having left the branch, and individuals having been granted temporary privileged access which was not subsequently revoked.

Although processes and controls to govern Global IDs access management (those with access to HNG-A terminals in any branch and transactional processing tasks within, rather than specific branches) are more comprehensively documented in comparison to the branch-level, deviations from the process were identified for 5/25 access requests through this internal audit (including lack of sufficiently robust and attributable approval documentation, as well as approvals from individuals not on the authorised approvers list) and the number of users with privileged access to maintain Global IDs is considered excessive (over 300 users).

While POL doesn't directly manage privileged access to the back-end of the HNG-A system (i.e. the database and operating system layers), there is a lack of documentation and consideration of what is deemed privileged access at the database and operating system layers. The root cause of this is a lack of pro-active governance and monitoring over the services provided by, and controls operated by, third parties on behalf of POL.

POL00448344

Executive Summary

Whilst there is monitoring around privileged generic account ("APPSUP") logins (from third-party Fujitsu) being reported to POL, there were limitations in the reporting received by POL from Fujitsu. These limitations were the absence of completeness and accuracy checks completed by POL for monthly reports received from Fujitsu, and reporting being limited to logon events rather than comprehensive activity logs to support the APPSUP usage review. As part of this internal audit, it has not been possible to validate the completeness and accuracy of reports used for this emergency privileged access reporting. This is due to these emergency privileged access reports provided to POL by Fujitsu lacking information required to enable the internal audit to validate the completeness and accuracy of the reports (including a lack of sufficient detail on report parameters used and a lack of audit logging extracts for the usages reported on).

PLEASE NOTE: Due to a lack of Fujitsu personnel cooperation in supporting audit queries, the reported findings relate to the POL processes only. Our assurance work has not in any way considered the controls operated by Fujitsu to support this process. Further, sampling of POL branches was limited at POL's request to a "friendly" branch list provided by POL's management team, and so our assurance is limited to branches sampled from within this pool and does not provide assurance over the entire pool of POL branches leveraging the HNG-A system.

We would like to take this opportunity to thank POL's management teams for their cooperation and support during the audit planning, fieldwork and reporting.

Management Comment

I thank the team for this detailed audit on key elements of the way we manage access to our core trading platform. I note the comments around engagement with Fujitsu and reiterate that my position remains that I will be seeking assurances via the annual ISAE audit (the scope of which has been reviewed for this year).

I will be discussing the branch related findings with relevant colleagues to ensure we execute against the management actions below.

Simon Oldnall, Branch IT Director

POL00448344

Summary of Findings and Observations

The table below sets out the scope it has been possible to cover given the limitations arising from access restrictions to Fujitsu together with the observations mapped against the relevant scope area.

Finding	POL coverage	Fujitsu coverage	Finding and Observation Refs. & Priorities
Scope Objective 1 - To assess the effectiveness of privileged access management controls over the HNG-A system.			
Scope Area 1 - Privileged Access Management to HNG-A: Governance and documentation	Tested. Findings identified	Not tested	1 – P2
Scope Area 2 - Privileged Access Management to HNG-A: PAM general controls for POL managed privileges	Tested. Findings identified	Not tested	2 – P1 3 – P1 4 – P1 5 – P1 6 – P1
Scope Area 3. Remote Privileged Access Functionality	N/A – Fujitsu control	Not tested	N/A
Scope Area 4. Access limitations & reporting	N/A – Fujitsu control	Not tested	N/A
Scope Objective 2 - To understand and report on counter transaction success rates and reasons for transactional failure through analytical review of transaction metadata.			
Scope Area 5a. HNG-A transactional data analysis	N/A – Fujitsu knowledge required	Not tested	N/A
Scope Objective 3 - To understand and report on the impacts on transaction integrity in the system given certain unique complications (specifically lack of receipt printing, power failure mid-transaction, and network failure mid-transaction).			
Scope Area 5b. HNG-A Counter walkthroughs	Tested. Observations reported.	N/A – POL process	7 – Observation
Scope Objective 4 - To understand and report on the effectiveness of specific Branch Reconciliation Team ("BRT") processes and controls as detailed in SoW. These controls should prevent inappropriate users from approving reconciliations and associated balancing transactions.			

