POL00337564

KPMG

Horizon report

Report on the progress made to address six areas derived from HIJ findings

Post Office Limited



KPMG LLP
June 2021
V4.2 – Final report

Notice: This Report is provided in confidence and its circulation and use are limited – see notice on next page

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity

Document Classification: KPMG Confidential

POL00337564

Notice

This Report has been prepared on the basis set out in our Work Order with Post Office Limited (the "Client") effective 19 October 2020 and signed 29 October 2020 by the Client and 3 November by KPMG (the "Agreement", and should be read in conjunction with the Agreement.

Please note that except as required by law, the Report is not intended to be copied, referred to or disclosed, in whole or in part. The Report is confidential. Any disclosure of the Report beyond the Client may substantially prejudice KPMG LLP's commercial interests. If you receive a request for disclosure of the Report under the Freedom of Information Act 2000 or the Freedom of Information (Scotland) Act 2002 we would ask that in accordance with recommended practice, you let us know and not make a disclosure in response to any such request without consulting us in advance and taking into account any representations made.

Nothing in this Report constitutes a valuation or legal advice.

We have not verified the reliability or accuracy of any information obtained in the course of our work, other than in the limited circumstances set out in the Agreement.

This Report has not been designed to be of benefit to anyone except the Client. In preparing this Report we have not taken into account the interests, needs or circumstances of anyone apart from the Client, even though we may have been aware that others might read this Report. We have prepared this Report for the benefit of the Client alone.

This Report is not suitable to be relied on by any party wishing to acquire rights against KPMG LLP (other than the Client) for any purpose or in any context. Any party other than the Client that obtains access to this Report or a copy (under the Freedom of Information Act 2000, the Freedom of Information (Scotland) Act 2002, through the Client's Publication Scheme or otherwise) and chooses to rely on this Report (or any part of it) does so at its own risk. 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 Client.

In particular, and without limiting the general statement above, since we have prepared this Report for the benefit of the Client alone, this Report has not been prepared for the benefit of any other entity nor for any other person or organisation who might have an interest in the matters discussed in this Report, including for example general staff of the Client.

POL00337564

Contents

1	**Context**	**6**
1.1	Purpose	6
1.2	Background	6
1.3	Requested scope	6
1.4	Approach	8
1.5	Report iterations	8
1.6	Report structure genesis	8
1.7	What is Horizon?	9
1.8	Strategic Platform Modernisation (SPM)	11
1.9	Nature of Fujitsu involvement in this report	11
2	**Executive Summary**	**13**
2.1	Overall Summary	13
2.2	Core conclusion 1	15
2.3	Core conclusion 2	17
2.4	Core conclusion 3	20
3	**Observations in summary**	**23**
3.1	Horizon issues mapping	23
3.2	Privileged access management and remote access	25
3.3	SDLC, Testing and Quality Assurance	28
3.4	Known error logs (KELs) – current	33
3.5	Known error logs (KELs) – historic	34
3.6	Horizon Next Generation (HNGA) Robustness	35
3.7	Foundational Issues	37
4	**Observations in detail**	**41**

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.1	How to read this section	41
4.2	Observations in detail, by theme	43
4.3	Governance	44
4.4	Process	59
4.5	Capability	81
4.6	Culture and product	83
4.7	Data	85
4.8	Systems	86
4.9	Supplier and performance management	87
4.10	Technology	89
4.11	Further observations	96
5	**Appendices**	**98**
5.1	Appendix 1: Documentation	98
5.2	Appendix 2: Contributors	105
5.3	Appendix 4: Glossary	110
5.4	Appendix 5: Short-term Fast Fix tactical remediation	113
5.5	Appendix 6: Long-term remediation planning	115
5.6	Appendix 7: Engagement Terms of Reference	118
5.7	Appendix 8: Analysis, findings, and improvement recommendations – Horizon AP-ADC scripts and reference data solution	122
5.8	Appendix 9: Horizon IT Delivery Robustness Analysis – POL Horizon IT Maturity Assessment	123

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

Document Classification: KPMG Confidential

POL00337564

Document details

Version history

Version	Date	Notes
V3.1	27/04/2021	Draft following Fujitsu engagement, for POL stakeholder review
V4.1	10/05/2021	Final Draft for POL Executive review
V4.2	8/06/2021	Final version incorporating all comments received

List of figures

Figure 1: Logical visualisation of Horizon 'as-is' 9

Figure 2: Horizon 'as-is' in Fujitsu Belfast datacentre (below dotted line) 10

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

01

Context

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

Document Classification: KPMG Confidential

POL00337564

1 Context

1.1 Purpose

In October 2020 POL engaged KPMG LLP ("**KPMG**"). Our scope included the provision of an independent assessment of progress made by POL to address Horizon Issues and provide recommendations against observations, allowing POL to report into the ongoing Post Office Horizon IT Inquiry ("The Inquiry"). This report is the culmination of that activity.

1.2 Background

Post Office Limited ("**POL**") is currently addressing historical findings in respect of its core Branch computer system ("**Horizon**"). Horizon is used to record transactions between POL and its Postmaster Branch network, and is owned, maintained, and managed by Fujitsu Services Limited ("**Fujitsu**"). A description of Horizon is provided in *Section 1.7*.

Postmasters raised issues with Horizon, and these were linked to prosecution and conviction[1] 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 and passed several Judgements. In February 2020 a public inquiry was announced into the matter, with Terms of Reference and the appointment of a Chair 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**". We use the term "Horizon Issues" in this report to refer to the issues highlighted in Judgement No. 6.[2]

1.3 Requested scope

The engagement Terms of Reference can be found in *Appendix 7: Engagement Terms of Reference*. The scope of the assessment was directed at six areas[3], as defined by POL. The following is an extract of the six in-scope areas:

---

[1] Cases were referred to the Court of Appeal by the Criminal Cases Review Commission
[2] Judgment (No.6) "Horizon Issues" December 2019 (Horizon Issues Judgement – HIJ)
[3] These six areas are an amalgamation of Horizon Issues and in most cases do not follow a one-to-one mapping with the HIJ – this is illustrated in *Section 3.1*.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

1. Privileged Access Management[4]: Establish who has what privileged access to Horizon.

2. Remote Access[3 & 5]: Establish how remote access into the Post Office network is conducted – both currently and pre-COVID – to include Branch equipment and Branch Database (BRDB).

3. Software Development Lifecycle, Testing and Quality Assurance: Establish how: i) changes to Horizon progress from requirements analysis through development, testing and into early live support; and ii) how such changes become fully live under mainstream support arrangements.

4. Known Error Logs ("KELs") – current: Establish how Fujitsu are made aware of an error.

5. Known Error Logs – historic: For each historic KEL establish whether the condition remains or not. The Historic KELs cover 62 incidents from 1999 through to 2018.

6. Horizon Next Generation (HNGA) Robustness: Establish the functional and non-functional robustness of Horizon Next Generation. A separate set of reports have been produced to discuss robustness in more detail (refer to sections entitled *Appendix 8: Analysis, findings, and improvement recommendations – Horizon AP-ADC scripts and reference data solution*).

7. *Appendix 9: Horizon IT Delivery Robustness Analysis – POL Horizon IT Maturity Assessment*. These reports use the KPMG IT Maturity Assessment Tool, which is based on ITIL, COBIT and CMMi to assess maturity. Note that the definition of robustness used in this report is the ITIL standard definition and differs from the definition used within the Horizon Issues Judgement[6].

Observations made in this Report relate to the situation we observed during the period of our review from October 2020 to April 2021.

Our remit was to focus on the Horizon system and related processes. We did not review the systems or infrastructure supported by Computacenter or Verizon.

