POL00031727

KPMG

# Horizon audit

## Interim report into the progress made to address six HITJ Report issues

Post Office Limited

**Please be aware that this report does not yet include inputs from Fujitsu Solutions Limited*

**16 December 2020**

**V2.2 – Client draft release**

This interim report is provided pursuant to the terms of our contract with Post Office Limited (POL). The report is intended solely for internal purposes by the management of POL and should not be used by or distributed to others, without our prior written consent. To the fullest extent permitted by law, KPMG LLP does not assume any responsibility and will not accept any liability in respect of this Report to any party other than the Beneficiaries

# Contents

01 **Executive summary**
*A summary view of our current findings and reflects on the substantive issues that have emerged beyond those examined through the lens of Judgement No. 6.*

02 **Emerging observations**
*Our observations are summarised in this section. They are aligned to the six HITJ Report issues we are auditing.*

03 **Emerging observations in detail – mapped to themes**
*These observations are currently limited to our interactions with POL stakeholders.*
***As access to FJ is facilitated this section of report will be validated / clarified.***

04 **Appendices**
*Documents examined, stakeholders and meetings*

**Please note:**

- **Emerging observations relate primarily to the currently reviewed Post Office Limited (POL) elements of Horizon or POL's ability to view/manage identified elements of Horizon.**
- **At the time of drafting this interim report engagement with Fujitsu (FJ) has not been possible. Content is therefore the product of the evolving engagement with POL stakeholders only and review of FJ elements POL have been able to provide.**
- **It is anticipated that information from FJ will be available from mid January to mid February 2021, at which time this interim report will be validated and updated where necessary. As such the contents of this report may not accurately reflect the current state.**

DRAFT FOR DISCUSSION PURPOSES ONLY

# Context

## Context

Post Office Limited ("**POL**") is going through a major program of work to address historical failings in its core Branch computer system ("**Horizon**"). Horizon is used for transactions between POL and its Postmaster branch network, and is owned, maintained and managed by Fujitsu Services Limited ("**FJ**").

Postmasters raised issues with Horizon and these were linked to prosecutions and convictions of Postmasters for offences such as theft and false accounting.

In December 2019 POL settled with a group of claimants who established legal action against POL in response to their convictions. Following this settlement, the High Court ruled in the claimants' favour. In February 2020 a public inquiry ("**Inquiry**") was announced into the matter, with terms of reference and the appointment of a chair being announced in September 2020.

The terms of reference of the Inquiry include "whether lessons have been learned and concrete changes have taken place or are underway at Post Office Ltd", with respect to Judgment (No3) "Common Issues" and Judgment (No 6) "Horizon issues".

**Subsequent actions**

In response to the Judgement in October 2020 POL engaged KPMG LLP ("**KPMG**") to review progress made since the Judgement in 2019 and to provide recommendations against observations. The engagement was established to help POL report into the public inquiry; specifically, Judgement No 6, the Horizon issues, summarised on page 9. The content of this report was thus predicated upon KPMG's review against these six areas of concern.

## Scope

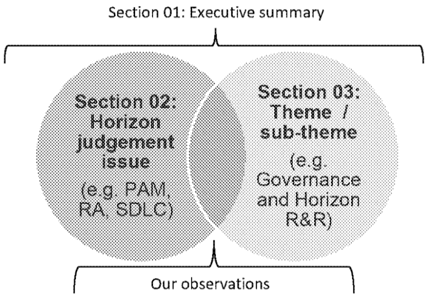
To provide an independent view of progress made to address previously identified failings categorised in Judgement No. 6 as the following six areas:

- Privileged Access Management
- Remote Access
- Software Development Lifecycle, Testing and Quality Assurance
- Known Error Logs – current
- Known Error Logs – historic
- Horizon Next Generation (HNGA) Robustness

## Structure

Section 1 introduces our report findings and key themes and a proposed remediation programme structure. We raise Fundamental Issues which we see as underlying issues which need to be addressed to prevent the improvements that are needed from being sustained. The main body of the report has two lenses for our observations, Section 2 provides a summary view based upon each of the above scope areas and Section 3 provides our detailed findings within key themes, mapped to the HIJT report.

Appendices 1 to 3 provide details of the documents, interviewees and meetings which have shaped our opinion in this report.


Section 01: Executive summary
Section 02: Horizon judgement issue
(e.g. PAM, RA, SDLC)
Section 03: Theme / sub-theme
(e.g. Governance and Horizon R&R)
Our observations

POL00031727

# 01

# Executive summary

This section provides a summary view of our current findings and reflects on the substantive issues that have emerged beyond those examined through the lens of Judgement No. 6.

*Please be aware that does not yet include inputs from Fujitsu Solutions Limited*

# Core message

**Change is happening, but fundamental issues remain to be addressed to effectively re-establish Postmaster trust.**

### The Inquiry demands change and (data) integrity

One of the central tenets of the Inquiry is that POL must change and be able to confidently assure Postmasters on the integrity of their branch data, and that POL must be able to provide externally assured confidence in the approach by key suppliers (or by itself). In short Postmaster trust must be re-established.

This requires POL to demonstrate it understands its Postmasters and the demands they face as the customer-facing sales force. It must be able to manage and address risk in the broadest sense of the business definition, both internally and, by extension of the approach, with its suppliers, and be based upon a stable platform within a supportive environment for its Branch network, be it direct or franchisee. It needs to make its business and that of its representatives safe, trusted, uncomplicated to run and accountable.

### Change is happening

POL's appointment of a GLO/Horizon IT Director and the building of a capability with a revised operating model to manage the Horizon IT estate and relationships is a clear signal of intent by the POL.

The team is assessing the current Known Errors in Horizon and has established a method of approach which both improves inclusion and alleviates the impact on Postmasters. Encouragingly, this signposts that the 'voice of the Postmaster' is central to C-level understanding of the need to accelerate change in what is a unique organisation, with a core social purpose.

### Fundamental issues remain

Our observations to date have established that there are fundamental issues which must be first addressed in order to effectively drive the change that is desired. This is critical in successfully landing the Strategic Platform Migration (SPM) currently being derived in a newly formed transformation unit. By way of illustration:

- The established organisational design and culture, and the way in which process and risk are managed in the areas identified within the Judgement means that governance and process gaps exist;
- The outsourcing of activity has affected the (assumed) delegation of accountability; and
- Individuals are primarily concerned with their own area of responsibility. There is no apparent challenge between siloed roles to broaden, connect or change this, thus no visible collective management of risk and controls.

Consequently, there is a lack of consistent, reliable management of Horizon; process, frameworks and approaches are not currently fit for purpose. Moreover, the Horizon operating model and that of POL which it interfaces with require significant attention to transform the Post Office into a successful and future-proof direct and franchise-based model. Our observations, therefore go beyond and behind the core findings of Judgement No. 6 as the two cannot be separated.

Two high-level illustrations of the reach of our observations are:

- Process – Section 9D – 3LOD. This highlights the lack of internal communication of the Judgement finding actions to relevant teams in the context of the need to address these at an operational level.
- Process – Section 14A – No User Acceptance Testing of Horizon releases is performed and the impact of change on branch users is not considered.

# Core message (cont.)

## There is more that needs to be done.

The main body of this report (Section 3) is categorised according to eight themes. They align to the GLO/ Horizon IT target operating model currently being designed and are split as follows:

| Organisational wide | Horizon service management |
|---|---|
| 1. Governance | 5. Data |
| 2. Capabilities | 6. Systems |
| 3. Processes | 7. Supplier and performance management |
| 4. Culture and conduct | 8. Technology |

We also provide a HITJ report issues view – this is found in Section 2 and summarised on page 9. Both point to Fundamental Issues (summarised on pages 7 and 8) which go to the core of POL being able to address the HITJ report issues. As such, significant further remediation is needed across all eight themes in order to address the six HITJ report issues and land the SPM. In effect, addressing the observed themes will allow POL to drive a successful business through its direct and franchise branch network.

**Implementation roadmap**

POL and the Horizon team are making progress. The immediate challenge however must be to ensure that any in-flight activities, such as the migration from Belfast and the underlying arrangements are assured as fit-for-future.

The workstreams we propose within the GLO/ Horizon IT target operating model are all critical to the delivery of SPM (see page 10). However, our concern is that there is limited value in commencing these if POL does not embrace the changes which have to originate from the parent body. Put simply, the new Horizon team needs the support of POL to succeed. Culture, roles, responsibilities, understanding of risk, processes cannot be sustained in isolation, nor can the interdependencies be ignored.

The proposed roadmap must start with an organisation
that collaborates internally as well as with its Branches and its vendors, and identifies areas of quick-fix and foundational change, such as:

- Establish an oversight board to coordinate and govern the programme.
- Identify interdependencies between POL, vendors and Horizon.
- Review, update and train staff in key roles of risk and governance.

In summary, the observations thus far point to issues which extend to people, process and technology at a POL-wide level, and whilst change can be effected within Horizon, POL must lead and follow the same path to succeed.

**Conclusion**

There is an apparent culture within POL which needs to adapt quickly, embracing a collective responsibility where changes, in areas such as vendor management, roles, responsibilities, process, training and technology, will endure within the new operating model.

POL needs to reflect its Social Purpose in its internal business engagement by adapting and maturing as an organisation to embed the improvements it is about to make within Horizon. It needs to ensure these are driven through its public-customer facing lens; that of the Postmasters, and these must be driven throughout the POL organisation. The following pages of this section expand upon this point.

***Please note, our conclusion will continue to develop following receipt of information from FJ, and in some cases may change as a result.***

# Fundamental issues

## Fundamental issues are present which go to the core of you being able to address the HITJ report issues.

Our report includes a set of broad-based observations or fundamental issues that must be addressed, without which any resolution of the wider observations will be unsustainable. They are summarised here and denoted throughout the report with this symbol ✱.

These Fundamental Issues have been uncovered throughout the Horizon investigation to date, however, it must be noted that it is highly probable that these issues are POL-wide, and may have a much wider impact than just within Horizon. It would be appropriate for POL to investigate further, to ensure that company wide policies, processes and approaches are in place, and that these are effective. This would validate that the expected management of other vendors, platforms and systems is taking place within the company.

Additionally, a number of Emerging Issues have been identified during the architectural review. These items do require further investigation, however, as they have the potential to cause serious problems that would align with the concerns of the Judgement, we have included them in this report for awareness. These are found on the following pages.

| #. Theme (as denoted in Section 4) | Narrative |
|---|---|
| 1. Governance | • The accountability, ownership and responsibility for all management and control aspects on Horizon is not clearly defined between POL, FJ and other vendors.<br>• Notable gaps exist in vendor management, service performance management and contract renewal. |
| 4. Regulatory Compliance | • KPMG has a concern that the lack of coordination in areas of Governance, above, and the absence of collaborative effort between monitoring and oversight of Horizon regulatory compliance and risk management is significant, which may have impacted POL's ability to meet its FCA/PRA obligations. POL and FJ have a programme in place to resolve a non-compliance issue regarding unencrypted PCI data, and GDPR PII requirements are not currently being met. |
| 8. Risk Management maturity | • POL's approach to risk assessment and management is unclear with regards to how IT operational risks are managed. This is compounded by concerns over the use and suitability of Archer as a tool to monitor, identify dependencies, aggregate risks and highlight potential impact. |
| 9. Risk Management at Three Lines of Defence (3LoD) | • The Second Line and Third Lines of Defence do not seem to work in coordination and appear to operate independently. Review and assessment of Horizon is provided by Fujitsu (via monthly reports); this self-assessment is not challenged by POL, and there seems to be no independent review of Horizon by POL 3LoD staff. Audits conducted by the third line of defence tend to be thematic rather than risk based, and do not delve into IT controls to determine the effectiveness of these controls.<br>• We observed that the judgement issues have not been shared with the second and third lines of defence, meaning that the items were not being tracked as corporate risks, or used as focus items for Internal Audit to examine. |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Fundamental issues (cont.)

| #. Theme (as denoted in Section 4) | Narrative |
|---|---|
| 10. Contractual Arrangements (Process) | • The strategic IT vendor management process is performed on an ad-hoc basis rather than at regular, set intervals. These ad-hoc reviews do not apply the latest business needs or re-evaluation of the required service levels against the contracts. |
| 13. IT Controls Framework (Process) | • The IT COBIT controls are not implemented at a meaningful and granular level, and the controls framework does not actually apply robust and effective controls to IT processes across delivery, operations, change management and vendor management. |
| 17. Ambiguous attitude to taking accountability, ownership and responsibilities especially for GLO remediation (Culture and Conduct) | • There appears to be a lack of understanding and/or acceptance of responsibilities and accountability across the POL landscape. Furthermore, the importance of process changes required from the Inquiry does not seem to be understood, and there is a lack of urgency to develop the appropriate response to the judgement items.<br>• Apart from within the GLO team, there appears to be no detailed planning to address the judgement findings.<br>• There seems to be little willingness to challenge vendors within supplier relationships, and the contractual management framework is trusted as being fit for purpose and is not challenged. |

**As stated on Page 6, the following section is specific to our emerging themes, which are reflective of the ongoing discovery of the Horizon and wider POL points of impact on Horizon. These are of sufficient note that even at the early stage of discovery, they have been included within this report.**

| Emerging issues | Narrative |
|---|---|
| "Non recoverable" or "lost" transaction types | • It is possible, in the current architecture, to begin the process of buying a product and then to exit from the process before payment is attempted. The fact that this process was initiated, and a basket created, is not captured or persisted (generally) until such time as the process is completed by making a payment. This means that certain products can be allocated and provided without there ever being a record that this was done. This feature of the architecture allows various undocumented work-arounds and has potential to be a vector for fraudulent transactions. |
| Branch workarounds | • There are various mechanisms within the Horizon platform that facilitate variations in the way Postmasters use the platform depending on their particular business situation. For example; where a Postmaster operates a retail shop and a Post Office Limited and has no separate EPOS system for their non Post Office Limited business, Postmasters may feel the need to use workarounds such as stamp reversals to allow them to use the Horizon platform and payments mechanisms to pay for stock items not supplied by the Post Office Limited for the sake of supplying a convenient single payment point for their shop customers. These processes and working practices have a high degree of risk associated since errors and accounting mistakes can easily be made and there are some variations on how these facilities are used. |
| Enfranchisement | • The franchise structure that POL has set up has to take into account the various types and formats of the POL counters (dedicated, mixed business, supplementary business, hybrid), however this does not seem to be the case. Our initial findings indicate that there is not an adequate and standardised base which can be used to build upon a complex, multifunctional organisation that can act in a consistent and reliable manner. For example, franchise post offices, when hiring staff, use their own contracts which are not necessarily POL templates or standardised POL contracts. This means that there is no consistency between POL's staff contracts.<br>• More investigation is required in this area. |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Horizon judgement issues

**There is a significant amount of additional remediation required to satisfy all six issues.**

Please note: Emerging observations relate primarily to the currently reviewed Post Office Limited (POL) elements of Horizon or POL's ability to view/manage identified elements of Horizon. At the time of drafting this interim report engagement with Fujitsu (FJ) has not been possible. Content is therefore the product of the evolving engagement with POL stakeholders only and review of FJ elements POL have been able to provide. It is anticipated that information from FJ will be available from mid January to mid February 2021, at which time this interim report will be validated and updated where necessary. As such the contents of this report may not accurately reflect the current state.