POL00448344

Detailed Findings and Agreed Actions

Scope Area 6. Branch Reconciliation Team (BRT) process & controls	Tested. Findings identified	N/A – POL process	6 – P1

POL00448344

Detailed Findings and Agreed Actions

Scope Area 1: Privileged Access Management to HNG-A: Governance and documentation

IT privileged access management control design should be underpinned by documented access management policies, procedures and controls.

For POL's HNG-A system, there is a split of responsibilities between POL and the third-party managed service provider, Fujitsu.

This report covers only POL-owned Privileged Access Management policies, procedures and governance arrangements for the HNG-A system. Fujitsu-owned Privileged Access Management policies, procedures and governance arrangements have not been considered given the lack of cooperation from Fujitsu personnel. Please refer to the table overview on page 6 for a detailed breakdown of scope coverage versus the original Statement of Work.

The detailed scope of this section of the work is outlined below:

a) Documentation detailing processes to grant privileged access to the system is in place (including processes for approvals, new joiners, changes in access and leavers).
b) Roles and responsibilities in the granting of privileged access are clearly identified and defined.
c) Management Information on the usage of privileged access is created and communicated appropriately.
d) Appropriate change management processes exist over any changes to this process.

POL00448344

1. Absence of regular policy updates and associated change management – P2

The POL HNG-A Access Control Policy v8.0 was reviewed, and it was noted that the document was last updated in 2009 (labelled for the previous iteration of the system, HNG-X). This indicates a lack of regular, review, update and approval of the document with associated policy change management procedures. The following critical elements of the policy document were not present:

- Which specific access layers exist for the HNG-A system – including Smart ID, Global ID, emergency APPSUP access, BRDB access and UNIX server access.
- Which specific roles are deemed privileged at each access layer (application, BDRB or OS – i.e., local Windows Servers in branch, Linux Servers underpinning the BRDB).
- The process for requesting, approving and assigning privileged access in relation to Smart ID user maintenance.

Whilst a separate inventory of the application-level roles available was observed, this document also did not define which roles within the inventory were deemed privileged.

The POL interim CISO at the time of testing suggested that Fujitsu may have additional up to date documentation (to which the fieldwork team have not had access) that may address some of the points above, however it is important that POL have documented procedures and governance in place to cover the processes and controls operating over their systems. In the absence of Fujitsu personnels' cooperation with audit fieldwork processes, no assurance can be given over this area.

Risk

Lack of clarity on access deemed privileged and the mechanisms at each access layer could lead to accidental elevated access ("privilege creep") and exploitable access mismanagement.

Suggested Management Actions

- Management should update the HNG-X Access Control Policy, modernising and refining the guidance within the latest iteration of the system, HNG-A. At a minimum this should include which specific access layers exist for the HNG-A system, which specific roles are deemed privileged for each access layer identified and why these roles are considered privileged.
- Management should implement an annual policy review process to refine and update the renewed HNG-A Access Control Policy, to reflect changes to the processes, role design and system architecture over time. This policy and procedures should be communicated and updates incorporated in relevant training materials.

Action Owner: Simon Oldnall, Horizon and GLO IT Director **Date:** 30 August 2024

POL00448344

Scope Area 2: Privileged Access Management to HNG-A: PAM general controls for POL managed privileges

The privileged access management controls in scope for this part of the internal audit were:

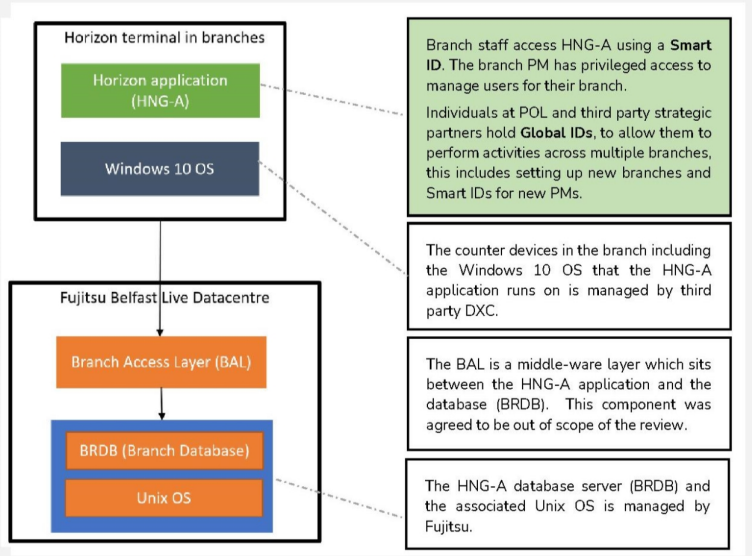
- Access provisioning and associated approvals by designated role owners
- Access deprovisioning and associated notifications from line managers
- Access review processes, including validation of all (including privileged) role assignments across the user base on a regular basis
- Logical security controls, to prevent unauthorised access to all (including privileged) accounts on the system
- Temporary elevated access controls (or "emergency access" controls) whereby highly privileged access is granted to a user for a strictly limited timeframe for a specific and approved purpose, after which the access is revoked and activity validated via audit log review

As shown in Figure 1 on the first page which is repeated for convenience on the right of this page, the privileges managed by POL are both the Smart IDs and Global IDs which are used to gain access to the HNG-A.

This report covers results from testing on the Global ID (cross-branch application level) and the Smart ID (individual branch application level) access layers **only**, shown in green on Figure 1. As such (with the exception of one emergency access related finding, identified based on POL visibility of the Fujitsu process) reporting is limited to the POL-led access management of these layers only.

For branch level testing POL provided a list of 12 branches (labelled, "friendly" branches by the POL management team) to sample from. From this small sub-set of branches a sample of eight was selected by Internal Audit, in line with the statement of work. Sampling was limited at POL's request to a "friendly" branch list provided by their management team, and so our assurance is limited to branches sampled from within this pool and does not provide assurance over the entire pool of POL branches leveraging the HNG-A system. POL's rationale for this selection was the existence of a good working relationship with the PMs of these branches, therefore these branches would be open to participating in the internal audit. The branches sampled for testing were Sunderland, City of London, Redditch, Musgrave, Jeanfield, Canary Wharf, WH Smith Liverpool and London Road. Due to the lack of response from branches WH Smith Liverpool and London Road and the recurring findings across the first six branches tested, no further testing was performed for WH Smith Liverpool and London Road. This is a very small and non-random sample. Results can only be drawn based on the sample provided and may not be representative of the wider branch network.

Fig. 1: HNG-A system: key components



POL00448344

2. Smart ID branch-level privileged access control limitations – P1

PMs are responsible for managing access at the branch level. Whilst they are provided with training to setup users for their branch, no training is provided on which roles are considered privileged. PMs responsibility for implementing and operating effective privileged access management controls was not well understood by the sampled branches.

As such, a number of inappropriate users were identified with privileged access at each sampled branch (as at time of testing, data obtained w/c 15th May 2023). Details of these users are as follows:

- At the Sunderland branch, one user account IRRELEVANT belonging to a prior cover manager remained active with the privileged IRRELEVANT role at the time of testing , despite having finished supporting the branch on 28 September 2022.
- At the City of London branch, one former employee was observed to have duplicate privileged (IRRELEVANT role) accounts IRRELEVANT and IRRELEVANT active on the system. The user had resigned in early May 2023.
- At the Musgrave branch, one privileged user with IRRELEVANT role access IRRELEVANT who had resigned in February 2023 remained active at the time of testing. Additionally, one user IRRELEVANT had inappropriately retained MANAGER access following a temporary role elevation to complete a specific task.
- At the Jeanfield branch, one privileged IRRELEVANT user account was identified as having retained access, despite a last login of February 2023. It was confirmed this account to a temporary branch manager position held in February 2023, with access not revoked from the branch subsequently.
- No exceptions were identified with regards to privileged Smart ID access for the Canary Wharf and Redditch branches.