---

[4] Fujitsu use the term "remote access" interchangeably to cover both remote connectivity (the technical act of connecting to a remotely-hosted system) and privileged access. Although not an industry standard definition, for the purposes of our report and how these relate to Horizon Issues, we agree with this simplification of terminology and have adopted a similar approach.
[5] A number of remote access observed Horizon Issues are based upon the precursor to the current version of Horizon, when Postmaster data was held on the Branch terminals.
[6] Please note that the robustness definition used within the Judgement is located at "Ref 54 page 21" of the Judgement documentation.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

1.4 Approach

This report is based on document reviews, stakeholder meetings and discussions over the course of 7 months from October 2020 (please *see* *Appendix 1: Documentation* and *Appendix 2: Contributors*).

We would like to thank all those stakeholders involved in discussions and reviews of early drafts.

Access to stakeholders and documents initially only included POL. Over time access to Fujitsu enabled a wider perspective to be considered. We had initially planned for the assessment to be completed over a shorter timescale. This was not possible due to delays as we waited for Fujitsu to provide input in the form of written responses to our questions. Details showing what form of access Fujitsu took can be found in *Section 1.7*.

Observations are specific to the period October 2020 to April 2021.

1.5 Report iterations

Our observations have iterated during our review, as more information has come to light from Fujitsu and POL stakeholders.

1.6 Report structure genesis

Our work began in October 2020 focusing on the six in-scope areas summarised in *Section 1.2* and *Appendix 7: Engagement Terms of Reference*. Over the first few weeks, reviewing documentation and from discussion, it became apparent that there were a series of more Foundational issues present, which if unaddressed would hinder efforts to address Horizon Issues remediation work.

Our assessment ran in parallel to our wider contractual scope to document a target operating model high-level design for the newly formed GLO/Horizon IT function (Part B of our Terms of Reference, described in *Appendix 7: Engagement Terms of Reference*).

1.6.1 Report structure

This report is split into three primary sections and the Appendices which list documents reviewed and contributors that we have spoken to. Also documented is short and long-term remediation efforts, programme planning and our Terms of Reference.

1. **Executive summary.** We have observed that for remediation against the six in-scope areas to take place there are six control areas that also need to be addressed (*see Section 3.7*). These are necessary as they provide the required foundations to facilitate sustained Horizon Issues improvement and management whilst the move to a new IT platform is realised within the next four plus years.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

2. **Observations in summary.** In our early analysis we observed that several areas of improvement were required across all six in-scope areas. Since this early analysis, tactical improvement activity has begun, and longer-term remediation is planned.

3. **Observations in detail.** We have documented 73 observations, structured according to eight themes, aligned to the POL target operating model planning: Governance, Processes, Capability, Culture and Conduct, Data, Systems, Supplier and performance management and Technology.

1.7 What is Horizon?

In its simplest form 'Horizon' is a set of technologies, both software and hardware, which exists physically in circa. 11,500 Branches and at the Fujitsu Belfast datacenter, facilitating Postmasters to sell a wide variety of services to the public (such as stamps or fishing licenses) and conduct limited Branch administration (e.g. accounting, stock replenishment, communication with third parties and external service providers, reporting and granting user access).

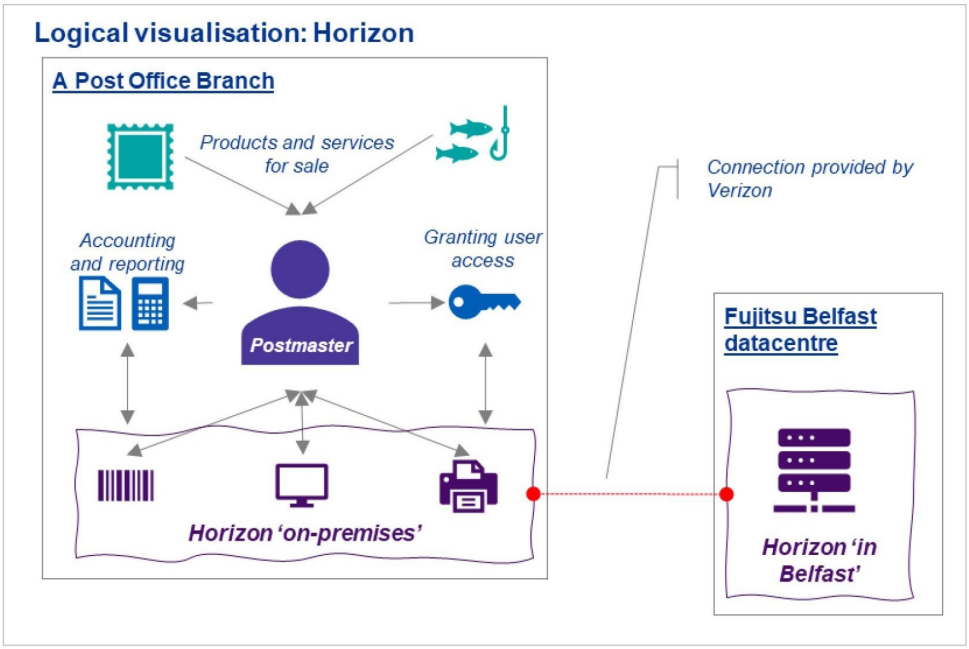


Figure 1: Logical visualisation of Horizon 'as-is'

Horizon has existed since the late 1990's after POL contracted International Computers Limited (ICL), acquired by Fujitsu Limited in 2002, to design and build it. Ownership and management of Horizon and intellectual property rights reside with Fujitsu. The current version of Horizon is HNG-A or Horizon Next Generation – Anywhere, which came into production 2017-18 as part of a phased deployment. In February 2021, Horizon processed close to 160 million transactions.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