Observations are summarised here according to the six HITJ report issues. More detail can be found in Section 2.

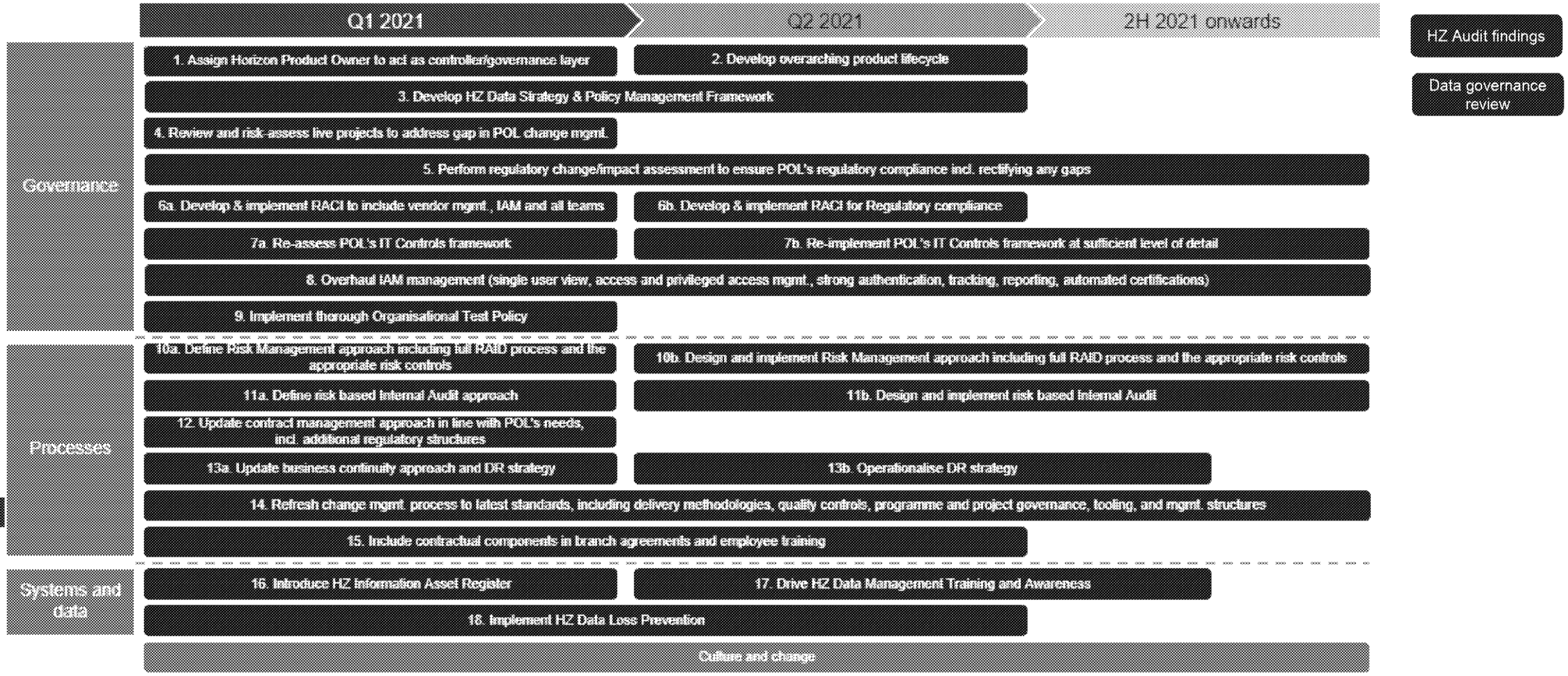
- **Privileged Access Management:** There is no notable progress on an approach to privilege or elevated access controls within the POL Horizon environment beyond basic user enablement and access. No tooling is deployed to automate and reduce human error. Moreover, there are scripts or applications that are used to resolve issues within Horizon for which do not use such controls either.
- **Remote Access:** The POL environments use limited controls around Remote Access and although a few operational changes have been implemented since the Judgement (post COVID) these do not represent an improvement in the overall profile for Remote Access, which remains sub-optimal.
- **Software Development Lifecycle, Testing and Quality Assurance**: Overall, the governance and control of the SDLC and Testing within POL is immature and requires immediate attention, with critical actions to take place as soon as possible. It is clear that limited focus has been applied to this area, and there have been no substantial or incremental improvements since the judgement in November 2019.
- **Known Error Logs (KELs) – current:** Whilst there has been definite improvement in the handling of current KELs, this progress has occurred recently, with the commissioning of a dedicated owner, with a support team, to take control of the KELs and drive them to conclusion. An updated and improved process is being implemented, and tighter controls have been put in place. Buy-in and commitment from the third parties has likewise improved.
- **Known Error Logs – historic:** Without more technical detail being supplied for each of the historic KELs it is not possible to determine if each of these items has been successfully resolved, or if they are still outstanding. Whilst POL has improved the tracking and monitoring of the historic KELs, there is still a large gap on the levels of information being supplied from the third parties regarding these KELs/ Without that information forthcoming, it will not be possible to conclusively close each of these items.
- **Horizon Next Generation (HNGA) Robustness:** This is a critical outstanding area; POL has not implemented the expected and required controls regarding robustness to give confidence that the Horizon platform is resilient and reliable. Currently there is too much reliance upon FJ and other vendors to handle robustness; this is not appropriate, and leaves POL in a high risk position, as each vendor may be monitoring and controlling their own scope, but the holistic and overall responsibility lies with POL.

POL00031727

DRAFT FOR DISCUSSION PURPOSES ONLY

# Implementation roadmap

**The suggested implementation approach is outlined below.**


Q1 2021
Q2 2021
2H 2021 onwards
HZ Audit findings
Data governance review
Governance
1. Assign Horizon Product Owner to act as controller/governance layer
2. Develop overarching product lifecycle
3. Develop HZ Data Strategy & Policy Management Framework
4. Review and risk-assess live projects to address gap in POL change mgmt.
5. Perform regulatory change/impact assessment to ensure POL's regulatory compliance incl. rectifying any gaps
6a. Develop & implement RACI to include vendor mgmt., IAM and all teams
6b. Develop & implement RACI for Regulatory compliance
7a. Re-assess POL's IT Controls framework
7b. Re-implement POL's IT Controls framework at sufficient level of detail
8. Overhaul IAM management (single user view, access and privileged access mgmt., strong authentication, tracking, reporting, automated certifications)
9. Implement thorough Organisational Test Policy
Processes
10a. Define Risk Management approach including full RAID process and the appropriate risk controls
10b. Design and implement Risk Management approach including full RAID process and the appropriate risk controls
11a. Define risk based Internal Audit approach
11b. Design and implement risk based Internal Audit
12. Update contract management approach in line with POL's needs, incl. additional regulatory structures
13a. Update business continuity approach and DR strategy
13b. Operationalise DR strategy
14. Refresh change mgmt. process to latest standards, including delivery methodologies, quality controls, programme and project governance, tooling, and mgmt. structures
15. Include contractual components in branch agreements and employee training
Systems and data
16. Introduce HZ Information Asset Register
17. Drive HZ Data Management Training and Awareness
18. Implement HZ Data Loss Prevention
Culture and change

Document Classification: KPMG Confidential

02

# Emerging observations

Our observations are summarised in this section. They are aligned to the six HITJ Report issues we are auditing.

POL00031727

# Horizon judgement mapping

**We have mapped our emerging observations against the Horizon judgement issues.**

For each emerging observation detailed in Section 4 we have themed them and provided a mapping to one or more of the six HITJ report issues we have been tasked with auditing. These are:

- Privileged Access Management
- Remote Access
- Software Development Lifecycle, Testing and Quality Assurance
- Known Error Logs – current
- Known Error Logs – historic
- Horizon Next Generation (HNGA) Robustness

On the following pages we provide a summary narrative for each HITJ report issue, pulling together multiple low level observations into higher level observations. In this table we list the number of themes mapped to each issue.

| HITJ report issue | # of themes mapped |
|---|---|
| Privileged Access Management | 4 |
| Remote Access | 2 |
| Software Development Lifecycle, Testing and Quality Assurance | 5 |
| Known Error Logs – current | 1 |
| Known Error Logs – historic | 1 |
| Horizon Next Generation (HNGA) Robustness | 1 |

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

# Privileged access management

**The observations that align to privileged access management are as follows.**

**Overall theme: - a low-maturity, inefficient and uncoordinated approach in all aspects of IAM, with no view of priorities/risk exposures, requiring immediate attention.**

| Theme | Sub-theme | Narrative |
|---|---|---|
| 1. Governance | 3. Identity administration, Access governance, Privileged and Remote Access (IAM) - Core systems and management | • No coherent approach to IAM exists, with high degrees of manual process and no consolidated source of truth for all users creating a sub-optimal process for all joiner-mover-leaver and certification processes.<br>• There are no policies, guidance or controls to manage or audit elevated access.<br>• There is a lack of visibility of vendors' users or activities including elevated and privileged users with differing processes and lack of correlation between user groups.<br>• Toxic combination and segregation of duties checks are not made upon user creation or rights elevation. |
| | 3. Identity administration, Access governance, Privileged and Remote Access (IAM) - certification and remediation | • Access review of all user types is inconsistent in timing and conducted 6-monthly for Global users, and within seven days for Global users leavers. No such process exists for Branch users.<br>• The lack of understanding of the Horizon estate inhibits risk-based good governance processes. |
| 3. Governance | 3. Identity administration, Access governance, Privileged and Remote Access (IAM) (Branches) | • Postmasters can create user types and have elevated function rights including password creation. No auditing or controls are driven by POL to limit the use of these rights. |
| 3. Process | 12. SmartID/Authentication | • Joiner-mover leaver processes are not defined, with leaver detection based primarily on inactivity, thus inactive users including those with elevated or privileged rights may continue to be active. This is a known issue in the Branch network for SMARTID users. |
| | 12. SmartID/Authentication (Branches) | • Leavers' accounts are left active by Branch managers with elevated rights, enabling user account sharing. |
| | 12. SmartID/Authentication | • The approval process for access rights does not have a four-eyes check approach for POL Global users and Branch users. |
| | 12. SmartID/Authentication | • There is no method of consistently enabling, monitoring, ceasing or auditing elevated and privileged access to ensure prompt and appropriate access. |
| 8.Technology | 23. Tooling – IAM & GRC | • POL makes minimal (tactical) use of its current commercial IAM tools and has no strategy for IAM/GRC. |

KPMG

DRAFT FOR DISCUSSION PURPOSES ONLY

# Remote access

## The observations that align to remote access are as follows.

**Overall theme: - there a lack of a consistent approach to authentication or a linkage to IAM (see Privileged Access) / remote access within the POL environment.**

| #. Theme | Sub-theme | Narrative |
|---|---|---|
| 1. Governance | Identity administration, Access governance, Privileged and Remote Access (IAM) | Inefficiencies in IAM governance results in inconsistent visibility or management of any user including those with remote access and a heavy reliance upon third parties' governance. |
| 2. Process | 12. SMARTID/Strong Authentication | Strong/multi-factor authentication is not used consistently, and weak passwords are used for all Branch users. A consistent approach is required to ensure identification of Global, third party and elevated users, particularly where credential theft is an exposure. |
| | 12. SMARTID/Strong Authentication | SmartID and password management processes for Branch users are not formalised and are communicated to relevant individuals via email. |
| | 12. SMARTID/Strong Authentication | There is no evidencable auditing of user activity. |