This could undermine the TA and TC process, given the ability for these users to reset the passwords of PMs tasked with accepting reconciling corrections in the system. Direct testing of activity performed by users with privileged access is not in scope for this internal audit.

Risk

Exploitable elevated access levels at the branch level could undermine the integrity of the transactional data in the system and increase the risk of low-level fraud or error.

Suggested Management Actions

- Management should implement robust training on privileged access management controls covering at least (joiners, movers, leavers and periodic access review controls) its importance, and the role of PMs in managing access, to ensure PMs are suitably supported to manage their own branch's IT environment.

Action Owner: Melanie Park, Central Operations Director **Date:** 30 August 2024

POL00448344

3. Global ID cross-branch access management deviations – P1

Process documentation was observed outlining the process for granting new users access to the system, including a maintained list of access approvers. Despite this, at the Global ID (i.e., multi-branch user) level, the following deviations from the process were identified from testing a sample of 25 access requests:

- One access request was requested and approved by employees not present on the authorised list (user IRRELEVANT.
- One user had an account creation date (8 December 2022) prior to the request submission date (12 December 2022), suggesting that the account setup process had been circumnavigated with retrospective approval submitted (user IRRELEVANT).
- One user had access approved by an employee not present on the authorised list, and was granted highly privileged AUDITOR-E access in place of TRAINER access (user IRRELEVANT).

Additionally, repudiable digital signatures (typed into an Excel form) are used in place of a non-repudiable authorisation system. In the absence of a robust non-repudiable authorisation, request forms submitted for two out of the sampled 25 Global ID access requests did not include the named approver in the email communication (for users IRRELEVANT and IRRELEVANT). Further, it was identified from the role design documentation that the following roles have access to create and amend Smart ID users: IRRELEVANT; and "IRRELEVANT".

In total, 306 Global IDs had access to at least one of these roles IRRELEVANT 22 users; IRRELEVANT 146 users; IRRELEVANT 30 users; IRRELEVANT 45 users; IRRELEVANT 63 users). This volume of users with privileged access is considered excessive. Additionally, in contrast to the 63 admin users who have permissions to setup Global ID users, it was identified that there are only two HNG-A terminals from which this activity can be performed. The lack of terminals may impact POLs ability to setup Global ID users in case of an issue with these terminals. This could also undermine the Transaction Acknowledgement (TA) and Transaction Correction (TC) process, given the ability for these users to reset the passwords of PMs tasked with accepting reconciling corrections in the system.

Risk

Exploitable elevated access levels at the branch level could undermine the integrity of the transactional data in the system and increase the risk of fraud or error. Inability to sufficiently manage the Global ID creation process in case of issues with the only two terminals that can be used to setup Global IDs.

Suggested Management Actions

- Management should deploy a non-repudiable access approval system for HNG-A, or in the absence of this should require all named approvers to be sighted on related communications. Approvers should also consider the existing userbase with privileged access prior to approving additional requests.
- Review the role design to identify and remove excessive privileges, for example reducing the number of roles with access maintain user access, and significantly reduce the volume of users with privileged Global ID access.
- Management should seek to confirm that for the identified deviations, the accounts referenced hold the appropriate level of access in retrospect.
- Management should seek to expand the number of terminals capable of creating Global IDs.

POL00448344

Action Owner: Simon Oldnall, Horizon and GLO IT Director / Melanie Park, Central Operations Director	**Date:** 30 August 2024

POL00448344

4. Privileged and emergency access reporting limitations – P1

Privileged access reporting for POL managed access (Global ID and Smart ID)

There is no regular reporting on branch level privileged account activity, via Smart IDs or Global IDs, such as resetting user passwords or modifying of user roles.