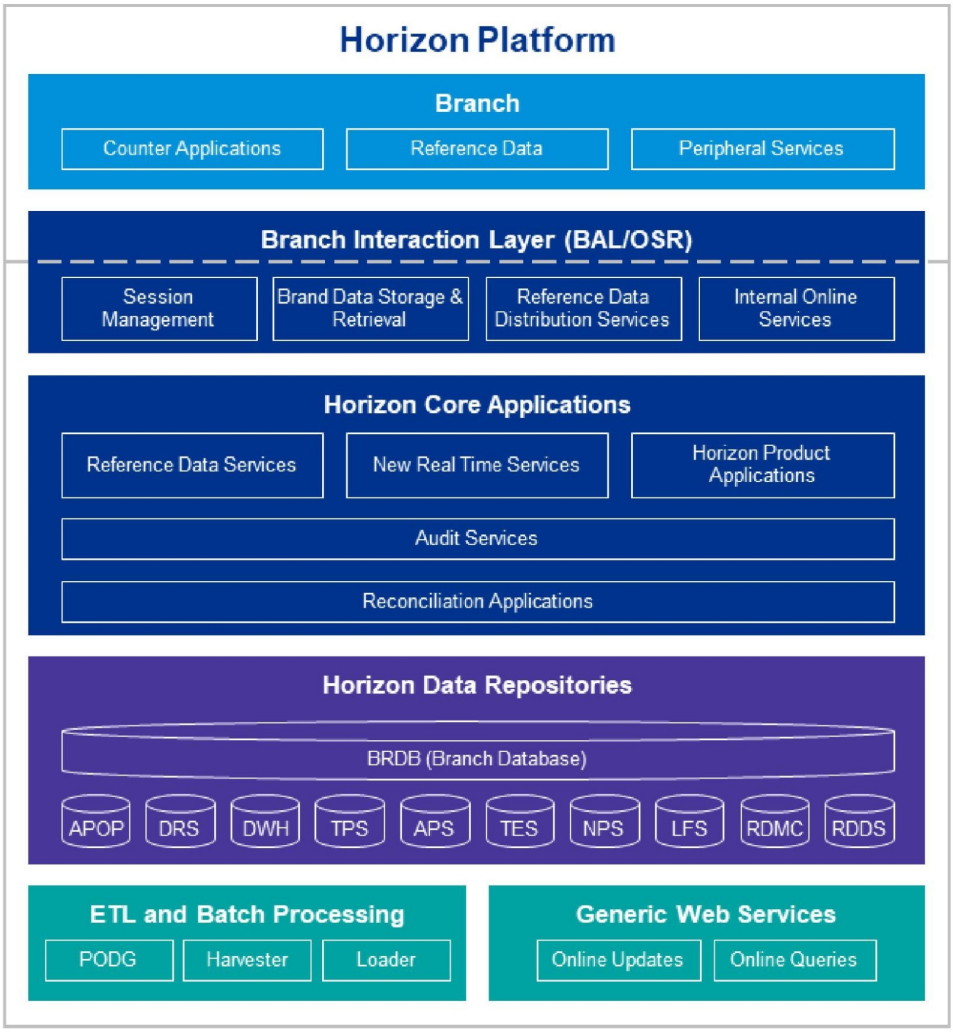


Figure 2: Horizon 'as-is' in Fujitsu Belfast datacentre (below dotted line)

Fujitsu's contractual responsibilities include the development and maintenance of Horizon. This means the development of software within its datacentre and the management of component services, hardware, operating systems, supporting security applications, software, underlying databases, the general "lights on" maintenance services and components that facilitate root-cause analysis and remediation. The activities undertaken by Fujitsu to maintain Horizon include platform patching/update and performance tuning.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

1.8 Strategic Platform Modernisation (SPM)

A major programme of activity, known as the Strategic Platform Modernisation (SPM), will design an application architecture to replace Horizon software components. This programme *"is designed to improve robustness and transparency, increase agility, refocus on core customers and products, whilst supporting the Network Strategy (right services, right places, right time)"*[7]. It is due to commence in 2021 and run over the next 5-6 years.

In parallel, there is a proposal for POL to extract the part of Horizon that resides in the Fujitsu Belfast datacentre and place it in a POL owned Amazon Web Services instance.

1.9 Nature of Fujitsu involvement in this report

This overview is provided to describe the relationship between Fujitsu Business Services Limited (Fujitsu) and Post Office Limited (POL) with specific reference to the areas of focus within this report.

KPMG's review and report, referred to in the preceding section, has been directed at both POL and Fujitsu as POL's systems and infrastructure contribute to the service provided to Postmasters as part of Horizon service.

KPMG was able to discuss and examine the appropriate areas of POL's directly managed estate and form views in discussion with service or platform owners.

Our original approach with Fujitsu was to perform a series of interviews, document reviews and reviews of process related to the six in scope areas. This approach could not be agreed with POL and Fujitsu, instead the approach was built upon a series of exchanged written reports with follow-on written questions and written responses. The reports and responses are itemised in *Appendix 1: Documentation*. In the period referred to by this report we have been unable to verify all the information provided in the reports or detail in subsequent responses to queries raised by us, having requested but not being provided the opportunity for technical walk-throughs of the approaches described.

[7] POL Draft Case for change/objectives of the Horizon replacement

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

02

Executive Summary

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

Document Classification: KPMG Confidential

POL00337564

2 Executive Summary

2.1 Overall Summary

The Inquiry shines a spotlight of expectation on POL, which can become reality if a scale of change is met with significant remediation.

2.1.1 The Inquiry demands change and (data) integrity

One of the central tenets of the Horizon Issues Judgement (HIJ) is that POL must change, restore, and sustain Postmasters confidence in POL's ability to maintain the integrity of their Branch data. Moreover, concerns over the reliability and operation of Horizon must be addressed.

Key suppliers, in particular Fujitsu, are integral to the delivery of the current Horizon service and to restoring confidence with Postmasters. The current platform will need to be sustained over the coming 4+ years whilst POL migrates to its new Postmaster-facing platform under the Strategic Platform Modernisation Programme.

As a part of this, POL is required to demonstrate several things, including.

- An understanding of Postmasters and the demands they face as the customer-facing sales force, by having effective lines of communication.
- An ability to manage and address risk in the broadest sense of the business definition, both internally and, by extension of the approach, with its core suppliers (in this case Fujitsu), supported by an effective risk management and controls regime.
- A reliable application (be it Horizon or its replacement, the Strategic Platform Modernisation (SPM)) including implementing appropriate user design, following standard usability protocols, within a supportive environment for its Branch network, be it direct or franchisee; and
- In the light of the Horizon Issues, a restoration in the belief by its workforce and the public that it is well run, trusted and accountable.

Over the page we summarise our core conclusions.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

2.1.2 Core conclusions

We have accounted for what the Inquiry demands, as well as the Horizon Issues in drawing our conclusions.

In summary they are:

1. POL has made improvements responding to the Horizon Issues (*see Section 2.2*);

2. Significant remediation is still required across the six in-scope areas *(see Sections 2.3*); and

3. The scale of change required is extensive, which includes the need to address Foundational Issues (*see Section 2.4*).

2.1.3 Moving forwards

The culture of POL should reflect the Board's ambition to improve its engagement and provision of service to Postmasters, embracing clear accountability as part of a culture of 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 must ensure that there is an alignment of all programmes that are directed to the betterment of POL and its Postmaster business. This includes the SPM, POL cultural programmes, and the Postmaster Journey programme with its stated aim of "putting Postmasters at the heart of its business".

POL needs to mirror its social purpose[8] in its internal business engagement by adapting and maturing as an organisation to embed and sustain improvements. It needs to ensure these are driven through its public customer facing channel; that of the Postmasters, and these must also be driven throughout the POL organisation.

The migration programme to a new platform and branch-side application will bring significant improvements. The expected delivery timeline for these needs to be balanced against the desire to maintain Postmaster engagement on the current platform. POL's investment in improvement of the current platform rightly needs to be balanced against that of investment in the future, but not to the disadvantage of Postmasters, nor the public perception of improvements expected in the immediate future.

---

[8] Post Office Corporate – Social purpose "more than just a Post Office" POL organisation.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

2.2 Core conclusion 1

POL has made improvements since the Horizon Issues were raised.

2.2.1 Change is happening

In Autumn 2020 POL started to build a capability to be specifically responsible for the management of the Horizon IT estate and its vendors. A GLO/Horizon IT Director was appointed in September 2020 with a mandate to effect improvement in Horizon and its supporting operations. This capability has begun to be established, drawing upon current POL staff and experienced hires (amounting to 20 staff currently).

2.2.2 Remediation

With the support of POL leadership, the Horizon IT capability are driving both short- and long-term remediation *(see Appendix 5: Short-term Fast Fix tactical remediation* and *Appendix 6: Long-term remediation planning*).

Short-term Fast Fix tactical remediation

POL has instigated a Fast Fix programme which has prioritised what it believes to be the most critical items to begin to address the Horizon Issues and, in particular, the six prioritised areas described in Section *1.3* (*see Appendix 5: Short-term Fast Fix tactical remediation*). The Fast Fix plan intends to deliver initial improvements by the end of May 2021.

Long-term remediation

A further two phases of delivery are currently being planned for the next 24 months (*see Appendix 6: Long-term remediation planning*). The objectives of the programme are specifically designed to address the Horizon issues and the findings of this report. This will run in parallel with the SPM Programme.