DRAFT FOR DISCUSSION PURPOSES ONLY

# SDLC, Testing and Quality Assurance

**The observations that align to SDLC, Testing and Quality Assurance are as follows.**

**Overall theme: - there is a complete lack of effective governance, control, management and ownership across the entire SDLC.**

| Theme | Sub-theme | Narrative |
|---|---|---|
| 1. Governance | 1. Horizon governance roles and responsibilities | • The accountability, ownership and responsibility for all management and control aspects on Horizon is not clearly defined between POL, FJ and other vendors, which leads to confusion and contradiction regarding change being delivered into Horizon. |
| | 2. Vendor management governance and oversight | • There are notable gaps in vendor management processes around service performance management and contract renewal, leading to "rogue" third parties acting on their own accord and making decisions for POL, without POL input or approval. |
| | 5. Test Governance | • There is no organisation Test Policy in place, and as such the test governance is fragmented and incoherent (e.g. quality gates are poorly enforced).<br>• Requirements traceability is incomplete or missing.<br>• There is a lack of a clearly defined test environment and data strategy. |
| | 6. SDLC Governance | • POL does not have a Project Delivery Capability Framework in place, and there is no standardised delivery methodology. Individual programmes can implement their own delivery mechanisms, which means that there is no consistency between ongoing programmes. Likewise governance and control varies from programme to programme. |
| 2. Capabilities | 7. POL Horizon capabilities | • There is a lack of POL in-house technical capabilities, which imposes heavy reliance upon a number of vendors to manage Horizon (i.e. FJ for architecture, development and testing; ATOS for reference data and testing), or short term contractors. POL have no capability to control the quality of technical delivery; they rely on third parties to fulfil this role. |

KPMG

DRAFT FOR DISCUSSION PURPOSES ONLY

# SDLC, Testing and Quality Assurance

| Theme | Sub-theme | Narrative |
|---|---|---|
| 3. Processes | 11. Product management | • There is no Product Owner for Horizon, and no product lifecycle is currently in place. This implies that there is no one single person with an overarching and holistic view of all the changes ongoing across Horizon, with a clear and concise understanding of how these changes impact POL's business and customer front end. Additionally, there is no single approver for these changes.<br>• The level of involvement from architects across Horizon change is limited; there is a poor understanding of the Horizon enterprise and system architecture. There is limited understanding within POL of how Horizon works, what it does, and how change can be effectively applied. |
| | 14. Testing | • POL does not perform appropriate and effective User Acceptance Testing or Non-Functional Testing.<br>• Regression testing is patchy and poorly applied to the platform. |
| | 15. Change Management | • POL does not have a clearly defined change management process that is applied across all change and all third parties. |
| 7. Supplier and performance management | 20. Vendor performance management | • Service Key Performance Indicators (KPIs) appear to be poorly defined with performance being self-reported by Fujitsu and no subsequent independent assurance activities being undertaken by POL as part of its own governance structure. |
| 8. Technology | 21. Tool Support for change delivery | • Spreadsheets are used to manage projects, as the use of DOORS and ALM having been discontinued. |
| | 24. AP-ADC Scripts allow uncontrolled change | • Automated Payments – Advance Data Scripts (AP-ADC) are used to make changes in Production & Reference Data. There are limited controls in place around this change, and most of the change implemented using these scripts is unrecorded. |

KPMG

POL00031727

DRAFT FOR DISCUSSION PURPOSES ONLY

# Known error logs (KELs) - current

**The observations that align to current KELs are as follows.**

**Overall theme: - Positive progress has been made in this area, with the implementation of a new process, and a dedicated team in place to handle the current KELs.**

| Theme | Sub-theme | Narrative |
|---|---|---|
| 2. Process | N/A | • POL have assigned a senior staff member, with a support team, to take ownership of the current KELs, to ensure that these outstanding items are appropriately managed, tracked and resolved. Additionally, a new process to manage KELs has been designed and is currently being implemented and embedded with all stakeholders. This process will be automated and coordinated via Service Now. Weekly reports are being produced to track the progress on resolving the current KELs, and there is oversight with a CAB in place. The CAB is staffed by the appropriate SMEs and people with the required seniority to make (and sign off on) decisions. Third party engagement is currently in place, and the third parties are onboard with the new process; teams within POL are likewise onboard and involved.<br>**This is a positive improvement.** |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Known error logs (KELs) - historic

**The observations that align to historic KELs are as follows.**

**Overall theme: - Without detailed technical information for the historic KELs it is not possible to determine if these items have been effectively resolved and can be considered closed. The investigation in this area is ongoing.**

| Theme | Sub-theme | Narrative |
|---|---|---|
| 2. Process | 16. KELs (Historic) | • KELs documentation lacks adequate details (particularly technical details for the issue and fix)<br>• KEL reports are not always consistent with status reports. |

POL00031727

DRAFT FOR DISCUSSION PURPOSES ONLY

# Horizon Next Generation (HNGA) Robustness

## The observations that align to HNGA robustness are as follows.

**Overall theme: - The investigation in this area is ongoing, and requires details to be supplied from the third party vendors. However, there seems to be a clear lack of ownership within POL, and no individual has been identified as having responsibility for the management and control of HNGA robustness.**

| Theme | Sub-theme | Narrative |
|---|---|---|
| 8. Technology | 22. Business Continuity Plan (BCP) / Disaster Recovery (DR) | • The SV&I test environment doubles as the DR environment. This is a high-risk solution and is not an effective DR strategy. The test environment is not an appropriate DR environment because code versioning would be different and may not be reflective of the production environment (e.g. missing integrations / applications, size and scale).Repurposing the test environment for DR could result in code conflicts, data issues and/or other code configuration issues which could invalidate certain test results. |

# 03

# Emerging observations in detail – mapped to themes

The observations detailed on the following pages are currently limited to our interactions with POL stakeholders. As access to FJ is facilitated this section of report will be validated / clarified.

DRAFT FOR DISCUSSION PURPOSES ONLY

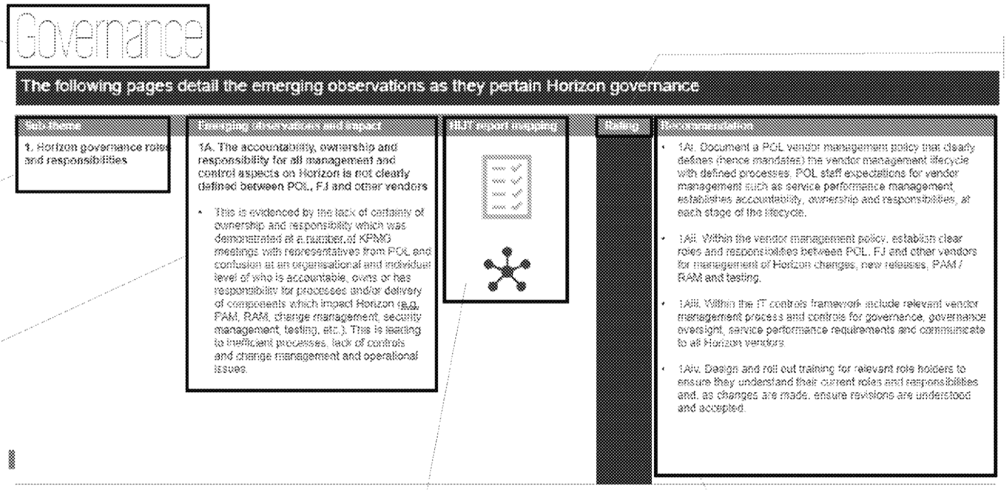
# How to use this section

The following pages include our emerging observations in more detail. Each page is set out accordingly.

These titles denote either an organisational wide or Horizon service management theme.

Here we break the high level theme into sub-themes.

Observations are provided here. They are followed by what evidence was observed to draw our conclusions.



## Governance

The following pages detail the emerging observations as they pertain Horizon governance

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| 1. Horizon governance roles and responsibilities | **1A. The accountability, ownership and responsibility for all management and control aspects on Horizon is not clearly defined between POL, FJ and other vendors**<br>• This is evidenced by the lack of certainty of ownership and responsibility which was demonstrated at a number of KPMG meetings with representatives from POL and confusion at an organisational and individual level of who is accountable, owns or has responsibility for processes and/or delivery of components which impact Horizon (e.g. PAM, RAM, change management, security management, testing, etc.). This is leading to inefficient processes, lack of controls and change management and operational issues. | | ■ | • 1Ai. Document a POL vendor management policy that clearly defines (hence mandates) the vendor management lifecycle with defined processes. POL staff expectations for vendor management such as service performance management, establishes accountability, ownership and responsibilities, at each stage of the lifecycle.<br>• 1Aii. Within the vendor management policy, establish clear roles and responsibilities between POL, FJ and other vendors for management of Horizon changes, new releases, PAM / RAM and testing.<br>• 1Aiii. Within the IT controls framework include relevant vendor management process and controls for governance, governance oversight, service performance requirements and communicate to all Horizon vendors.<br>• 1Aiv. Design and roll out training for relevant role holders to ensure they understand their current roles and responsibilities and, as changes are made, ensure revisions are understood and accepted. |

This is our rating based on a KPMG scale, as detailed below.

| Rating | Description |
|---|---|
| ■ | High risk issues or critical gaps identified. Immediate action required to rectify. |
| ▨ | Serious issues or major gaps identified. Rectification a high priority. |
| ░ | Minor issues or gaps identified. Mitigations planned, or in progress. |
| ▨ | No issues or gaps identified, area is on track. |
| ▨ | Area complete, or completing shortly. No issues or gaps identified. |
| ▨ | Not assessed during this review. |

Where possible we have mapped to the section of the HIJT report that is relevant.

PAM RA SDLC cKEL hKEL HNGA

Or, where the observation isn't specific to a section or is POL wide, we have used the following.

POL wide

Where recommendations are possible or appropriate we make them here.

KPMG

DRAFT FOR DISCUSSION PURPOSES ONLY

# Governance

## The following pages detail the emerging observations as they pertain Horizon governance

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **1. Horizon governance roles and responsibilities** | **1A. The accountability, ownership and responsibility for all management and control aspects on Horizon is not clearly defined between POL, FJ and other vendors**<br>• This is evidenced by the lack of certainty of ownership and responsibility which was demonstrated at a number of KPMG meetings with representatives from POL and confusion at an organisational and individual level of who is accountable, owns or has responsibility for processes and/or delivery of components which impact Horizon (e.g. PAM, RAM, change management, security management, testing, etc.). This is leading to inefficient processes, lack of controls and change management and operational issues. |  | ■ | • 1Ai. Document a POL vendor management policy that clearly defines (hence mandates) the vendor management lifecycle with defined processes, POL staff expectations for vendor management such as service performance management, establishes accountability, ownership and responsibilities, at each stage of the lifecycle.<br>• 1Aii. Within the vendor management policy, establish clear roles and responsibilities between POL, FJ and other vendors for management of Horizon changes, new releases, PAM / RAM and testing.<br>• 1Aiii. Within the IT controls framework include relevant vendor management process and controls for governance, governance oversight, service performance requirements and communicate to all Horizon vendors.<br>• 1Aiv. Design and roll out training for relevant role holders to ensure they understand their current roles and responsibilities and, as changes are made, ensure revisions are understood and accepted. |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Governance (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **2. Vendor management governance and oversight** | **2A. There are notable gaps in the vendor management process, with service performance management poorly defined and contract renewal treated in an ad-hoc manner.**<br>• This could result in misalignment with enterprise-wide vendor management expectations, non-compliance with regulatory requirements, regulatory criticism, penalties, fines and further reputational damage to POL. This was confirmed during discussions with POL representatives (29-Oct-2020 and 3-Nov-2020), no formal evidence has been supplied at this point in time..<br>**2B. The contractual management framework is trusted as being fit for purpose and is not challenged.**<br>• The contract management framework does not provide the required and expected contractual controls that a typical vendor contract should contain, and the boundaries on the third party are quite loose. There does not appear to be any challenge from POL staff regarding the contract and how is has been configured. This is evidenced by review of the provided "Contract Management Framework Final 2020" and during discussions with POL representatives (29-Oct-2020). | ☑<br>✱ | ■ | • 2Ai. Perform a gap analysis between the vendor management policy and the existing vendor management and service management processes. Identified gaps should be used to formulate process(es) and controls that should be implemented.<br>• 2Aii. Newly formed process(es) and controls should then be included in the IT controls framework, where they should be monitored, reported and self-assessed as per vendor management policy defined intervals (also please refer to recommendation 1Ai and observation 13A).<br>• 2Aiii. Vendor contracts should be updated to match and meet POL expectations of vendor delivery. Appropriate KPIs and SLAs need to be included within the contract.<br>• 2Bi. Review the existing Contractual Management framework against the 'National Audit Office Good practice Contract Management framework' and update the existing POL framework accordingly. |

# Governance (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **3. Identity administration, Access governance, Privileged and Remote Access (IAM)** | **3A. There is no coherent IAM approach for Horizon and POL's approach is forms driven, with no clear workflow that ensures each step of an overall process is linked, thus it is disconnected, manual and sub-optimal.**<br>**3B. Identity and Access management processes are disparate for different user groups such as Global Users and Postmasters, and are run by separate operational process.**<br>**3C. Governance and administration is heavily decentralised, and is owned by third parties. POL has no visibility into FJ IAM processes or how access to Horizon is granted to FJ-side operatives.**<br>• POL is therefore unable to provide assurance to one of the core findings of the judgement; integrity of data and thus confidence in the Horizon system, as it cannot demonstrate control over the risk of unauthorised or unaccountable access to critical infrastructure and systems. i.e. it cannot prove who has or had access to what. This was confirmed during discussions with POL representatives (9-Nov-2020 and 17-Nov-2020), no formal evidence has been supplied at this point in time. | 🔑<br>📱 | | • 3Ai. Improve the overall IAM posture of POL. Establish strong policy, controls and accountability for identity and access management for POL and third-party users. |