Privileged access reporting for Fujitsu managed systems (HNG-A BRDB database and supporting operating system)

POL's management team have stated that Fujitsu regularly requires temporary privileged access to the operating system and the BRDB database that underpin the HNG-A application. This access is gained via the APPSUP account. Usage of this account is reported on by Fujitsu to POL security team members on a monthly basis. The following issues were identified with the reporting:

- Reporting on APPSUP usage was limited to ticket numbers, times and dates. Details of the activity performed by users whilst having access to this account are not reported.
- Reporting on the APPSUP process was provided directly from Fujitsu to POL. No first-line assurance mechanisms operate to validate the completeness and accuracy of the reporting.
- Report parameters are not provided to POL, with reporting pre-formatted by Fujitsu into a standardised template.

Risk

Incomplete and inaccurate privileged and emergency access reporting resulting in poor identification rates for exploitation of privileged access.

Suggested Management Actions

- Management should seek to engage Fujitsu to improve reporting on APPSUP account usage, to ensure that the identified data fields are included in future reporting packs.
- Management should seek to configure regular reporting on overuse of branch and cross-branch application level privileged access rights, including excessive password reset usage or user role modification.

Action Owner: Simon Oldnall, Horizon and GLO IT Director **Date:** 30 August 2024

POL00448344

5. Poor timeliness of ongoing and compliance with privileged access review and associated maintenance activities – P1

Smart ID user access reviews

At the branch level, PMs are expected to complete access reviews regularly given their role in managing access for the branch, however, these are not instructed or documented. Given the franchise model, individual Post Office branches are responsible for managing and notifying POL of leavers. In the absence of documented leaver records by the six sampled branches (Sunderland, City of London, Redditch, Musgrave, Jeanfield and Canary Wharf), All user accounts at each of these six branches were considered at the HNG-A Smart ID access layer, with a number of active leaver accounts identified (refer to Finding 2 for identified issues). The identification of missed leavers in Finding 2 suggests that these reviews are not occurring effectively for branch level Smart IDs.

Global ID user access reviews

POL state in the Community Information Security Policy for Horizon and Horizon Online (v4.0 provided for review) that complete user access reviews are completed on a 90-day basis, rather than monthly. Despite this, it was confirmed at the time of testing in March 2023 that reviews are carried out in practice over the Global ID user list bi-annually.

Review of the latest, at the time of fieldwork, post-bi-annual review Global ID List (dated 16 January 2023), confirmed that of 319 accounts:

- 17 users had not logged in for at least 6 - 12 months (last login between January 2022 and June 2022) but remained active and undeleted.
- 14 users had not logged in for 12 - 24 months (last login between January 2021 and December 2021) but remained active and undeleted.
- 24 users had not logged in for >24 months (last login before January 2021) but remained active and undeleted.

This analysis suggests undetected legacy access that has not been revoked from Global IDs during the latest or previous user access reviews.

Risk

Exploitable elevated access levels at the branch level could undermine the integrity of the transactional data in the system and increase the risk of low-level fraud or error.

Suggested Management Actions

- For Smart ID access reviews, management should seek to reiterate that branches perform robust privileged access reviews for users with access to their branch. POL should provide training and coaching to PMs as recommended in Finding 2.
- For Global ID access reviews, management should complete spot checks and ongoing first-line assurance activities to better reinforce the requirement to complete user access reviews effectively with access owners.

Action Owner: Simon Oldnall, Horizon and GLO IT Director / Melanie Park, Central Operations Director **Date:** 30 July 2024

POL00448344

6. Transaction Acceptance (TA) and Transaction Correction (TC) process for HNG-A counter transactions undermined by widespread privileged access – P1

Given extensive privileged access creep across the application (highlighted by the number of users with privileged Smart IDs and Global IDs, refer to **Findings 2 and 3** above) the appropriateness of those individuals with access to instruct and approve TAs and TCs could not be validated. Whilst an initial list of users with the ability to instruct TAs and TCs was viewed and validated, the approval of these at the terminal level in Post Offices across the country is dependent on PM approval of correcting entries. In the absence of sufficient branch-level privileged access management, there is widespread ability to access password reset functionality and account permissions management. There is therefore the potential for branch and central POL personnel to inappropriately compromise Smart ID and Global ID accounts with the ability to approve correcting entries, therefore system managed TA and TC approvals cannot be relied upon.