The workstreams proposed in the 24-month programme are key to improving the management of Horizon, both now and to its end of life, and importantly embedding the structure and capabilities that will be critical to the delivery of SPM and its subsequent running. However, any programme must have the support of POL to succeed. To deliver this, each component of the programme and the supporting POL organisation must have appropriate budgets and understand its roles and responsibilities. Furthermore, there should be a POL-wide understanding of risk, and processes to manage risk appropriate to its potential impact.

At this point, it is encouraging to see the support from the Group Executive for the long-term remediation programme that looks to the above. This will need to endure for the length of the remediation – which will likely extend beyond 24-months.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

2.2.3 Moving forward

POL and the GLO/ Horizon IT team are making progress. The immediate challenge however must be to ensure that any in-flight activities, such as data migration from Fujitsu's Belfast datacentre to a Post Office cloud-based environment and the underlying arrangements, are assured as fit-for-future by integrating them into the emerging activities.

The current Horizon operating model and that of the broader POL organisation require sustained attention to transform the Post Office into a stable and future-proof direct and franchise-based model. Our observations (in *Section 4*) have, by necessity, looked to the organisation as well as the Horizon Issues.

The 24-month programme must start with an organisation which collaborates internally as well as with its Postmasters and its vendors, delivers against the Fast Fix-fix and addresses the Foundational Issues. Early steps should include:

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

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

2.3 Core conclusion 2

Significant remediation is still required across the six in-scope areas

2.3.1 Privileged Access Management and Remote Access[9] (*see Section 3.2*)

Across the entire Horizon domain, there is a low level of maturity, based upon KPMG's Maturity assessment levels, namely - mostly manually based with an uncoordinated approach across all the domains of Identity and Access Management (IAM) including privilege/elevated access, authentication (for local or remote access), joiner, mover and leaver management, and reporting.

Moreover, POL's visibility of vendor (Fujitsu in particular) activity is limited and this is not sufficiently challenged. Noting the lack of opportunity to test Fujitsu's responses as previously stated in *Section 2*, Fujitsu's approach, although in the main based upon manual process, appears to be well documented.

Although remediation is in-flight (such as manual improvements to process, due by end of May 2021) further work is needed to reach an ideal maturity level that introduces automation, efficiency and reduces the risk of human error. POL can address this by automating user enablement and management within its own domain, introducing IAM tooling to improve its maturity to a point where it has full visibility of all users including those within Fujitsu's domain. Appropriate controls should be agreed with Fujitsu and introduced to ensure timely approval and/or visibility of Fujitsu user activity, thereby enabling POL to successfully manage all users and what they can do when they gain access.

2.3.2 Software Development Lifecycle (SDLC), Testing and Quality Assurance (*see Section 3.3*)

The overall governance and control of the SDLC and Testing processes within POL, and with respect to delivering technical change for Horizon, is immature when measured against industry standard frameworks. For example, no formal Release Management process is in place. Actions are being taken to uplift these

---

[9] We have considered privileged access management (PAM) and remote access (RAM) within this report in the context of the nature of data being accessed, the risk or concern exposed in doing so and the approaches to properly control and report on these activities. As such, our observations consider a wider approach to access than that of an industry standard view of privileged access, driven by use cases we have seen. These include the ability for users to act on behalf of others, such as Postmasters or engineers, and finance staff, who, although they are carrying out their daily routine in accessing Postmasters' financial records could be deemed to have access which should be seen as privileged.

In Footnote 4 on page 7 we describe Fujitsu's view of remote connectivity and privileged access; this broadly fits with the interpretation we have made for our work and aligns with a lay view, which is one Postmasters are more likely to align with.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

processes, and appropriate controls are now being implemented. However, this is not a quick fix, and will require time to fully embed. As such they have been allocated to the long-term remediation planning.

2.3.3 Known Error Logs (KELs) – current (*see Section 3.4*)

Fast fix activity has improved the handling of current KELs, with the commissioning of a dedicated owner and a support team, to take control of the KELs and drive them to conclusion (i.e. rectification, retest, and closure). Further updates and refinements to the new process are currently being implemented (expected completion of 30th May), and tighter controls have been put in place, such as standard templates for capturing KEL details, quality checks, detailed technical analysis, and status tracking. Buy-in and commitment from the third parties (including Fujitsu) has likewise improved.

2.3.4 Known Error Logs – historic (*see Section 3.5*)

To date 45 of the 62 Historic KELs have been closed. POL and Fujitsu both now have sets of actions to work through to facilitate the testing and closure of the remaining historic KELs, expected to be closed by end of June. POL and Fujitsu have held joint technical workshops, and these have enabled a deeper level of analysis of the historic KELs. Test activity for the remaining outstanding historic KELs has commenced.

2.3.5 Horizon Next Generation (HNGA) Robustness (*see Section 3.6*)

Work to address HNGA robustness has included improving and restructuring the Architectural approach, updating the AP-ADC script delivery process and refining change delivery.

Despite these improvements there remain several areas in relation to Governance, Process and Management of Horizon which introduce the potential for issues to occur with Horizon.

Our overall conclusions in this area are that:

1. The platform itself is not managed, from an end-to-end perspective, in a mature manner, when measured against industry frameworks such as ITIL, COBIT and CMMi; and

2. The delivery of technical change into the Horizon platform is not handled in a mature and well-governed manner, although rapid improvements are being made through the Change Management process.

As a result, this has the potential for changes introduced to cause detrimental impact and increases the risk of incidents due to system errors and/or failures when implementing changes. Without more mature processes in place, and governed appropriately, POL is not effectively managing the Horizon platform.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Our conclusions drawn in this area are informed by two detailed reports included at *Appendix 8: Analysis, findings, and improvement recommendations – Horizon AP-ADC scripts and reference data* solution and *Appendix 9: Horizon IT Delivery Robustness Analysis – POL Horizon IT Maturity Assessment*.

A summary is provided here.

Horizon AP-ADC scripts and reference data solution

A core tenet of HNGA is reference data and AP-ADC scripting. Reference data is how much of the Horizon user functionality is configured and created. AP-ADC scripts are a means of coding sequences of transactions executed by Branch staff or changing current transaction flows. Both mechanisms are created, changed, and deployed by POL with minimal input from Fujitsu.

AP-ADC scripts and reference data elements are not primary causes of error and discrepancy; they are simply tools used by POL staff to introduce change into the Horizon platform. However, due to the lack of appropriate controls and governance regarding how this change is introduced, it is possible for incidents, discrepancy, detriment, and reputational harm to occur. For instance:

- The design of the user interface and the Postmaster experience, as defined by POL, is not considered from the perspective of user-centricity;
- The way in which POL manage change of user functionality is immature; and
- The way in which POL test change does not account for user testing, which would ordinarily allow weaknesses in the solution to be identified

However, the potential to cause discrepancy is partly mitigated by the controls the reference data team put in place while building reference data and AP-ADC scripts.

POL Horizon IT Maturity Assessment

KPMG assessed the robustness of the Horizon IT capability, by analysing how Horizon IT Services are delivered against pre-defined maturity levels from the industry standard framework for the delivery of IT services, ITIL, COBIT and CMMi and KPMG's reference IT Maturity Assessment Tool.

An assessment of 22 areas points to low maturity. Across the cycle of plan, develop, build, test, release & deploy, run & operate, monitor & improve, and manage & govern remediation is needed. For example: POL does not have a Release Management process, and the Release Manager role is taken by the Service Managers, who approve what is released into the live environments.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

2.4 Core conclusion 3

The scale of change required is significant, which includes the need to address Foundational Issues.

2.4.1 The scale of change

Section *3* of this report provides a clear impression of the scale of change required. A summary view of our observations in Section *4.2* illustrates this point, with just under half of these observations (48.6%) marked as High, requiring immediate action.