POL00031727

# Governance (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(…cont.)*<br>**3. Identity administration, Access governance, Privileged and Remote Access (IAM)** | **3D. Due to the decentralised model, there is no consolidated source of truth for internal or third-party users (Fujitsu, ATOS, CC).**<br>• This compounds POL's inability to create a consistent framework for IAM where joiners, movers and leavers are managed on a timely, easily audited manner; nor can POL maintain visibility into who has access to what across its branches nor supporting organisation and vendors.<br>• Without a single source of identity, correlation of users to system accounts is difficult as identity formats are inconsistent.<br>• Without this, POL is unable to change the current decentralised approach, nor correlate or control third party user activity itself. This was confirmed during discussions with POL representatives (17-Nov-2020), no formal evidence has been supplied at this point in time. | 🔑 | ■ | • 3Di.Maintain a single source of truth for all users or by user type (employees, non-employees, service accounts etc.) and have reliable correlation between accounts and users. Theme 23 Technology – highlights existing tooling which should be considered as a part of this approach. |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Governance (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(…cont.)*<br>**3. Identity administration, Access governance, Privileged and Remote Access (IAM)** | **3E. JML processes are inefficient and inconsistent across POL. Repeatable processes are identified in Global user access management, with gaps in mover and leaver handling.**<br>**3F. Postmasters create user types independently of Data Services team that manages Global User accounts and there is no apparent audit or control.**<br>**3G. Data Services places Global Access users into roles by a forms-based request with no access review for conflicting rights.**<br>• This is inefficient, prone to error and consequently falls short in providing a service to deliver an effective joiner-mover-leaver process for any user type. This can result in accumulation of access, violation of least privilege policy and insider threat. This was evidenced during discussions with POL representatives (5 Nov-2020, 17-Nov-2020) and review of email received (26-Nov-2020, 14:22) "RE: Global User Admin Access.msg". | 🔑 | | • 3Ei. Establish central and unified Joiner, Mover and Leaver processes, including immediate termination, with associated SLAs for users across branches, global users, and third-party users. |

**DRAFT FOR DISCUSSION PURPOSES ONLY**

# Governance (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(…cont.)*<br>**3. Identity administration, Access governance, Privileged and Remote Access (IAM)** | **3H. Branch Managers have full access to branch user management functions such as create Horizon accounts, manage passwords for these accounts. Elevation of user authority in branches is not audited or controlled by POL. POL user administration is inefficient and the expediency of an informal approach to allow a branch to run effectively is a known issue with no current practical resolution.**<br>• The ability to share accounts, creation of accounts with incorrect ownership, and use of such accounts to conduct transactions exposes franchise owners, branch management, staff and POL to the risk of accusations regarding inappropriate activities, albeit that the employer in the Post Office Limited-franchised branches is the business owner, i.e. the Postmaster. This was confirmed during discussions with POL representatives (3-Nov-2020), no formal evidence has been supplied at this point in time.<br>• Postmasters are currently provided with temporary access to global access roles (due to COVID remote help) which allows them elevated access. This was confirmed during discussions with POL representatives (17-Nov-2020), no formal evidence has been supplied at this point in time.<br>***Please also refer to 'Theme 12 - Process – SmartID'.*** | 🔑 | ■ | • 3Hi. Review and strengthen multi factor authentication processes. Implement MFA for branch users alongside/replacing SmartID. (Please see Theme 12 - Process – SmartID)<br>• 3Hii. Improve the audit and reporting capabilities for identity, password and account related activities.<br>• 3Hiii. Educate Branch owners and staff on the risks and impact of such activities and consider incorporating this into supporting staff contracts. |

**DRAFT FOR DISCUSSION PURPOSES ONLY**

# Governance (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(…cont.)*<br>**3. Identity administration, Access governance, Privileged and Remote Access (IAM)** | **3I. Within POL limited policies, no guidance or controls exist to manage or audit elevated access.**<br>**3J. Toxic combinations are not defined, especially for elevated access. POL defined roles such as Branch Managers, Auditor E and Admin do not have any Segregation of Duties (SOD) rules in the system. The creation process is paper based and does not check for SOD, and the recertification process does not check for adherence to joiner processes.**<br>• This exposes franchise owners, branch management, staff and POL to the risk of accusations regarding inappropriate activity, deniability of actions, misuse of privileges and to insider threat. This was evidenced during discussions with POL representatives (17-Nov-2020) and email received (26-Nov-2020,14:22) "RE: Global User Admin Access.msg". | 🔑 | ■ | • 3Ii.Improve current controls for elevated access usage, governance and adequate logging, monitoring and auditing for elevated access activity via automation.<br>• 3Iii Improve current processes to introduce maker-checker (four eyes) controls.<br>• 3Ji Review elevated access and identify toxic combinations. Establish strong SOD policies and a process to handle violations, exceptions and remediations. |

**DRAFT FOR DISCUSSION PURPOSES ONLY**

# Governance (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(…cont.)*<br>**3. Identity administration, Access governance, Privileged and Remote Access (IAM)** | **3K. Access review timings are not uniform and remediation tracking is not streamlined and mostly manual.**<br>• Bi-annual access reviews are conducted only for Global users, which include FJ users, by users' respective line managers. The window of exposure to accumulated privileges is between 6-12 months. This was evidenced during discussions with POL representatives (17-Nov-2020) and review of email received (24-Nov-2020) "FW: Global User accounts - removal from stock units.msg".<br>• Leaver checks for Global access are carried out weekly based on a report from HR, with remediation taking between 1 – 6 days resulting in residual access exposure of 7-14 days. This was confirmed during discussions with POL representatives (17-Nov-2020), no formal evidence has been supplied at this point in time. | 🔑 | | • 3Ki. Prioritise applications and define access recertification frequency, ownership and SLA's for access remediation.<br>• 3Kii. Reduce manual intervention in the access recertification and remediation process. |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Governance (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **4. Regulatory compliance** | **4A. There is an absence of collaborative effort between monitoring and oversight of Horizon regulatory compliance and risk management within POL.**<br>• A lack of regulatory compliance monitoring is in place to ensure compliance of POL and its vendors with regulatory requirements (e.g. GDPR, PCI DSS, DPA) which could result in significant fines, damage to reputation, possible withdrawal of services from financial services from partners, all of which would lead to significant loss of revenue and impact the sustainability of POL. This was confirmed during discussions with POL representatives (3-Nov-2020), no formal evidence has been supplied at this point in time. | ✱ | ■ | • 4Ai. POL need to assess, record and plan against the regulatory controls they are subject to ensure timely and appropriate compliance and clear statements on the consequences of non-compliance..<br>• 4Aii. Compliance approaches should be embedded within the appropriate operating models – Risk, operations etc<br>• 4Aiii. Establish clear responsibilities and plans for appropriately authorised individuals with pathways for escalation to leadership.<br>• 4Aiv. Review the IT risk management framework to establish regulatory compliance expectations to be identified, evaluated for risk and impact, escalated to leadership for awareness and remediation plans to be formulated. |

KPMG

DRAFT FOR DISCUSSION PURPOSES ONLY

# Governance (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(…cont.)*<br>**4. Regulatory compliance** | **4B. FJ are not meeting their GDPR regulatory requirements as Data Processors. FJ are dependent upon POL to provide strategic, organisational and formally documented and agreed ways of working - but cannot absolve themselves from being a Data Processor.**<br>• For both POL and FJ, this could result in non-compliance by POL leading to significant fines, damage to reputation and loss of trust by business partners. This was confirmed during discussions with POL representatives (16-Oct-2020), no formal evidence has been supplied at this point in time.<br>*(Please see Theme 18 – Personal Identifiable Information.)*<br>**4C. There is a lack of awareness within areas of POL the impact of financial services regulatory requirements surrounding Operational Resilience (OR).**<br>***This is flagged as TBA as KPMG is still investigating this but should be viewed along with Theme 22 – BCP/DR.*** | ✱ | | • 4Bi. Add to IT risk register whilst remediation plans are being implemented.<br>Please see Recommendations 18 i-iv – Personal Identifiable Information |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Governance (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **5. Test Governance** | **5A. No organisational Test Policy appears to be in place, and an overarching test framework does not seem to exist.**<br>• This results in inconsistent test approaches and processes being adopted across various projects and vendors, thereby increased testing effort and cost. This was evidenced during discussions with POL representatives (2-Nov-2020) and ATOS representatives (11-Nov-2020).<br>**5B. Test Governance is fragmented, and is applied inconsistently.**<br>• Little or no POL test governance over internal and third party test delivery. This leads to inconsistent quality, lack of coherent test outputs and delivery, and ambiguous results which cannot be verified or relied upon. This was evidenced during discussions with POL representatives (06-Nov-2020,12-Nov-2020) and ATOS representatives (11-Nov-2020).<br>**5C. Requirements traceability is incomplete or missing.**<br>• Without clear traceability in place it is difficult to determine if a requirement has been designed, built and then tested. This is evidenced by reviewing documents shared by ATOS representative (11-Nov-2020), and during discussions with POL representatives (30-Nov-2020). | ☑ | | • 5Ai. Create and implement an overarching organisation wide Test Policy which applies to all testing ongoing within POL, including any third party testing.<br>• 5Aii. Create and enforce a formal test framework, which outlines and determines the required test deliverables for each type of test engagement.<br>• 5Bi. Implement appropriate and effective test governance to ensure that all testing follows and adheres to POL's test framework.<br>• 5Ci. Traceability of requirements should be both mandatory, and automated via an appropriate tool. |

KPMG

# Governance (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(cont.)*<br>**5. Test Governance** | **5D. Lack of a clearly defined test environment and data strategy**<br>• The pathway to live for change is unclear, and how code is applied to the test environments appears to be inconsistent and uncontrolled. Whilst it is understood what each test environment should be used for, there doesn't seem to be a cohesive approach to managing the test environments. Likewise, test data is treated as an after-thought and does not appear to be controlled. This is evidenced by review of the provided "Edge Fujitsu Test Environment Review Report v1.1" and during discussions with ATOS representatives (11-Nov-2020) and POL representatives (06-Nov-2020,12-Nov-2020). | ☑ | | • 5Di. Implement and maintain a Test Environment & Data Strategy to ensure the appropriate management of the test environments and test data. This strategy should also cover the test environment components and support / operations (e.g. how batches are organised and executed, etc.). |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Governance (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **6. SDLC Governance** | **6A. POL does not have a formal Programme or Project Delivery Process**<br>• Whilst POL does have a formal Portfolio Management Process, it does not have a Programme or Project Delivery Process. The decision on which programme delivery methodology to use is inappropriately delegated to the individual programmes or projects. This was evidenced during discussions with POL representatives (29-Oct-2020, 2-Nov-2020).<br>**6B. Documents do not adhere to POL standard templates, and the quality of the documents varies greatly. Sign-offs for documentation also vary.**<br>• Without standardisation and appropriate quality standards in place test documentation is unreliable and may not contain required information. Furthermore POL is not obtaining a clear and precise understanding of any ongoing testing. This is evidenced by review of the provided "Test Strategy R1", "CM-POL-IT Change Management Policy v1.0", "POA-TSR-DM0119468 - Environment Agency - GDPR changes v0.3" - etc. | ☑ | ■ | • 6Ai. POL to implement a formal Programme and Project Delivery Process which outlines exactly how programmes and projects will be delivered within POL.<br>• 6Bi. POL to adopt standardised templates for all documentation that is produced by POL and its vendors. A document management process, and formal repository, should also be implemented, and applied across all change delivery within POL, and third parties. |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Capabilities

## The following pages detail the emerging observations as they pertain Horizon capabilities

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **7. POL Horizon capabilities** | **7A. There is a lack of POL in-house technical capabilities, which imposes a heavy reliance upon a number of vendors to manage Horizon (i.e. FJ for architecture, development and testing; ATOS for reference data and testing, Verizon for networks and infrastructure, etc.), or short term contractors. POL has no capability to control the quality of technical delivery; they rely on third parties to fulfil this role.**<br>• This could lead to lack of control over Horizon data, gaps in testing quality control, future litigations, regulatory criticism, fines, and reputational damage to the POL brand with Postmasters and the public. This was confirmed during discussions with POL representatives (16-Oct-2020, 29-Oct-2020 and 11-Nov-2020), no formal evidence has been supplied at this point in time. | ☑<br>✱ | ■ | • 7Ai. Establish a target operating model for Horizon and ensure this is supported by a complementary model in the broader organisation and by the vendors..<br>• 7Ai. Identify relevant skills and capability gaps.<br>• 7Aiii. Where capabilities are lacking, consider hiring or contracting the required capabilities to design and assure Horizon processes and testing, noting that good practice dictates these as separate functions.<br>• 7Aiv. The need for improvement in skills, capabilities and culture is one which needs to be addressed corporately as a part of the POL's strategy, feeding down into the various business areas, such as Horizon.<br>• 7Av. The POL strategy for change should drive a training and development programme for POL Horizon associated staff and those who will be relied upon to support Horizon in the wider POL business. |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Process

## The following pages detail the emerging observations as they pertain Horizon process

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **8. Risk Management maturity** | **8A. POL's approach to risk assessment and management is unclear as to how IT operational risks are managed. Currently there are 42 active risks with expected response dates ranging from 31 July till 1 December 2020.**<br>• This could lead to high risks not being identified and open risks not being addressed resulting in misalignment with POL's risk appetite, exposing POL to potential regulatory criticism including future reputational damage. This was confirmed during discussions with POL representatives (3-Nov-2020) and review of evidence provided (26-Nov-2020) "20201104 Security Risk.xlsx". | ✱ | ■ | • 8Ai. Establish a clear process for risk and dependency management with defined roles and responsibilities.<br>• 8Aii. Re-evaluate risk management processes to identify gaps and remediate accordingly. |