Further, manual approval for 1/25 TCs sampled could not be provided (TC No. 6000200534), and therefore mitigating manual controls were deemed insufficient to rely upon.

Risk

Exploitable elevated access levels at the branch level could undermine the integrity of the system driven TA and TC processes and increase the risk of low-level fraud or error.

Suggested Management Actions

- Management should implement the recommendations highlighted in **Findings 2 and 3**.
- Management should ensure that all manually documented TA and TC approvals are retained centrally, and available for audit. Retrospective approval should be obtained and retained for the transaction highlighted (TC No. 6000200534).

Action Owner: Melanie Park, Central Operations Director **Date:** 30 August 2024

POL00448344

7. Counter walkthrough results (Observations)

Note – These walkthroughs (of one example transaction for each scenario) were performed to provide observations on the system's operation in the model branch at POL HQ in London only. Our results comprise of observations made by the fieldwork team on the system's operation, and do not consider whether this operation is as intended by the system developer, Fujitsu, or by POL as the consumer of the system.

The below results relate to a specific request in the scope to perform the walkthroughs described and provide the results without a control conclusion. The observations made are reported below.

The following observations were made during each scenario test:

Lack of printer:

It was observed that for a transaction when the printer was disconnected, a transaction was still posted per the terminal, with the following terminal outputs displayed:

- The receipt printer is defective – "There was an error printing, unable to print."
- The receipt printer cover is open – "Print cover is open."
- There is no ink cartridge in the receipt printer – "Ink cartridge missing, insert ink cartridge to resume printing."
- The printer is not connected to the till system – "There was an error in printing....the printer is currently offli"e–""- "There was an error printing, unable to pri"t."
- The receipt printer cover is op–n"- "Print cover is op"n."
- There is no ink cartridge in The receipt print–r"- "Ink cartridge missing, insert ink cartridge to resume printi"g."
- The printer is not connected to The till syst–m"- "There was an error in printing....the printer is currently offli"e."
- The transaction was still visibly posted in the terminal.

Loss of power:

It was observed for a transaction whereby the power was suddenly lost that the transaction was still posted per the terminal on system restore, with the following terminal outputs displayed:

- On re-booting the system, the following message appeared: "A failure occurred during the previous session. Starting recovery process."
- On clicking continue, and the following two messages appeared in sequential order: "Please wait whilst the PIN pad is initialised." "Checking reference data integrity," "Recovery is complete."

POL00448344

Loss of network connection:

It was observed with a transaction whereby the network connection was suddenly lost that the transaction was posted after pressing the “retry” button on network connection being restored.

For an intermittent network issue simulation, the following was observed:

- The system hung on "Processing request" when the ethernet cable was unplugged and re-plugged continually.
- When the ethernet cable was permanently plugged back in when the following message was displayed "Press Retry or Cancel" was shown. Clicking "Retry" processed the transaction.

For a sustained network connection loss, followed by reconnection, the following was observed:

- "Processing request."
- After a few minutes the terminal displayed the following message:
- "Unable to contact the data centre to authenticate login details."
- When the cable was reconnected, the recovery is complete message was on logging back into the terminal, with the transaction posted.

Risk

N/A – observations reported as observed in line with Statement of Work.

Suggested Management Actions

N/A – observations reported as observed in line with Statement of Work.