Rating	Definition	Qty.
High	High risk issues or critical gaps identified. Immediate action required to rectify	35
Serious	Serious issues or major gaps identified. Rectification a high priority	32
Minor	Minor issues or gaps identified. Mitigations planned, or in progress	2
None	No issues or gaps identified; area is on track	2
Complete	Area complete or completing shortly. No issues or gaps identified	1
TOTAL		**72**

Of the 72 observations 13 include Foundational Issues. Section *3* includes Foundational Issues, which further evidence the scale of change needed.

2.4.2 Foundational Issues

Despite the recent progress, there is no room for complacency. Our Foundational Issues are summarised in *Section 3.7* and detailed within *Section 4.*

Observations include:

- The established organisational design and culture, and the way in which process and risk are managed results in governance and process gaps, thus POL cannot demonstrate consistent management of Postmaster interests;
- the outsourcing of services to third parties resulted in an assumed delegation of accountability by POL role holders. This is being addressed by POL

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

Document Classification: KPMG Confidential

POL00337564

leadership and management to facilitate greater Postmaster reassurance that POL has control of its business and suppliers; and

- individuals have been primarily concerned with their own area of responsibility with insufficient collaboration or questioning of others, leading to a sustaining of the status quo that existed.

There is now a change in approach from POL that is addressing the previous lack of consistent, reliable management of Horizon; process, frameworks and approaches are being established or reviewed and changed. The perceived lack of collective responsibility is changing but the change must be embedded culturally.

Further, SPM with its intent is "to improve robustness and transparency, increase agility, refocus on core customers and products, whilst supporting the Network Strategy (right services, right places, right time)" must be accounted for in the content of these Foundational Issues. We have discussed the content of our report with POL Leadership. The Foundational Issues we have raised must be addressed to effectively embed and sustain the change that is needed. Some of these are being introduced in workstreams within the overall Horizon Improvements Programme V1.0, a copy of the current draft plan for which is at Section 5.5.4.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

03

Observations in summary

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

Document Classification: KPMG Confidential

POL00337564

3 Observations in summary

3.1 Horizon issues mapping

The following table depicts our understanding of the mapping of Horizon Issues Judgement to each of the six in-scope areas. It is intended to help the reader understand how each of our observations (summarised on the following pages) link to Horizon Issues.

Note this is not a definitive mapping but illustrates that there is not a 1:1 correlation between the six scope areas and Findings.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

KPMG

Post Office Limited

KPMG LLP

HIJ finding title	HIJ sub-category	HIJ Finding #	HIJ	PAM	RAM	SDLC	KELs - C	KELs - H	HNGA
Bugs Errors and Defects	Accuracy and integrity of data	1	Bugs cause discrepancies			X	X	X	X
		2	No bug/error alert			X	X	X	X
		3	Robustness			X	X	X	X
	Controls and measures for preventing/ fixing bugs and developing the system	4	Errors from forms			X	X	X	X
		5	Reconciliation			X	X	X	
		6	Controls did not stop errors	X	X	X	X	X	X
Operation of Horizon	Remote access	7	Remote access	X	X				
	Availability of Information and report writing	8	Comms to SPM & Fujitsu						
		9	Reports & investigation for SPMs	X	X				
	Access to and/or Editing of Transactions and Branch Accounts	10	Remote change with no PM consent	X	X	X			X
		11	Permission controls	X	X				
		12	PAM & records	X	X				
		13	PAM affect reliability	X	X				
	Branch trading statements, making good and disputing shortfalls	14	No dispute ability	X	X		X	X	
	Transaction corrections	15	Transaction corrections	X	X	X	X	X	X

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

KPMG

3.2 Privileged access management and remote access

Across the entire Horizon domain, there is a low level of maturity which is mostly manually based and has an uncoordinated approach across all domains of Identity and Access Management including privilege/elevated access, authentication, and controls. Moreover, visibility of vendor activity is limited, and this has not been sufficiently challenged.

The observations that align to privileged access management and remote access are as follows:

Theme	Sub-theme	Narrative
Governance	3. User identification, access management and reporting *Core systems and management of users and rights including third parties (vendors)*	• The current POL approach to Identity and Access Management (IAM) has a low level of maturity based upon industry standard measures, characterised by limited automation, undocumented processes and oversight that does not sufficiently examine or challenge vendor activity. The reliance on third parties does not alleviate this due to contractual and operational limitations. Please see *Fujitsu*, below in respect of vendor monitoring and reporting. • The low maturity of IAM and complexity of the POL/Horizon estate makes management of users and their access rights, and the reporting of this, inefficient and subject to human error as there is no single view of all users who access Horizon and its supporting systems. • Because of the current state of their identity data and processes, and vendors reporting, it is difficult for POL to confidently state or demonstrate that it has good control over users and their appropriate and timely access to Postmaster data.
	3. User identification, access management and reporting	• User lifecycle management (i.e. JML) is not timely causing exposure to users who should be removed from systems still being present, with the ability to gain inappropriate access. Re-approval of access (certification) checks are manually driven, and response rates are insufficient for POL to be confident of their effectiveness. This undermines POL's ability to adequately control timely and appropriate access to systems. • Certification is not carried out to uniform times across the user and application base, which further exposes POL in respect of users with accumulated or conflicting access rights giving excessive

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

KPMG

Theme	Sub-theme	Narrative
	Joiners-movers-leavers (JML) and certification *Post Office controlled*	authority within systems. Changes are underway to address critical areas of two points, above, under the Fast Fix programme. • The lack of user visibility through a single view across the Horizon estate inhibits risk-based good governance processes.
	3. User identification, access management and reporting *Branches*	• Postmasters can create user types and have elevated function rights, including password resets. There is a risk of manipulation or misuse of counter staff identities for which POL has no visibility, as this is deemed to be a Postmaster responsibility to manage. • Governance over Branch staff relies upon Postmasters' notifications for leavers; with over 90% of leavers only being identified by inactivity (defined as 60-90 days) reports. See Process – sub-theme 11 on next page.
	3. User identification, access management and reporting *Fujitsu*	• Fujitsu provide a PAM and APPSUP (see next page and *Appendix 4: Glossary)* user report (within the Fujitsu Security Report) to POL's ISMF for elevated and privileged users which is being improved under the Fast Fix programme but has will still have insufficient detail to understand who has done what and on which system unless detailed and timely user activity reporting is provided by Fujitsu. • The POL ISMF team should act upon the contents of the Security Report provided by Fujitsu report to demonstrate the value of the proposed improvements and POL Internal Audit reviews should consider the extent to which reports have been challenged and appropriate actions taken.Fujitsu has well documented methods which, if applied consistently, are likely to be effective and enable good governance. • User management and certification processes are likewise well documented, relying upon emails and user lists maintained in spreadsheets and local databases. Processes are regular and include both planned and ad-hoc checks. KPMG has not had the opportunity to test or observe the above points directly in Fujitsu's environment.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Theme	Sub-theme	Narrative
		• Fujitsu has limited automation for IAM and log management. Detailed reporting of user activities and events is inhibited by the current lack of a means of extracting appropriate records to enhance visibility and controls over privileged users.
Process	11. User journeys, approvals, and controls processes *Post Office controlled*	• Strong/multi-factor authentication (MFA) is not deployed extensively within POL, with only initial system sign in username and password enabling access to POL systems such as CFS (financials) and for all Branch network accounts. Though there are currently technical limitations, consideration for use of MFA, if even on a selective basis, would enhance security. The practicality of improving authentication for the Branch user network could also reduce the risk of credential sharing. The use of MFA may also alleviate concerns regarding the level of visibility and control that Postmasters have over their employee user accounts, where at present SmartID usernames and first-time passwords are communicated via the Postmaster.
	11. User journeys, approvals, and controls processes *Fujitsu*	• Postmasters manage the joiner-mover-leaver process for their employees. The leaver process, in particular, is not followed, with fewer than 10% of users who have left being notified. There is therefore opportunity for Postmasters to maintain use of a leaver's account, though if the SmartID account remains dormant the Governance process (see previous page in respect of Branch user management should capture this.
		• Fujitsu's documented manual process includes detailed matrices for user types, systems being accessed and authentication approaches to enable and mange users and for elevated access. Users are allocated "teams" which are maintained within Active Directory. Elevation processes are described and reported upon (see previous page). There has not been an opportunity to test this nor examine the user base for additional user types that may not be described within the information provided.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Theme	Sub-theme	Narrative
		• A user type known as APPSUP is used for non-balance impacting (financial) actions, such as correcting corrupted transactions, removing blocked user sessions, or rolling over trading periods. This provides a user full read/write privileges which are controlled by documented process and approval flows. The process is currently being improved to create a full audit trail that will be held in one place.
Technology	21. Tooling – IAM & GRC *(all)*	• POL makes limited use of its current commercial IAM tools to automate and improve controls within the Horizon POL estate. A strategy is being developed to address this and integration with any prospective or existing Fujitsu tooling.