KPMG

DRAFT FOR DISCUSSION PURPOSES ONLY

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(cont.)*<br>**8. Risk Management maturity** | **8B. The inadequacy of the Archer risk management framework tool to track (e.g. date of risk identified), monitor, identify dependencies, aggregate risks and highlight potential impact makes Archer not fit for purpose for the size and complexity of POL.**<br>• This could cause failures in management of internal controls to provide complete and accurate reporting metrics leading to inefficient strategic and operational decisions being made by POL leadership. This was confirmed during discussions with POL representatives (3-Nov-2020) and review of evidence provided "20201104 Security Risk.xlsx" (26-Nov-2020). | ✱ | ■ | • 8Bi. Consider platform consolidation - for example, ServiceNow, to enable a single pane approach across all relevant teams and improved collaboration.<br>• 8Bii. Ensure agreed Risks, Assumptions, Issues and Dependencies (RAID) are tracked & maintained. |

KPMG

DRAFT FOR DISCUSSION PURPOSES ONLY

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **9. Risk Management at Three Lines of Defense (3LoD)** | **9A. The annual Service Organisation Controls Report ISAE3402 (SOCR) obtained from FJ reviews high level infrastructure controls and does not provide reasonable assurance for FJ managed controls over Horizon. The 3LoD do not review the report, challenge FJ on findings or self-assure that any findings are risk managed.**<br>**See also 9B.**<br>• This could result in lack of knowledge and awareness of FJ activities, insufficient management of FJ as a vendor, resulting in regulatory criticism, potential fines, reputational damage and possible further litigation against POL. This was confirmed during discussions with POL representatives (3-Nov-2020 and 5-Nov-2020), no formal evidence has been supplied at this point in time. | ✱ | ■ | • 9Ai. Second and third LoD to review all internal, external audit reports and controls reports initiated by POL or Horizon vendors. Any identified findings with potential risks to Horizon to be included in Archer, second LoD to discuss with first LoD and formulate actions to be taken and dealt with accordingly as a part of continual dialogue between first and second LoD.<br>• 9Aii. Second and third LoD to adopt a collaborated approach to strength the internal control framework at POL by holding open discussions regularly pertaining to all areas of Horizon.<br>• 9Aiii. Second and third LoD to leverage the findings from this interim report to agree roles and responsibilities between POL and Horizon vendors. |

KPMG

DRAFT FOR DISCUSSION PURPOSES ONLY

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(…cont.)*<br>**9. Risk Management at Three Lines of Defense (3LoD)** | **9B. Lack of self-assurance activities performed around Horizon with no apparent cohesion between POL's 3LoD.**<br>• This could result in lack of knowledge and awareness of FJ activities, insufficient management of FJ as a vendor, resulting in regulatory criticism, potential fines, reputational damage and possible further litigation against POL. This was confirmed during discussions with POL representatives (5-Nov-2020), no formal evidence has been supplied at this point in time.<br>***(Impact comment also applies to 9A)*** | ✱ | ▨ | • 9Bi. POL to consider external risk based internal audit training such as 'Fundamentals of Risk-based Auditing' by the Institute of Internal Auditors (IIA) or use professional services to deliver training to IA (Senior Management).<br>• 9Bii. IA to adopt a risk based approach to Internal Audits to initially create audit universe of all entities around Horizon and Horizon vendors (Also please refer to recommendation 9Ci).<br>• 9Biii. Subsequently IA to expand the audit universe to create all other entities within POL, create audit plans for the next 12 months to 3 years and provide assurance over controls for Horizon and broader POL.<br>• 9Biv. As part of the collaborated efforts between second and third LoD , third LoD to continually monitor emerging risks, conduct business monitoring, risk assessments and refresh audit plans accordingly. |

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(…cont.)*<br>**9. Risk Management at Three Lines of Defense (3LoD)** | **9C. Third LoD Internal Audit assurance activities are based on thematic reviews. These reviews do not include assurance over controls specifically around Horizon and POL IT Controls framework, thereby resulting in a lack of risk management activities and appropriately scoped reviews of in-house and outsourced controls around Horizon.**<br>• This could make it difficult for third LoD to satisfy regulatory requests, and to align third LoD with the first LoD to provide assurance over internal controls within POL. This was confirmed during discussions with POL representatives (5-Nov-2020 and 9-Nov-2020) and review of email response (19-Nov-2020, 15:43) "Project Iris - IA evidence requests". | ✱ | ▨ | • 9Ci. Third LoD IA teams to review and update current structure to reflect and mimic POL departmental structure – including as it evolves with changing operating model structures. This will assist IA to formulate entities and therefore formulate risk based IA activities including risk assessments.<br>• 9Cii. As part of the risk based audit activities, POL IA should concentrate efforts primarily on IA of Horizon and Horizon vendors. The review should include all identified judgement issues scope areas. |

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(…cont.)*<br>**9. Risk Management at Three Lines of Defense (3LoD)** | **9D. We observed that the judgement issues have not been shared with the second and third LoD.**<br>• This could result in misalignment between second and third LoD assurance activities, lack of collaborative efforts from all LoD at POL, lack of risk management, lack of knowledge and information sharing and insufficient controls and decision making to address GLO judgement issues. This was confirmed during discussions with POL representatives (3-Nov-2020 and 5-Nov-2020), no formal evidence has been supplied at this point in time. | ✱ | ■ | • 9Di. GLO to include second and third LoD in all discussions around judgement issues and planned remediation actions for risk management. Second and third LoD to input into the discussions and remediation actions to ensure any pending risks are captured and dealt with accordingly. |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **10. Contractual Arrangements** | **10A. The strategic IT vendor management process is performed on an ad-hoc basis rather than at regular, set intervals. These ad-hoc reviews do not seem to apply the latest business needs or re-evaluation of the required service levels against the contracts.**<br>• This has caused significant gaps between business needs and vendor provided services resulting in vendors not meeting with business expectations leading to Horizon performance issues. This was confirmed during discussions with POL representatives (29-Oct-2020), no formal evidence has been supplied at this point in time. | ✱ |  | • 10Ai. Determine the key issues and gaps within the service delivery, and address these core issues within the vendor contract.<br>• 10Aii. Implement appropriate and required SLAs to ensure that FJ meets POL's expectations when delivering support service regarding Horizon.<br>• 10Aiii. Implement POL process to assure and present challenge to FJ and other relevant vendors as a part of the revised operating model. |

KPMG

DRAFT FOR DISCUSSION PURPOSES ONLY

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **11. Product management** | **11A. There is no Product Owner for Horizon.**<br>• There is no single person responsible for ownership of the Horizon platform - i.e. with responsibility across change, operations, strategic vision, business support, etc.<br>• Updates are made based on requests by Business Product managers with limited oversight from POL IT on sequencing and prioritisation.<br>• These items were evidenced by discussions with POL representatives (22-Oct-2020 and 28-Oct-2020).<br>**11B. Level of involvement from architects is limited.**<br>• Late or inadequate engagement of a Solution Architect have resulted in poor documentation (including design documentation) thereby resulting in design issues/gaps. These was evidenced by discussions with POL representatives (22-Oct-2020). | ☑ |  | • 11Ai. POL should assign a Product Owner for the Horizon platform, with the remit of owning all change being implemented onto the platform.<br>• 11Bi. Mandate early and continuous engagement of enterprise and solution architects for any change across Horizon. |

KPMG

DRAFT FOR DISCUSSION PURPOSES ONLY

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **12. SMARTIDs/ Strong Authentication** | **12A. Multi-factor authentication is used by support staff but its use is not extensive – for example - SmartID consists of a four-letter identifier and a login of an additional two numeric digits (e.g. ABCD & ABCD01).**<br>• This does not provide a meaningful way of identifying users, thus sharing of logins and impersonation of users are is easily achieved , compromising auditability and security. This was confirmed during discussions with POL representatives (19-Nov-2020), no formal evidence has been supplied at this point in time. | 🔑 | ▨ | • 12Ai. Linking of POID to SMARTID should be unique and should be tied to personnel along with branch.<br>• 12Aii. Enable MFA for users where there is the potential for credential theft, and assess the benefits for extending this to Branch user access. |
| | **12B. Joiner Mover Leaver (JML) processes for SMARTID are not fully defined. Mover and leaver processes are reactive. Leaver detection is largely based on inactivity.**<br>• There is a lack of in-house POL controls or oversight on creation and use of SMARTIDs. This was confirmed during discussions with POL representatives (17-Nov-2020), no formal evidence has been supplied at this point in time.<br>• Dormant account policy is not efficient, based upon a 60 – 90 days' inactivity window. This was confirmed during discussions with POL representatives (17-Nov-2020), no formal evidence has been supplied at this point in time. | | | • 12Bi. JML processes for SMARTID must be defined, periodically reviewed and updated as necessary.<br>• 12Bii. Immediate termination of leavers is recommended for SMARTIDs as they provide critical access to Horizon and Branch hub.<br>• 12Biii. Assess current operations and identify opportunities for automation to improve efficiency and reduce human error. |

KPMG

DRAFT FOR DISCUSSION PURPOSES ONLY

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(…cont.)*<br>**12. SMARTIDs/ Strong Authentication** | **12C. It is known that inactive SMARTIDs are actively transacting.**<br>•In all of the observations, 12 A to C, the current process is demonstrably inefficient and error prone and does not provide adequate governance and control for the POL or managers to be able to assert and prove that only duly authorised individuals obtain appropriate access. This was confirmed by review of email received from POL representatives (21-Nov-2020) "RE: Document Evidence Request for POL - 20Nov2020_v0.2.xlsx ".<br>**12D. Though SMARTIDs are owned by personnel, logon information is shared via the branch managers' email addresses.**<br>**12E. Password management is solely owned by branch managers, and no process is identified for password management.**<br>•This is an exposure for franchise owners, branch management, staff and POL as it provides branch managers full access to Horizon IDs and SMARTIDs of their entire branch staff. This was confirmed during discussions with POL representatives (19-Nov-2020), no formal evidence has been supplied at this point in time. | 🔑 | ▨ | •12C. Refer to 12Bii.<br>•12Di. Until such time as the current process can be improved (emailing of user names and passwords), audit and notify changes to end user accounts to a checker identity, and ensure end users acknowledge changes to their account information.<br>•12Dii. Implement maker checker controls (manual or automated) for all JML actions undertaken.<br>•12Ei. Define and implement segregation of duties for elevated access roles such as Branch manager.<br>•12Eii. Establish strong controls over branch manager access. Ensure adequate logging, monitoring and auditing is enabled. |

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(...cont.)*<br>**12. SMARTIDs/ Strong Authentication** | **12F. Leavers' accounts remain available and are "useful" where staff replacements are waiting for their own accounts.**<br>• This could breach staff contracts or referenced policies on appropriate use, if these are in place, allowing staff who have not passed mandatory training to access Horizon and is likely to breach centrally developed policies, irrespective of whether these are communicated appropriately to Postmasters and their employees/staff. This was confirmed by review of email "Document Evidence Request for POL - 20Nov2020_v0.2.xlsx" provided by POL representatives (21-Nov-2020,10:31). | 🔑 | ▨ | • 12Fi. Check and address devolved policies and contracts, training and understanding for:<br>1. employment contracts for staff,<br>2. regulations and processes in particular for Postmasters (Direct and Franchisee), and<br>3. auditing of these at a branch level.<br>Consider these in the viewpoint of franchisee enablement (See S2. Emerging Observations - Enfranchisement)<br>• 12Fii. Refer to 12Bii. |

KPMG

DRAFT FOR DISCUSSION PURPOSES ONLY

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(…cont.)*<br>**12. SMARTIDs/ Strong Authentication** | **12G. Post-Covid, only one POL staff member from BSC can create, amend and delete SMARTIDs.**<br>• Single point of failure risk exists. This was confirmed during discussions with POL representatives (17-Nov-2020) and email received (18-Nov-2020) "FW: Post Office Limited Horizon discussions - follow up check".<br>• The process does not have a four-eyes approach to protect the individual and POL as a good governance process. This was confirmed during discussions with POL representatives (17-Nov-2020) and email received (18-Nov-2020) "FW: Post Office Limited Horizon discussions - follow up check".<br>***Please see Governance – IAM Section 3G onwards.*** | 🔑 | ▨ | • 12Fii. Refer to 12Bii.<br>• 12Gi. Ensure elevated / privileged access is approved, monitored, periodically reviewed and promptly remediated.<br>• 12Gii. Evaluate existing processes and identify single point of failure / risk and implement necessary interventions |

KPMG

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **13. IT Controls Framework** | **13A. The IT COBIT controls are not implemented at a meaningful and granular level, and the controls framework does not actually apply robust and effective controls to IT processes across delivery, operations, change management and vendor management.** | ✱ | ■ | • 13Ai. Update and extend the COBIT IT controls framework to include the required relevant control processes, documentation and objective control descriptions to implement effective controls across the IT landscape withing POL, including vendor supported applications. Design the controls accordingly to ensure the controls are granular, well understood by the staff performing CSAs, and are applicable to POL.<br>• 13Aii. Ensure that an independent and periodic internal audit of the IT Controls Framework is performed.<br>• 13Aiii. Finalise In–Scope Controls and periodically review the controls to ensure their relevancy is maintained. i.e. any aged or duplicate controls should be updated and/or removed<br>• 13Aiv. Enhance the IT Control reporting schedules, and ensure the reporting contains the required information to accurately determine the effectiveness and completeness of the controls.<br>• 13Av. Develop and implement the Controls Process Management document, and ensure adherence. |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(…cont.)*<br>**13. IT Controls Framework** | • The lack of an efficient IT Controls Framework could hinder management's ability to identify and address issues relating to functioning of internal controls, thereby resulting in delayed improper decision making which could potentially affect company's brand or reputation. This was confirmed during discussions with POL representatives (10-Nov-2020) and a subsequent review of the extracted controls "Copy of Risk and Control Matrix.xlsx". | ✱ | ■ | |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **14. Testing** | **14A. POL does not perform appropriate or comprehensive User Acceptance Testing.**<br>• Without appropriate UAT being performed there is no user validation of the change. Postmasters do not have exposure to the change until after it goes into Production, so there is little chance for them to comment or examine the change in detail prior to being forced to use it. This was evidenced during discussions with ATOS representatives (11-Nov-2020 and 8-Dec-2020) and POL representatives (30-Nov-2020). | ☑ | ■ | • 14Ai. A UAT phase should be Introduced as standard for all Horizon change. UAT should be conducted within it's own non-Production environment, post the completion of functional testing. |