POL00448344

Distribution List

	Name	Job Title
Executive Sponsor:	Simon Oldnall	Branch IT Director
Distribution:	Neil Bennett	CISO
Audit Team:	Internal Audit team members	Carol Murray – Partner Helen Cutting – Partner Lewis Keating – Director Matt Brennan – Senior Manager Tina Kitson – Manager Craig Dixon – Manager Sarah Oosthuizen – Senior Consultant
Key Dates:	ToR	23 January 2023
	Fieldwork	1 February 2023 – 9 June 2023
	Draft Report	16 June 2023
	Final Report	24 April 2024
	RCC	07 May 2024
	ARC	21 May 2024

POL00448344

Appendix 1 – Terms of Reference

Background:

The Horizon IT system (the latest version of which is known as "HNG-A") is used by Post Office Limited ("POL") to account for transactions in local Post Offices across the UK. Since the system was originally introduced in 1999, there have been several iterations of the Horizon system (the latest of which is known as "HNG-A"), provided and supported by vendor Fujitsu. Fujitsu has endeavoured to improve upon the system's previous technical capabilities and controls with each system revision. The CISO at POL engaged Internal Audit to complete an internal audit as an in-year addition to the agreed FY23 plan over privileged access management (PAM) for the system and Transactional Integrity (TI) of the system data.

Audit Objective:

The objectives of this audit was:

- To assess the effectiveness of privileged access management controls over the system. These controls should prevent the ability of non-privileged individuals to tamper with or erroneously modify transactional data. Remote access controls for these privileged users, including controls over remote access from the UK and the rest of the world, will also be included in the scope of the work.
- To understand and report on counter transaction success rates and reasons for transactional failure through analytical review of transaction metadata for a sampled six months.
- To understand and report on the system behaviour given certain unique complications (specifically for a walkthrough of one test transaction for each of the following scenarios: lack of receipt printing, power failure mid-transaction, and network failure mid-transaction).
- To understand and report on the effectiveness of specific Branch Reconciliation Team ("BRT") processes and controls as detailed in scope area 6 (under objective 4) on Page 6 of this report. These controls should prevent inappropriate users from approving reconciliations and associated balancing transactions.

The system in scope was the HNG-A system ("the system"). The system is comprised of the BRDB (including associated UNIX servers and Oracle DB instances), Branch Counter Terminals (including associated Windows Servers).

Timeline:

Pre-Work:	**12/01/2023**
Field Work:	23/01/2023 – 16/06/2023
Draft report:	30/06/2023
Final report	08/05/2024

Audit Team:

Internal Audit team members, including:

Carol Murray – Partner

Helen Cutting – Partner

Lewis Keating – Director

Matt Brennan – Senior Manager

Tina Kitson – Manager

Craig Dixon – Manager

Sarah Oosthuizen – Senior Consultant

Reporting:

We produced a report to management at the end of the audit and the results will be summarised for RCC and ARC meetings following the release of the final report.

POL00448344

Appendix 2 – Report and Finding Ratings

Report Ratings:

The specific rationale for the report opinion rating depended on a variety of factors including:

- The number of control issues identified
- The priority rating given to these issues
- The significance of the risks attaching to the area audited
- The overall status of the control environment for the business area audited

We categorised our report opinion according to the below rating criteria:

Rating	Description
Satisfactory	The framework of governance, risk management and control is adequate and effective.
Needs Improvement	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Needs Significant Improvement	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
Unsatisfactory	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

Finding Ratings:

Ratings*	Definition	Action Required
P1 (High Priority)	Significant weakness in governance, risk management and control that, if unresolved, exposes the organisation to an unacceptable level of residual risk.	Remedial action must be taken urgently and within an agreed timescale.
P2 (Medium Priority)	Weakness in governance, risk management and control that if unresolved exposes the organisation to a high level of residual risk.	Remedial action should be taken at the earliest opportunity and within an agreed timescale.
P3 (Low Priority)	Scope for improvement in governance, risk management and control.	Remedial action should be taken within an appropriate timescale that takes into account other priorities.

*Issue ratings are aligned to the HARM table defined in the Risk Policy, although professional judgement will be used where the risk maturity of the organisation does not provide for clear alignment.