3.3 SDLC, Testing and Quality Assurance

There was a lack of effective governance, control, management, and ownership across the entire SDLC until 2021. Recent changes are improving the situation.

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

Theme	Sub-theme	Narrative
1. Governance	1. Horizon governance roles and responsibilities	• During our review, we observed that the overarching accountability, ownership and responsibility for the management and control aspects of Horizon was not clearly defined; this was subsequently resolved in Feb 2021 with the appointment of a Horizon Product Owner. This Product Owner is now taking formal ownership of the Horizon Platform, with sign-off responsibility for change. A Product Strategy has not yet been developed, so the overall, detailed lifecycle for Horizon has not been implemented. This could lead to change being implemented in an ad hoc and fragmented manner, which does not align with the long-term POL strategy for the platform.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Theme	Sub-theme	Narrative
	2. Vendor management governance and oversight	• POL recognise that contract and vendor management need to be improved to enable meaningful engagement and outputs. Plans are being implemented to change the structure and approach in this important area.
	5. Test Governance	• During our review, we observed that was no effective test governance in place. This was partially resolved in Jan 2021 with the appointment of a senior test manager to take ownership of testing within the Horizon IT team. Up until that appointment, testing provided by third parties was accepted by POL unchallenged, and POL did not conduct any analysis or detailed review of the test results provided by the third parties, and there was no evaluation of the third part test outputs for quality standards or coverage requirements - as the party responsible for the Horizon platform, POL would be expected to ensure that third party testing met both industry and POL internal best practice, and without appropriate test governance structures in place, it is not possible to perform this task. There is now effort in place to rectify this gap. • There was no organisational Test Policy, test framework, test approach or test tooling in place to support POL test effort, and to guide and control third party test delivery. All test activity was outsourced to Fujitsu and ATOS, and POL retained no test knowledge, or staff skilled in testing, and so was fully reliant upon the third parties. As POL had no structure in place to validate the test approach (e.g. no quality gates were in place), scope and outputs being delivered from the third parties, there were gaps which enabled issues to leak out into Production. Actions are now being taken to implement and improve the overarching approach to testing. • There is no requirements traceability matrix in place, and traceability between test artefacts and business requirements and design is incomplete or missing. Thus, there is no apparent way to validate test coverage and scope. • POL lack a clearly defined test environment and test data strategy. The test environments for Horizon are owned and managed by Fujitsu, however POL should have a detailed understanding of the structure of the test environments, as well as the test data within those environments. This is to ensure

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Theme	Sub-theme	Narrative
		that the test environments remain reflective of the Production environment, otherwise the test environments are not supporting accurate and appropriate test effort.
	6. SDLC Governance	• POL does not have a Project Delivery Capability Framework in place, and there is no standardised SDLC delivery methodology or Project Management Lifecycle. Individual programmes can implement their own delivery mechanisms, which means that there is no consistency between ongoing programmes. Likewise, governance and control vary between programmes, with each individual programme structuring their own controls.
2. Capability	7. POL Horizon capabilities	• Although POL is implementing plans to build an in-house technical capability to manage Horizon, there remains a key reliance upon Fujitsu to manage the core Horizon platform (considering that Fujitsu retains the IP), as well as short-term contractors for technical change delivery.
3. Processes	11. Product management	• During our review, we observed that a Product Owner for Horizon was not present, and there was no Product Lifecycle in place. This was partially resolved in Feb 2021, with the appointment of a Product Owner for Horizon. The lack of a Product Owner indicates that there was no one single person with an overarching and holistic view of all the changes ongoing across the Horizon platform, with a clear and concise understanding of how these changes impact POL's business and customer front end. Without a Product Owner in place, there was no single approver for these changes, and no single person with a clear, strategic view of the platform's lifecycle. There was a risk that change introduced into the platform would not align with POL's long term, strategic goals, and that disparate change could conflict or overwrite other change being introduced at the same time. • The level of involvement from architects across the change being delivered into Horizon is limited; within POL 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

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

KPMG

Theme	Sub-theme	Narrative
		effectively applied. This has improved throughout 2021, as the recently hired enterprise architect team is reconstituting POL's understanding of the platform.
	14. Testing	• POL does not perform appropriate and effective End-to-End, User Acceptance or Non-Functional Testing. • Regression testing is patchy and poorly applied to the platform, and is not executed from a business user perspective, only from a technical functional perspective (if it is executed at all). The lack of regression testing has led to Production incidents occurring, with some of the Historic KELs being examples of these problems.
	15. Change Management	• POL has recently (Q1 2021), tightened up and improved its change control process; however not all change is funnelled through the improved process as yet (Reference Data is governed separately), and further updates are expected to occur in May and June of 2021.Whilst there has been improvement since KPMG's initial analysis in Q4 2020, there is still a great deal of further improvement yet to be implemented.
7. Supplier and performance management	20. Vendor performance management	• Service Level Agreements (SLAs) and Key Performance Indicators (KPIs) appear to be poorly defined, with performance against the KPI and SLAs being self-reported by Fujitsu, with no subsequent independent assurance activities being undertaken by POL as part of its own governance structure.
8. Technology	21. Tool Support for change delivery	• There is no standard change delivery tool used to capture User Journeys, business and technical requirements, design documentation, project management components (such as scheduling, resourcing, costs, etc.), or test management components (e.g. schedule, test scripts, test results, test evidence). Spreadsheets are used to manage some projects, which implies that many of the standard project tasks are performed manually, that there is no clear traceability, and no version control / access control to project documentation (so there is no change audit tracing).

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Theme	Sub-theme	Narrative
	24. AP-ADC scripts and Reference Data allow uncontrolled change	• Automated Payments – Advance Data Capture (AP-ADC) scripts are a means to make changes to the Horizon platform without requiring Fujitsu's input. The AP-ADC scripts have the ability to make fundamental changes to the underlying functionality of the platform, and until recently, this change was not well governed or controlled, and has resulted in defects being put into production which have caused discrepancy. • Reference Data is similar - it is a powerful tool to inject change into the Horizon platform, with few controls or governance in place. • There is a concerted effort underway to improve the governance of both AP-ADC scripts and Reference Data changes, with the aim to build a tightly controlled change process, as well as a repository of change records (see sub-theme 15 above).

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

3.4 Known error logs (KELs) – current

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.