KPMG

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **14. Testing** | **14B. The test environments are improperly managed and utilised, with single environments in use by multiple projects and test phases. Test data within the environments is not refreshed.**<br>• Conducting multiple test phases which have different test objectives in the same environment will result in environment conflict (e.g. different batches being run at the same time and on the same environment).<br>• Using obsolete test data can result in code conflicts, data issues and other code configuration issues which could invalidate certain test results.<br>• Additionally test analysts from different teams could attempt to use the same test data resulting in data conflicts.<br>• This is evidenced by review of the provided ”Edge Fujitsu Test Environment Review Report v1.1” and during discussions with ATOS representatives (11-Nov-2020, 8-Dec-2020). | ☑ | ■ | • 14Bi. Testing for each project should be carried out in dedicated environments with different data sets. The phases should be conducted sequentially (ST first, then SIT followed by UAT) and with robust entry and exit stage gates between these test phases. |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(…cont.)*<br>**14. Testing** | **14C. POL does not have an owner for Non-Functional Testing (NFT), and there is no overarching NFT approach.**<br>• The lack of POL ownership means that the third party vendors make their own decisions on NFT, which can leave POL exposed to risk. Additionally, without a POL NFT SME in place, validation and acceptance of NFT results is incorrectly delegated to the third parties; there is a risk that the required level of quality will not be met, and there is no independent validation of the results. This was evidenced during discussions with ATOS representatives (11-Nov-2020). | ✓ | ▨ | • 14Ci. POL to identify a NFT subject matter expert (SME) to take ownership of all non-functional testing, and govern third party delivery of NFT. |
| | **14D. POL do not have a standard set of Non-Functional requirements (NFRs) covering the Horizon platform.**<br>• Non functional aspects of the system cannot be designed, built and tested adequately thereby providing limited/no confidence around system robustness, performance, integrity and security. This was evidenced during discussions with ATOS representatives (11-Nov-2020). | | | • 14Di. Develop / identify a standard set of Non-Functional requirements which apply across the Horizon platform. |

KPMG

DRAFT FOR DISCUSSION PURPOSES ONLY

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(…cont.)*<br>**14. Testing** | **14E. The regression test suite should be enhanced and automated. Regression testing needs to be regularly executed across the Horizon landscape (at least monthly).**<br>• Without appropriate regression testing in place (and the regression suite being regularly executed) there is no guarantee of the stability of the platform after constant and ongoing change. This is evidenced by review of the provided "Rig 0094 - Regression Tests - Back Office", "Rig 0093 - Regression Tests - Front Office" " and during discussions with ATOS representatives (11-Nov-2020). | ☑ | ■ | • 14Ei. Enhance the current Regression test suite and automate the test scripts within the suite. This will enable the execution of consistent and continuous regression. |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **15. Change Management** | **15A. The POL change control process and framework is immature and poorly defined.**<br>• Not all change is governed by the change control process; some change is redirected to project work, some is not seen until after the change is implemented, some change occurs without passing through this process (e.g. Type X, the informal and undocumented relationships that exist between change initiators and change management).<br>• Due to the lack of a structured and formal framework, many of the decisions within the change management process are made subjectively and without consultation.<br>• Horizon change can come via non-IT projects; this change is sometimes unknown and does not pass through the change control process.<br>• This is evidenced by review of the provided "20200907 Horizon Governance Terms of Reference v1.0" and "CM-POL-IT Change Management Policy v1.0" and during discussions with POL representatives (27-Oct-2020).<br>**15B. Impact assessments of Horizon changes are irregular and inconsistent.**<br>• Inadequate impact assessments carry the risk that the impact of the change is not fully understood, and the change can have a more dramatic impact than expected. This was evidenced during discussions with POL representatives (27-Oct-2020, 30-Nov-2020). | ☑ | ▨ | • 15Ai. Uplift the Change Management Framework, Policy and Process Documentation to capture details on how the change process works (e.g. transition to different change status, objective risk assessment, impact assessments etc.) and ensure adherence by POL and all third parties.<br>• 15Bi. Enforce appropriate impact assessments, performed by POL experts and architects and technical staff. |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(…cont.)*<br>**15. Change Management** | **15C. The documentation provided by the third parties into the change process are limited, and do not adequately describe the change or the impact of the change. These documents are not appropriately challenged by POL.**<br>• Without clear and concise details, the full scope of the change cannot be understood, and there is a risk that the impact of the change may be wider than originally though. Additionally, without clear challenge there is no incentive for the third parties to provide more in-depth and accurate information. This is evidenced by review of the provided "20200907 Horizon Governance Terms of Reference v1.0" and "CM-POL-IT Change Management Policy v1.0" and during discussions with POL representatives (27-Oct-2020).<br>**15D. There is no obvious Design Authority type function.**<br>• Without a Design Authority in place to oversee changes or ensure they are consistent with Post Office Limited strategy, compliance or data governance, change can occur without oversight and appropriate review. This is evidenced by review of the provided 'Current Architecture and Forums.ppt' and during discussions with POL representatives (14-Dec-2020). | ☑ | ■ | • 15Ci. Enforce document standards, and challenge any documentation without an appropriate level of detail.<br>• 15Di. Implement a formal Design Authority, and ensure all change is appropriately routed through this group for review and analysis. |

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(…cont.)*<br>**15. Change Management** | **15E. There is no central change repository, which holds records of all change (historic and on-going).**<br>Changes, particularly to reference data and AP-ADC scripts, are not always persisted in a centralised repository which would allows oversight of change history and dependency management. Without this record in place, POL cannot determine the historical profile of change being applied to Horizon, or effectively analyse the impact of change to Horizon. This was evidenced during discussions with ATOS representatives (7Dec2020) and during discussions with POL Architects. | ☑ | ■ | - 15Ei. Set up a formal change repository, and require all change to be recorded and captured into this repository. |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Process (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **16. KELs (Historic)** | **16A. Historic KELs documentation lacks adequate details (particularly technical details regarding the issue, the cause and how it was resolved).**<br>- Without adequate details supplied, there is a level of confusion regarding whether or not the historic KEL has actually been resolved and is no longer impacting the Horizon platform. This is evidenced by review of the provided "Horizon Known Error Review ToR V1" and during discussions with POL representatives (06-Nov-2020,19-Nov-2020). |  |  | - 16Ai. Ensure complete technical details are sought from FJ. Once these have been supplied, an analysis of the historical KELs can be completed to determine if any are extant. |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Culture and conduct

## The following pages detail the emerging observations as they pertain Horizon culture and conduct

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **17. Ambiguous attitude to taking accountability, ownership and responsibilities especially for GLO remediation** | **17A. It is apparent that there is a lack of understanding, or a lack of acceptance, amongst general POL staff with respect to their accountabilities and responsibilities within their roles. This is especially apparent regarding implementing change to support the judgement issues**<br>• The abdication of responsibility, or lack of a sense of accountability, may cause challenges or delays to POL progressing with the required remedial actions. This is confirmed by discussions with POL representatives (21-Oct-2020, 23-Oct-2020, 29-Oct-2020, 30-Oct-2020, 3-Nov-2020 and 10-Nov-2020), no formal evidence has been supplied at this point in time. | ✱ | ■ | • 17Ai. Assign responsibility for the design and implementation of cultural change programme to address the cultural problems within POL.<br>• 17Aii. Update and refine the roles and responsibilities for managing Horizon risks and conduct appropriate training. |

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

# Culture and conduct (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(cont.)*<br>**17. Ambiguous attitude to taking accountability, ownership and responsibilities especially for GLO remediation** | **17B. Evidence of detailed planning, outside the GLO remediation team, to address the Horizon judgement findings appears to be missing. This is leading to a lack of urgency, awareness, drive and focus across POL to address the judgement items.**<br>• Implementation of the changes required to address the judgement issues may be delayed, unnecessarily challenged, or even resisted. This is confirmed by discussions with POL representatives (21-Oct-2020, 23-Oct-2020, 29-Oct-2020, 30-Oct-2020, 3-Nov-2020 and 10-Nov-2020), no formal evidence has been supplied at this point in time. | ✱ | ■ | • 17Bi. The comprehensive remediation plan for rectifying the Horizon judgment issues, and resolving the Horizon risks should be shared across the IT business unit, and wider as required. Backing and support from C-level executives may be required to enforce and insist upon implementation of the plan, and ensuring adherence to timelines and schedules. |

KPMG

DRAFT FOR DISCUSSION PURPOSES ONLY

# Culture and conduct (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| *(…cont.)*<br>**17. Ambiguous attitude to taking accountability, ownership and responsibilities for GLO remediation** | **17C. Willingness to challenge vendors within supplier relationship is lacking.**<br>- Without clear and appropriate challenge, vendors can go "rogue" - in effect, making decisions for POL which are not in POL's best interests, or take POL's risks into account. This is confirmed by discussions with POL representatives (27-Oct-2020 and 4-Nov-2020), no formal evidence has been supplied at this point in time. | ✱ | ■ | - 17Ci. Implement the new TOM, along with the appropriate vendor management and governance, with the required quality controls and SLAs, to empower POL personnel to appropriately challenge third parties. |

KPMG

DRAFT FOR DISCUSSION PURPOSES ONLY

# Data

## The following pages detail the emerging observations as they pertain Horizon data

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **18. Personal Identifiable Information (PII) at rest and in transit** | **18A. POL are not Payment Card Industry Data Security Standard (PCI DSS) compliant. Horizon contains PII data - managed by FJ - with data at rest and in transit not being encrypted.**<br>• If this breach in compliance is uncovered by the regulators, it could result in a formal finding of non-compliance with the Data Protection Act (DPA 2018) and General Data Protection Regulation (GDPR). This could result in high fines and reputational damage. This was confirmed during discussions with POL representatives (16-Oct-2020 and 12-Nov-2020), no formal evidence has been supplied at this point in time. | ✱ | ■ | • 18Ai. Continue to completion the PCI compliance in-flight project.<br>• 18Aii. Add PCI DSS non-compliance to the IT risk register.<br>• 18Aiii. Introduce GDPR and DPA compliance monitoring processes for Horizon.<br>• 18Aiv. Engage with FJ to design, implement, monitor and report compliance and non-compliance to relevant regulators and POL. |

KPMG

Document Classification: KPMG Confidential

# Systems

## The following pages detail the emerging observations as they pertain Horizon systems

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **19. Key dependencies** | **19A. Migration to AWS is in-flight however POL still have too many decisions to make (i.e. whether to stay with FJ to manage Horizon or not, integration or migration of legacy systems onto AWS).**<br>• Not remediating the identified findings from the current environment in Belfast datacentre could lead to future Horizon operational issues with potential cost implications. This was confirmed during discussions with POL representatives (29-Oct-2020 and 5-Nov-2020), no formal evidence has been supplied at this point in time. | ✱ | ■ | • 19Ai. Review interdependencies and the core contracts surrounding the migration to ensure no potential conflicts or future complications materialise.<br>• 19Aii. Ensure that the current POL - Fujitsu contract is fit for purpose to accommodate the in-flight migration and future states. |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Supplier and performance management

## The following pages detail the emerging observations as they pertain Horizon supplier and performance management

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **20. Vendor performance management** | **20A. Key Performance Indicators (KPIs) are too high-level with poorly defined service performance being self-reported by Fujitsu and no subsequent self-assurance activities being undertaken by POL.**<br>• High-level and non accountable performance reviews are leading to unacceptable and unjustified trust of the vendor provided services with no improvement expectations from stakeholders. These levels of trust lead to the Service Management Report (SMR) being accepted as is with no challenge from POL.<br>• The results of the metrics from the FJ provided SMR do not include sufficient technical analysis regarding any issues or problems which had arisen during the reported month.<br>• Lack of overall visibility and governance of the Horizon service, which could lead to performance metrics not being met and result in operational issues.<br>***This was confirmed during discussions with POL representatives (29-Oct-2020 and 9-Nov-2020) with subsequent review of the provided Service Management Report "SMR Pack - September 2020".*** | ✱ | ■ | • 20Ai. Develop service performance management frameworks for the current and future target operating models. Ensure there is inclusion of relevant forum(s) with FJ presence for POL to discuss and present relevant challenges on reported metrics in order to maximise service performance for Horizon.<br>• 20Aii. Review and update the defined expected KPIs and thresholds to meet with POL defined Horizon risk appetite.<br>• 20Aiii. After completion of 20Aii, working in collaboration with FJ revise the SMR to include relevant and detailed technical analysis to ensure that POL are made aware of Horizon related issues and problems that are being or have been resolved. |

KPMG

Document Classification: KPMG Confidential

**DRAFT FOR DISCUSSION PURPOSES ONLY**

# Supplier and performance management (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **20. Vendor performance management** | **20B. Horizon service performance is overseen through different governance routes such as the Information Security Management Forum (ISMF) and Service Management Report (SMR))**<br>• This drives a fragmented view of supplier performance leading to potential inaccurate or incomplete metrics used by POL leadership to manage the vendors and make strategic decisions. This was confirmed during discussions with POL representatives (29-Oct-2020) with subsequent review of the provided Service Management Report "SMR Pack - September 2020". | ✱ | ■ | • 20Bi. In collaboration with second LoD, service managers, compliance team and ISMF review the existing end to end vendor performance management process for FJ. Identified gaps to be addressed and understanding of the end to end process to be documented and made available to relevant teams in POL to adopt a standardised coherent approach. |

# Technology

## The following pages detail the emerging observations as they pertain Horizon technology

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **21. Tool support for change delivery** | **21A. Projects are managed via spreadsheets and email.**<br>• There seems to be no overarching tool in place to facilitate the delivery of project change or test management, which causes inefficient control and coordination on change management. This is evidenced by review of the provided "Test Strategy R1", "POA-TPN-2415 - PCI DSS Test Plan v0.2", "PCI DSS - Master Test Strategy v1.0" and during discussions with POL representatives (11-Nov-2020, 12-Nov-2020). | ☑ | ■ | • 21Ai. Whilst POL has IBM DOORS and Microfocus ALM present, these may no longer be suitable for use (and licensing may be expensive). A suitability assessment of the current market available tools should be conducted, and the most appropriate tools implemented - and their use enforced across all change. |

# Technology (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **22. Business Continuity Plan (BCP) / Disaster Recovery (DR)** | **22A. The SV&I test environment doubles as the DR environment.**<br>• This is a high-risk solution and is not an effective DR strategy. The test environment is not an appropriate DR environment because code versioning would be different and may not be reflective of the production environment (e.g. missing integrations / applications, size and scale).Repurposing the test environment for DR could result in code conflicts, data issues and/or other code configuration issues which could invalidate certain test results. This was evidenced during discussions with ATOS representatives (11-Nov-2020).<br>***This area is still under investigation.*** | 🏋 | ■ | • 22Ai. Build and establish a dedicated DR/BCP environment which is a mirror of Production, and is only used for DR purposes.<br>• 22Aii. Update BCP/DR plans (if available) to include Amazon DR approach now that Horizon is migrating to AWS. |

DRAFT FOR DISCUSSION PURPOSES ONLY

# Technology (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **23. Tools for IAM and GRC** | **23A. There is insufficient usage of technology and tools for IAM and risk management.**<br>• Although POL has ForgeRock, Microsoft Identity Manager, ServiceNow, TRACtion and Archer, their capabilities are not fully leveraged nor used in an integrated way, which if they were could:<br>○ alleviate, streamline and automate manual processes,<br>○ provide a single view of users/identities,<br>○ improve governance and reporting, and<br>○ reduce risk exposure.<br>***This was confirmed during discussions and evidenced during the share screen session with POL representatives on TRACtion to view the Risk and Control Matrix ((3-Nov-2020, 9-Nov-2020 and 10-Nov-2020).*** | ✱ | ▨ | • 23Ai. Assess existing tools and processes and create a strategic roadmap to leverage or consolidate current tooling.<br>• 23Aii. Consider additional Commercial Off The Shelf (COTS) tools where existing tools are not fit-for-future use or to achieve additional efficiency. |

# Technology (cont.)

| Sub-theme | Emerging observations and impact | HIJT report mapping | Rating | Recommendation |
|---|---|---|---|---|
| **24. AP-ADC Scripts allow uncontrolled change** | **24A. Automated Payments – Advance Data Scripts (AP-ADC) are used to make changes in Production & Reference Data.**<br>• AP-ADC scripts provide a facility for the Post Office Limited to make configuration and reference data changes to the platform. The scripting language provides potentially powerful functionality, is proprietary and extremely complex. There are currently over 900 such scripts in production each of which can contain 100s of lines of function of various levels of complexity and these can be changed relatively easily through formal and informal methods. This facility has evolved into a complex and relatively undocumented "system" which has the potential to cause unanticipated system behaviours and unwanted user experiences. There is currently a high volume of such changes at any time and this fact seems at odds with what should be a relatively stable platform essentially doing the same or similar things it has done for some time. This was confirmed during discussions with POL representatives (14-Dec-2020) with subsequent review of the provided 'AP-ADC script reference manual' (20Nov2020). | ✓ | ▨ | • 24Ai. Analyse and build an index of the AP-ADC scripts to fully understand what they can be used for, and how they are used within Horizon.<br>• 24Aii. Formalise the process by which AP-ADC scripts can be used to effect change, and restrict the access to these scripts to only the most appropriate people (PAM/Access controls).<br>• 24Aiii. Ensure all change involving AP-ADC scripts is appropriately routed through the updated change process, and any change is appropriately captured and recorded. |

POL00031727

# 04

# Appendices - to be updated

# A1: Document list - PAM/RAM

**In the course of this audit we reviewed several documents. They are listed below.**

| Title | Description | Source |
|---|---|---|
| IT Access Control Policy/Standards/Guidelines/Manual | Details provisioning of PAM and RAM access on Horizon. | POL |
| User Access Management Policy/Standards/Guidelines/Manual | Details permitted actions for user access management and privileged access management. | POL |
| Information Security Policy/Standards/Guidelines/Manual | Details security expectations or PAM and RAM. | POL |
| Records of corrective action(s) taken by Post Office Limited | Details corrective action(s) taken by Post Office Limited when failings in the PAM and RAM processes have been identified, discussed and actions taken to remediate/resolve and to ensure the same does not happen again. | POL |
| Horizon landscape document<br>Horizon analysis V0.3a<br>Horizon description (1)<br>ARC030 Horizon Solution Architecture Outline<br>ARCSECARC0003V6po<br>UEM-012b - POL IT Landscape v1.5 (002)<br>UEM-012b - POL IT Landscape v1 6 | Description of the environment and architecture. | POL |
| User access request form for requesting global access | Evidence for User Access Management activities performed by Data Services Team | POL |
| Bi-annual user access reviews and remediations of access | Evidence for User Access Management activities performed by Data Services Team | POL |
| 20201104 security Risk | Evidence of the IT risk register | POL |

DRAFT FOR DISCUSSION PURPOSES ONLY

# A1: Document list - PAM/RAM (cont.)

**In the course of this audit we reviewed several documents. They are listed below.**

| Title | Description | Source |
|---|---|---|
| Weekly leaver checks and access remediation of leavers | Evidence for the Global user access accounts | POL |
| Populated forms and approvals for creating new users for global access | Evidence for the Global user access accounts | POL |
| Evidence that the Admin role is only granted to users from Data Services Team | Evidence for the Global user access accounts | POL |
| Number of SMARTids that have not been used in the last 6 months to date | To evidence if any redundant or orphan accounts exist. | POL |
| Harm Table Published | The likelihood and impact table used by the POL Central Risk team | POL |
| ITGC Update - IT Audit result for discussion_POLv1 | | POL |
| IT Controls Progress Report | Results from the COBIT IT controls review | POL |
| CSA Monthly Detail Report | Results from the Controls Self Assessment (CSA) | POL |
| Risk and Control Matrix | | POL |
| Contract Management Framework | New POL Contract Management framework | POL |
| Archer IT Risk report 261120 | IT risk team report from IT GRC tool Archer | POL |
| POL – FJ contract | Current contractual agreement between POL and its business critical vendor FJ. | POL |

KPMG

DRAFT FOR DISCUSSION PURPOSES ONLY

# A1: Document list - PAM/RAM (cont.)

**In the course of this audit we reviewed several documents. They are listed below.**

| Title | Description | Source |
|---|---|---|
| Fujitsu-Post Office ISAE3402 FINAL report - 1 April 2017 to 31 December 2017 | Service Organisation Controls Report (SOCR) performed by EY, provided to POL by FJ | POL |
| Fujitsu-Post Office ISAE3402 FINAL report - 1 April 2018 to 31 December 2018 | SOCR performed by EY, provided to POL by FJ | POL |
| Fujitsu-Post Office ISAE3402 FINAL report - 1 April 2019 to 31 December 2019 | SOCR performed by EY, provided to POL by FJ | POL |
| JML - Final Report | Joiners, Movers and Leavers thematic internal audit conducted by POL IA in 2020 | POL |
| IA Audit Reports - HMU IT | IT Internal Audit plan for the thematic reviews (2016-2020) | POL |
| AP-ADC script reference manual | Reference manual for the AP-ADC scripts | 20/12/2020 |

KPMG

# A1: Document list - KELS, SDLC, HNGA

**In the course of this audit we reviewed several documents. They are listed below.**

| Title | Description | Source |
|---|---|---|
| Test Strategy R1 | Document covering all testing and integration activities performed for the HNG-X Programme | POL |
| Edge Fujitsu Test Environments Report v1.1 | Document covering Edge Testing's review of Fujitsu/Post Office Limited Test Environments estate and recommendations for improvement. | POL |
| Test Strategy Post R1 | Document covering all testing and integration activities performed for the HNG-X Programme | POL |
| Rig 0094 - Regression Tests - Back Office | Covers regression tests for back office | POL |
| Rig 0093 - Regression Tests - Front Office | Covers regression tests for front office | POL |
| Hydra_0823 | Covers test script & report for the CC (Computacenter) HNG-a Microsoft Patches | POL |
| Hydra_0817 | Covers test script & report for the CC (Computacenter) HNG-a Microsoft Patches | POL |
| Change Management Process V2 | Minutes of a meeting discussing the PO change process | POL |
| 20200907 Horizon Governance Terms of Reference v1.0 | Terms of Reference for the Horizon governance board | POL |
| 20201016 Horizon Known Errors Joint Review Working Group Tof R v1.2 | Terms of Reference for the Horizon Known Errors governance board | POL |
| Copy of Horizon Known Error Review WE161020 | Known Errors for 16th Oct 2020 | POL |

DRAFT FOR DISCUSSION PURPOSES ONLY

# A1: Document list - KELS, SDLC, HNGA (cont.)

In the course of this audit we reviewed several documents. They are listed below.

| Title | Description | Source |
|---|---|---|
| Horizon Known Error Review ToR V1 | Process for managing KEL items | POL |
| Horizon Known Error Review Agenda 191020_ | Horizon Known Error Review meeting agenda or minutes | POL |
| Horizon Known Error Review WE021020 | KELs for 2nd Oct 2020 | POL |
| SIP Test Action 1.1 | Response to SIP environment issues | Fujitsu |
| SIP Test Action 1.2 | Response to SIP transaction issues | Fujitsu |
| SIP Test Action 1.3 | Response to SIP automation issues | Fujitsu |
| SIP Test Action 1.5 | Response to SIP regression issues | Fujitsu |
| CM-POL-IT Change Management Policy v1.0 | The change management policy for IT | POL |
| CM-PRO-IT Change Management Process V2.0 | The change management policy for IT | POL |
| Change Control Framework Extract_October 2020 | Extract of Change Control Framework Deliverables | POL |
| Change Examples-> CHG0037290 Campus DR Change Request Draft V2 (5) | Change Example_Fujitsu | POL |
| CHG0037290 Change Plan DR_2020 | Script for CHG0037290 Change Plan DR_2020 | POL |
| CHG0037290 | Sample Fujitsu Change Request | POL |

DRAFT FOR DISCUSSION PURPOSES ONLY

# A1: Document list - KELS, SDLC, HNGA (cont.)

**In the course of this audit we reviewed several documents. They are listed below.**

| Title | Description | Source |
|---|---|---|
| Zip Tech CAB Agenda Minutes | Technical CAB Agenda and minutes detail sheet | POL |
| Zip Business CAB Agenda Minutes | Business CAB Agenda and minutes detail sheet | POL |
| CHG0037544 | Computacentre Change Request Sample | POL |
| CHG0037838 | Verizon Change Request Sample | POL |
| CHG0037846 | Verizon Change Request Sample | POL |
| CHG0037898 | Verizon Change Request Sample | POL |
| CHG0036991 | Computacentre Change Request Sample | POL |
| CHG0036992 | Computacentre Change Request Sample | POL |
| POA-TSR-DM0119468 - Environment Agency - GDPR changes v0.3 | Test Summary Report | POL |
| Fujitsu-Post Office ISAE3402 FINAL report - 1 April 2019 to December 2019 | Internal Audit Report - Fujitsu-Post Office report - 1 April 2019 to December 2019 | POL |
| POA-TSR-Drop & Go -EUM Restrictions v0.2.docx | Test Summary report - DROP & GO -EUM RESTRICTIONS | Atos |
| Test Plan - Drop & Go -EUM Restrictions v0.1.docx | Test Plan - DROP & GO -EUM RESTRICTIONS | Atos |
| PCI DSS - Master Test Strategy v1.0.docx | PCI DSS Master Test Strategy | POL/Atos |
| Pocono Regression Test Update Friday 9th October | Regression testing update Mail | Atos |

KPMG

DRAFT FOR DISCUSSION PURPOSES ONLY

# A1: Document list - KELS, SDLC, HNGA (cont.)

**In the course of this audit we reviewed several documents. They are listed below.**

| Title | Description | Source |
|---|---|---|
| POA-TSR-2415 - PCI DSS PIN Changes Test Summary Report v0.4 | Test Summary Report for a Large change | POL/Atos |
| POA-TPN-2415 - PCI DSS Test Plan v0.2.docx | Test Plan for a Large Change | POL/Atos |
| PCI DSS - Master Test Strategy v1.0 | Master test strategy for large project | POL |
| RiPE Project Closure Concurrence | Project closure documentation mail | POL |
| IT Concurrence - Guidelines v3.0 | IT Concurrence Document | POL |
| IT concurrence - Closure report IT Service transformation | Project closure documentation mail | POL |
| Copy of Risk and Control Matrix | Risk and Control Matrix sheet | POL |
| IT Controls Progress Report | IT Controls Progress Report | POL |
| Copy of CSA Monthly Detail Report | CSA Monthly Detail Report | POL |
| TSTSOTHTP4072 | SV&I Test plan for CP2459 – Payment Pilot – Phase 2 | POL/Fujitsu |
| TSTSOTREP4126 | SV&I - End of Testing Report - PBS Phase 1 and 2 | POL/Fujitsu |
| POA-TPN-0002411- Autumn Tariff Change Test Plan v0.1 | Atos reference data change test plan - Autumn Tariff | Atos |
| POA-TSR-0002411 - Autumn Tariff Change Test Summary Report - Approved v1.0 | Atos reference data change test summary report - Autumn Tariff | Atos |
| KELs Process Flow diagram(PEAK and KEL process Swimlanes MG2.5.vsdx) | KEL's management process diagram | POL |