The observations that align to current KELs are as follows:

Theme	Sub-theme	Narrative
2. Process	N/A	• Initially, the management of the current KELs was considered a "side-of-desk" best efforts endeavour added to the workload of the Horizon Operations team. The bulk of the process was owned and operated by Fujitsu, with POL involved but not directing or controlling the process. The KELs were tracked via spreadsheet, which was updated by Fujitsu, and tracked the Fujitsu based actions. • This approach was changed with the creation of the GLO IT Team, and a POL senior staff member, with a support team, was tasked to take ownership of the management of the current KELs to ensure that these outstanding items are appropriately managed, tracked and resolved. • A new process to manage KELs has been designed and has now been implemented and embedded across all stakeholders (since Jan 2021). This process will be automated and coordinated via Service Now (per Project Management documentation expected completion is May 2021), whereas previously it was spreadsheet based. Weekly reports are being produced to track the progress on resolving the current KELs, and there is oversight with a Change Advisory Board (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 onboarded to the new process; teams within POL are likewise onboarded and involved.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

KPMG

3.5 Known error logs (KELs) – historic

Initially, limited technical details for the historical KELs inhibited progress. However, POL and Fujitsu have been working in conjunction to analyse and determine the technical requirements to prove that the historic KELs either can be closed, or require further remediation to rectify.

The observations that align to historic KELs are as follows:

Theme	Sub-theme	Narrative
2. Process	16. KELs (Historic)	• The initial supplied documentation regarding the historic KELs was limited, and focused on the business components / impacts of each KEL. • For proper analysis, to determine the underlying root cause of the KEL, technical details were required. • Detailed technical workshops were held jointly by POL and Fujitsu, with the appropriate technical and operations staff involved, to tease out the required details to enable the analysis of these historic KELs. • From these workshops, POL and Fujitsu were able to determine that 45 of the 62 items could be closed, as the core system and functionality had extensively changed since these KELs occurred, and due to these changes, these specific problems could not occur again. • Of the remaining 17, POL and Fujitsu were able to determine that 14 required retesting, to validate that they no longer exist within the platform. This retesting effort is being jointly run by Fujitsu and POL, and is currently underway. Note that if this retesting does show the KEL is still extant, then the required remediation will be implemented to ensure the KEL is resolved. • Three of the historic KELs lack sufficient detailed technical information to determine what caused the issue. They also lack enough business information to determine what business process led to the issue occurring. At the time of writing, further discussion between POL and Fujitsu on the actions to be taken on these three items is planned to take place in the w/c 26th April 2021.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

KPMG

Post Office Limited

KPMG LLP

3.6 Horizon Next Generation (HNGA) Robustness

Whilst the high-level components for Business Continuity and Disaster Recovery are in place, there is a lack of detailed information and planning currently available. Usability and user interface design seems to be lacking, and is not included in the overall solution design for the Horizon platform's user interface.

The observations that align to HNGA robustness are as follows:

Theme	Sub-theme	Narrative
8. Technology	22. Business Continuity Policy (BCP) / Disaster Recovery (DR)	• Whilst there is a Business Continuity Policy in place, the next level plans do not exist. Without the business continuity plans for each business unit in place, there is no clear understanding of how the business units respond to an outage. • There is no consideration for resilience at the architectural level, the impact of which is that the solutions may not be fit for purpose from a BCP / DR point of view. • POL has no Business Impact Assessments (BIA) in place across the wider POL business landscape. BIAs are a standard component of a BCP, and inform the overall BCP approach and structure, and help prioritise the DR approach. • There is no clear linkage between the BCP approach and the DR approach, and the two areas act in siloes, where they should be tightly coordinated. • DR is disparate, and focuses on individual systems in isolation. This is due to the nature of the technological landscape within POL, with numerous third parties responsible for different areas of the overarching service. POL is not performing the required role of end owner and coordinator. • The DR approach is to repeat the same tests year on year, with no updates for results and changes to the systems.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Theme	Sub-theme	Narrative
		• Both the BCP manager and DR manager are coordinating teams of one (themselves). Based on the volume of work, and the complexity of the landscape, larger teams would be expected. • AP-ADC scripts and Reference data changes are not consistently captured within the DR space, and can be missed. This can cause issues with the DR testing, where the tests are not fully reflective of Production. This is further discussed in the "Horizon AP-ADC scripts and reference data solution" paper. Additionally, please note that the extent of this problem is difficult to quantify since there is not a reliable record of how many AP-ADC scripts there are in production.
	25. Usability and User Interface Design (Ux)	• Usability is not considered during solution design, and there does not appear to be a clear focus on the interface design and structure. Without this consideration in place, the interface used by Postmasters is complex, difficult to use, and contains legacy components which are no longer relevant.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

3.7 Foundational Issues

Foundational Issues are also present which go to the core of POL's ability to sustainably address the six in-scope areas

In assessing the six in-scope areas, we have identified a number of Foundational Issues that must be addressed to help underpin and sustain the required improvements as part of the Remediation Programme being put in place. They are summarised here and highlighted within the relevant observations within Section 4 (see Page 40 for our reading guide).

POL should consider the likelihood of these issues being reflective across the broader organisation, and having a much wider impact than just the six in-scope areas. Resolving these issues requires that organisational-wide policies, processes, and approaches are in place, and that these are effective.

Foundational issue	See section reference below for more detail
1. RACI. The accountability, ownership and responsibility for all management and control aspects on Horizon is not clearly defined between POL, Fujitsu, and other vendors. Notable gaps exist in vendor management, service performance management and contract renewal.	*Section 4.3.1 and 4.3.2*
2. Compliance. There is not sufficient collaboration in planning, monitoring and oversight of Horizon/broader POL IT compliance and risk management/3LoD.	*Section 4.3.4*
3. Risk Management maturity. POL's approach to risk assessment and management is unclear with regards to how operational IT risks are managed. This is compounded by concerns regarding the appropriate use of tooling to monitor, identify dependencies, aggregate risks, and highlight potential impacts.	*Section 4.4.1*

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Foundational issue	See section reference below for more detail
4. 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. Internal Audit reviews conducted by 3LoD tend to be thematic rather than risk based, and do not delve into Horizon-orientated IT controls to determine the effectiveness of these controls.	*Section 4.4.2*
5. Contractual Arrangements. 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. It is noted that vendor management is currently managed separately within POL to contract management, which deals purely with contract compliance. The intention going forward is for these activities to be more closely aligned.	*Section 4.4.3.*
6. IT Controls Framework. Weaknesses have been identified across the IT controls capability, including issues with content, application of the framework, reporting, governance, and technology. An effective IT risk capability requires each of these elements to be functioning correctly.	*Section 4.4.7*
7. POL Horizon capabilities and Culture There has been an apparent lack of defined, understood or acknowledged job roles in respect of incumbents' responsibilities and accountabilities in relation to Horizon, which is also observed by POL representatives, to have created an insufficiently collaborative and questioning culture. This has been especially noticeable regarding implementing change to support the Judgement issues. Detailed planning to fully address the Judgement findings is still in development. There has been limited technical ability and consequential willingness to challenge vendors within supplier relationships, with the contractual management frameworks being trusted as fit for purpose.	*Section 4.5.1 and 4.6*
9. PII at rest and in transit. POL is not Payment Card Industry Data Security Standard (PCI DSS) compliant. Horizon contains PII data - managed by Fujitsu - with data at rest and in transit not being encrypted.	*Section 4.7.1*