DRAFT FOR DISCUSSION PURPOSES ONLY

# A1: Document list - KELS, SDLC, HNGA (cont.)

**In the course of this audit we reviewed several documents. They are listed below.**

| Title | Description | Source |
|---|---|---|
| Summary Notes Post-HIJ | Historical KELs summary notes Post-HIJ | POL |
| Summary Issue Reports | Historical KELs summary reports Post-HIJ | POL |
| Copy of _DOC_159267141(2)_29 Issues - key details.xlsx | Historical KELs key details sheet | POL |
| 20201113 Known Error Log Decision and Funding Tracker v2.xlsx | Known Error Log Decision and Funding Tracker | POL |
| Horizon Known Error Review Minutes 161120.docx | Known Errors Review Minutes | Fujitsu |
| Horizon update November 2020 - Release Notes.docx | Release Notes for Horizon November update | POL/FJ |
| Knowledge Base - cardc2117L.151119.pdf | Knowledge Base Article | POL/FJ |
| Knowledge Base - dsed1614M 060420.pdf | Knowledge Base Article | POL/FJ |
| Knowledge Base - GelderR488Q 131120.pdf | Knowledge Base Article | POL/FJ |
| Knowledge Base - jsim1429I 151119.pdf | Knowledge Base Article | POL/FJ |
| Known Errors - Stakeholders and Management Update - 23 November.pptx | Horizon Known Errors – Latest Status of Open Items (as at 23/11/2020) | POL |
| MemoView Branch Reminder - Drop & Go Compliance Communication 17.11.2020.docx | Drop & Go Compliance Communication | POL/FJ |
| Current Architecture and Forums.ppt | Current Architecture and Forums details | POL |

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

# A2: Interviewees

**In the course of this audit we spoke to a number of individuals. They are listed below.**

| Name | Title | Area of Focus |
|---|---|---|
| Adrian Eales | [TBC] | Horizon walkthrough |
| Andrew Kenny | [TBC] | Demonstration of the Tier 2 team usage of HORice when conducting investigations |
| Adam Malach<br>Tony Hogg | [Head of Cyber Assurance]<br>[Head of Cyber Operations] | Meeting to understand PO side of security management |
| Graham Hemingway | [GLO Portfolio Manager] | Understand the GLO Portfolio and how the Horizon Issues programme fits in this bigger picture |
| Simon Oldnall<br>Martin Godbold<br>Paul Smith<br>Dean Bessell<br>Paul Kingham<br>Charlotte Muriel | [GLO and Horizon IT Director]<br>[Head of IT Service for Retail]<br>[TBD]<br>[TBD]<br>[TBD]<br>[TBD] | At least daily interaction on direction of travel, validation of hypotheses and emerging findings. |
| Dionne Harvey | [Contract Vendor Management ] | To understand the vendor relationship management aspect between POL and FJ. |
| Sree Balachandran | [TBD] | Obtain an understanding of the IT landscape (e.g. IT equipment, email, server, networking, etc) of the Post Office Limited and branches; understand how a Branch processes transactions and how data moves from Branch to Horizon; understand feedback from Postmasters |
| Joy Lennon | [TBD] | Overview of the process for management of global user accounts, Privileged Access Management, Remote Access Management |
| Dave King | [Head of Security Architecture] | Walk through privileged Access Management/PAM/RAM process(es) for Horizon at Fujitsu<br>Walk through break-glass procedure including approvals, monitoring, audit log reviews etc. |
| Shaun Turner | | Horizon Access Management: process for access to Horizon using Smart IDs |
| Ehtsham Ali | [Head of Cyber Security Compliance] | General overview and specifics around compliance checks with suppliers, detail on builds, understanding of approach |

# A2: Interviewees (cont.)

| Name | Title | Area of Focus |
|---|---|---|
| Aatish Shah | [TBD] | IT Change Framework: POL IT controls and the framework in place around these controls |
| James Brett | [ATOS Test Manager] | Discuss the testing which ATOS is responsible for delivering |
| Luke Harrison | [TBD] | Further develop understanding of the IT landscape (e.g. IT equipment, email, server, networking, etc) of the Post Office Limited and branches |
| Sally Rush | [TBD] | Understand the current documentation and processes for data management in Horizon |
| Rob Wilkins | [Director for Cloud Office] | Understand the Horizon move to Amazon Web Services |
| Gary Walker | [TBD] | Understand the Release management process |
| Ian Sage | [PM for AWS migration] | Discussion of how the Belfast Migration programme is governing change |
| Ben Owens | [TBD] | Introduction to the testing being performed across change occuring on Horizon, and how the testing is governend and controlled including the test approach for the Belfast migration. |
| Jonathan Acres<br>Diogo Vidinhas | [Internal Audit]<br>[TBD] | To understand the POL environment from IA's perspective and evaluate the internal audits involvement with risk management around Horizon and FJ |
| Rebecca Barker | [Head of IT & Digital Risk] | Understand the role/records/actions under POL's Risk Management function |
| Stephen Browell | [Fujitsu CISO] | Discussion of ways of working with Fujitsu including access to documentation and resources |
| Katrina Holmes | [TBD] | Horizon change mgmt, testing and incident management |
| Stuart Banfield | [TBD] | Horizon change processes |
| Harry Vazanias | [TBD] | Discussion of change management, gaps and problems in IT org structure and SDLC management |
| Joseph Moussalli | [TBD] | Discussion on how the PCI programme is being governed |
| Tony Jowett | [CISO] | Governance around Horizon and the IT controls framework |
| Steve Page | [Solutions Architect] | Library of architecture documentation on Horizon and an overview of the Horizon data flow |

DRAFT FOR DISCUSSION PURPOSES ONLY

# A2: Interviewees (cont.)

| Name | Title | Area of Focus |
|---|---|---|
| Saira Burwood<br>George Cross | [TBD]<br>[TBD] | Walkthrough of the portfolio process; Discussion on detailed programme and project management; Governance of third party delivery |
| Cherise Osei | [TBD] | Walkthrough and discussion of the POL change management process |
| Gareth Clark | [TBD] | Portfolio management within IT |
| Matthew Warren | [TBD] | Discussion of how ATOS are involved with POL change |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# A2: Interviewees (cont.)

**The following individuals were interviewed as part of the Investigations TOM work but relevant observations were shared and have been incorporated in this report:**

| Name | Title | Area of Focus |
|---|---|---|
| Tim Perkins | Head of Service and Support | Investigations TOM |
| Alison Bolsover | Branch Reconciliation Area Lead | Branch reconciliation |
| Colette Mcateer | Branch Reconciliation Operations Manager | Branch reconciliation |
| Alison Clark | Branch Analysis and Control Manager | Branch analysis and loss prevention |
| Andrew Kenny | Service Centre Manager | BSC Tier 2 |
| Louise Liptrott | Tier 2 Team Leader | BSC Tier 2 |
| Sharron Logan | Case Review Manager | Case review teams |
| David Southhall | Contract Investigation and Resolution Manager | Case review teams |
| Wayne Brant | [TBD] | Case review teams |
| Huw Williams | Contract Investigation and Resolution Team | Case review teams, key logging, ARQ process |
| Michelle Stevens | Loss Prevention Manager | Branch analysis and loss prevention |
| Paula Jenner | Head of IT Service for Corporate | IT Systems |
| Matt Quincey | Service Manager for Accenture and Verizon | IT Systems |
| Drew Mason | Network Monitoring and Support Analyst | Branch analysis and loss prevention, FREDD-O |

DRAFT FOR DISCUSSION PURPOSES ONLY

# A2: Interviewees (cont.)

**The following individuals were interviewed as part of the Investigations TOM work but relevant observations were shared and have been incorporated in this report:**

| Name | Title | Area of Focus |
|---|---|---|
| Ketul Patel | Network Delivery Director | Key logging and network analysis |
| Ruk Shah | Group MI and Analytics Director | Data Platform |
| Maria Opaniran | [TBD} | Data Platform |
| Dean Whitehead | Service Centre Support Manager | Dynamics and Puzzel |
| Laura Tarling | [TBD} | Flag Case Team |
| Tony Hogg | Head of Cyber Operations | Security operations |
| Matthew Lenton | Fujitsu | Investigation requirements for Fujitsu |
| Christopher Knight | Intel Team Manager | ARQ data request process |
| Min Dulai | ServiceNow System Manager | ServiceNow |

# A3: Meetings list

**The following meetings took place as part of the Investigations TOM work but relevant observations were shared and have been incorporated in this report:**

| Ref# | Focus Area | Attendees | Date | Comments |
|---|---|---|---|---|
| 1 | Horizon Overview | Adrian Eales | 16-Oct | Horizon walkthrough meeting |
| 2 | HORice walkthrough for investigations | Andrew Kenny | 16-Oct | HORice walkthrough |
| 3 | KPMG Engagement | Adam Malach<br>Tony Hogg | 21-Oct | Meeting to understand PO side of security management |
| 4 | Project Iris - Audit deliverables | Simon Oldnall | 23-Oct | To agree on the engagement deliverables and audit report structure using the examples that Amina provided and was agreed at this meeting. |
| 5 | Call with PO Head of Cyber Security Compliance | Ehtsham Ali | 23-Oct | General overview and specifics around compliance checks with suppliers, detail on builds, understanding of approach etc. |
| 6 | GLO Programme Overview | Graham Hemingway<br>Kevin Hutchinson | 28-Oct | Understand the GLO Portfolio and how the Horizon Issues programme fits in this bigger picture |
| 7 | Project Iris - Vendor management meeting | Dionne Harvey | 29-Oct | To understand the vendor relationship management aspect between POL and FJ. |
| 8 | Project Iris - CISO meeting | Tony Jowett | 30-Oct | Discussion on governance around Horizon and the IT controls framework |
| 9 | Project Iris - Branch process meeting | Sree Balachandran | 03-Nov | Session to understand how a branch processes transactions and how data moves from branch to Horizon |
| 10 | Risk Management | Rebecca Barker | 03-Nov | Understand the role/records/actions under POL's Risk Management function |
| 11 | Horizon Data Flow Overview | Steve Page<br>Martin Godbold<br>Charlotte Muriel<br>Dean Bessell<br>Martin Godbold<br>Paul Kingham<br>Sally Rush | 06-Nov | Session for Steve Page to introduce us to the library of architecture documentation he has on Horizon and an overview of the horizon data flow |

DRAFT FOR DISCUSSION PURPOSES ONLY

# A3: Meetings list (cont.)

| Ref# | Focus Area | Attendees | Date | Comments |
|---|---|---|---|---|
| 12 | Project Iris - Internal Audit follow-up meeting | Jonathan Acres | 09-Nov | Meeting to discuss Internal Audit coverage of Horizon controls. |
| 13 | Project Iris - Security Architecture meeting | Dave M King | 09-Nov | (PAM/RAM meeting) Discuss and obtain an understanding of the IT security architecture of the Post Office Limited and branches |
| 14 | IT Security: Initial Discussion | Dave M King | 09-Nov | (Forensics meeting) Discuss and obtain an understanding of the IT security architecture of the Post Office Limited and branches |
| 15 | KPMG GLO Assessment - IT Change Framework | Aatish Shah | 10-Nov | Discuss the POL IT controls and the framework in place around these controls |
| 16 | Project Iris - PAM/RAM evidence request | Simon Oldnall | 11-Nov | Discuss the testing ATOS is responsible for delivering |
| 17 | IT Scoping Discussion | Sree Balachandran Luke Harrison | 10-Nov | Discuss and obtain an understanding of the IT landscape (e.g. IT equipment, email, server, networking, etc) of the Post Office Limited and branches |
| 18 | Project Iris – Global User accounts meeting | Joy Lennon | 17-Nov | An overview of the process for management of global user accounts, role of Joy Lennon, Privileged Access Management, Remote Access Management |
| 19 | Project Iris - Security Architecture | Dave M King | 18-Nov | Walk through privileged Access Management/PAM/RAM process(es) for Horizon at Fujitsu<br>Walk through break-glass procedure including approvals, monitoring, audit log reviews etc. |
| 20 | Evidence request meeting | Simon Oldnall<br>Sree Balachandran | 18-Nov | Walkthrough the evidence list - meeting requested by Simon |
| 21 | Horizon Access Management | Shaun Turner | 19-Nov | Discuss the process for access to Horizon using Smart IDs |
| 22 | Horizon Change processes | Sree Balachandran<br>Sally Rush | 20-Nov | Discussion on our understanding on Horizon Change processes |
| 23 | Evidence request meeting | Sree Balachandran | 23-Nov | Walkthrough of the evidence list |
| 24 | Review document request list | Sree Balachandran | 25-Nov | Walkthrough of the evidence list - meeting requested by Simon |
| 25 | Project Iris additional documentation | Sree Balachandran | 10-Dec | Walkthrough of the evidence list for PAM/RAM |
| 26 | AP-ADC scripts | Steve Page | 14-Dec | Discussion regarding the AP-ADC scripts |

KPMG

home.kpmg/socialmedia

This report is provided pursuant to the terms of our contract with Post Office Limited (POL). The report is intended solely for internal purposes by the management of POL and should not be used by or distributed to others, without our prior written consent. To the fullest extent permitted by law, KPMG LLP does not assume any responsibility and will not accept any liability in respect of this report to any party other than the Beneficiaries