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Foundational issue	See section reference below for more detail
10. Key dependencies. Migration to AWS as part of the Belfast Exit is in-flight however POL still have a significant number of decisions to make (i.e. whether to stay with Fujitsu to manage Horizon or not, integration or migration of legacy product services onto AWS).	*Section 4.8.1*
11. Vendor management performance. Key Performance Indicators (KPIs) are too high-level, without well-defined service performance metrics, which is self-reported by Fujitsu and no subsequent independent assurance activities being undertaken by POL. Horizon service performance is overseen through different governance routes such as the Information Security Management Forum (ISMF) and Service Management Report (SMR).	*Section 4.9.1*
12. Tools for IAM and GRC. The use of appropriate tooling to improve efficiency, consistency of process and security is limited and further investment in the use of currently owned and new tooling will deliver significant improvements.	*Section 4.10.3*

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

04

Observations in detail

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

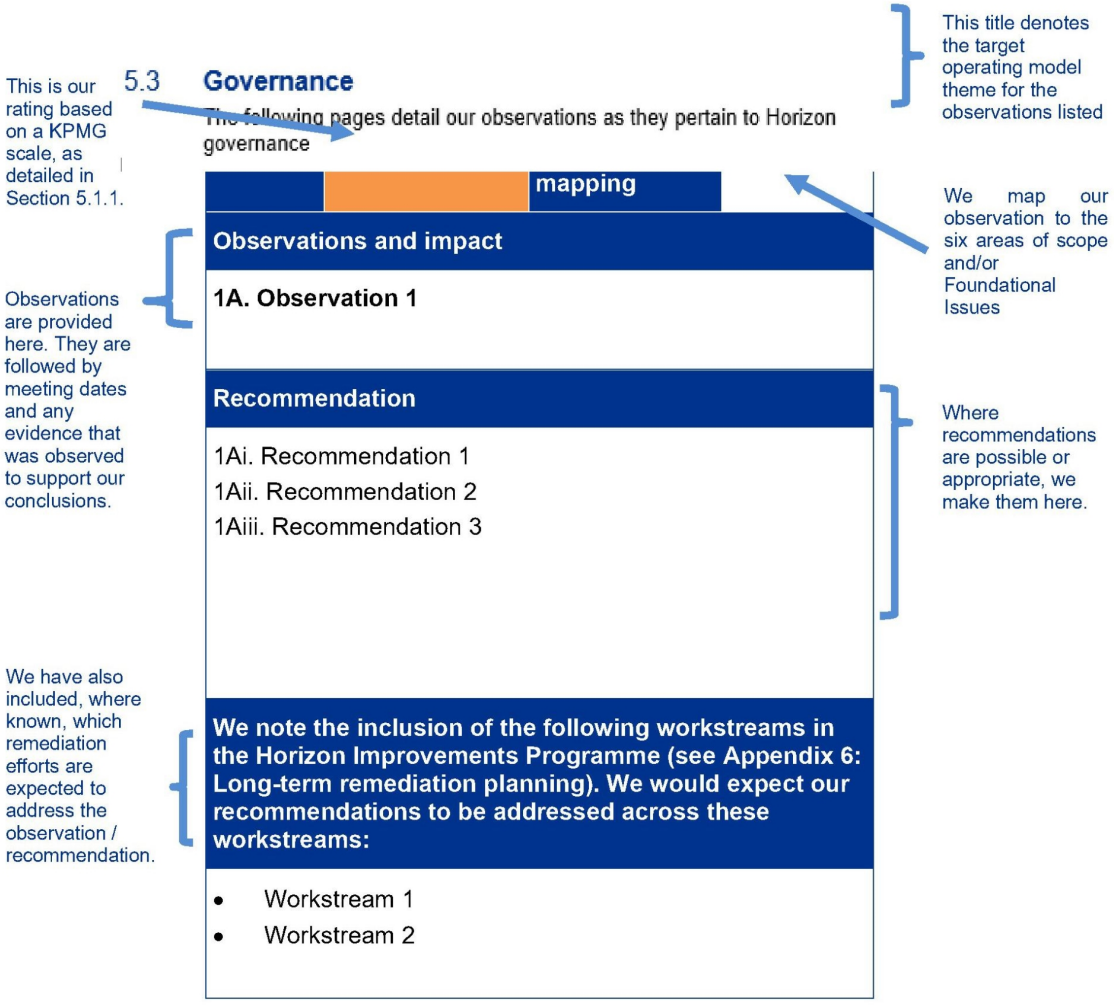
Document Classification: KPMG Confidential

POL00337564

4 Observations in detail

4.1 How to read this section

The following pages include our observations in more detail. Each page is set out as below.



© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

Document Classification: KPMG Confidential

POL00337564

4.1.1 Rating descriptions

Rating	Description
High	High risk issues or critical gaps identified. Immediate action required to rectify.
Serious	Serious issues or major gaps identified. Rectification a high priority.
Minor	Minor issues or gaps identified. Rectification not high priority, but still required in the longer term.
None	No issues or gaps identified; area is on track.
Complete	Area complete, or completing shortly. No issues or gaps identified.
Not Assessed	Not assessed during this review.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.2 Observations in detail, by theme

A total of 72 observations were made across the eight themes. Just under half of these observations (48.6%) are marked as high-risk issues or critical gaps that require immediate action.

Theme	High	Serious	Minor	None	Complete	Not assessed	
	High risk issues or critical gaps identified.	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	
Governance	13	11	-	-	1	-	**25**
Process	15	11	2	2	-	-	**30**
Capability	-	1	-	-	-	-	**1**
Culture and conduct	-	2	-	-	-	-	**2**
Data	-	1	-	-	-	-	**1**
Systems	-	1	-	-	-	-	**1**
Supplier and performance management	1	1	-	-	-	-	**2**
Technology	6	4	-	-	-	-	**10**
Total	**35**	**32**	**2**	**2**	**1**	-	**72**

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.3 Governance

The following pages detail our observations as they pertain to Horizon governance.

4.3.1 Horizon governance roles and responsibilities

Rating	Serious	In-scope area mapping	All

Observations and impact

1A. The accountability, ownership and responsibility for management and control aspects of Horizon is being addressed following the establishment of the new GLO/ Horizon IT function and the design of a governance structure which clearly defines these matters between POL, Fujitsu, and other vendors. Additionally, POL has engaged Fujitsu in the design of the new governance structure with the aim of taking learnings to relationships with other vendors. Importantly, the model being created will enable POL to migrate from Horizon to the future state under the Strategic Platform Modernisation and contribute to ensuring its success.

- Roles and responsibilities within the POL GLO/ Horizon IT function are forming and recruitment continues to build the team. The recommendations made are being addressed, however, this needs to be executed well and at speed to ensure that the impetus of the initial build up is not lost and an appropriate critical mass is achieved for the function so as not to impact the overall programme's timelines or scope.

Recommendation

1Ai. Implement a POL vendor management policy against which vendors can be measured and that clearly defines the vendor management lifecycle with defined processes, POL expectations for vendor management (such as service performance management), establishes accountability, ownership, and responsibilities.

1Aii. Within the vendor management policy, establish clear roles and responsibilities between POL, Fujitsu, and other vendors for management of Horizon, such as change, new releases, PAM / RAM, and testing.

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.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.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (*see Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- Fast Fix
- WS #1: Organisational Change and Communications
- WS #2: IT Target Operating Model
- WS #5: IT Controls

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

Document Classification: KPMG Confidential

POL00337564

4.3.2 Vendor management governance and oversight

Rating	Serious	In-scope area mapping	SDLC and Foundational

Observations and impact

2A. The implementation of a revised model for vendor management has commenced. Until this is fully developed and embedded with vendors, gaps in process and continuation the activities which were allowed by a poorly defined service performance management model will pervade.

- Until fully embedded within POL and with vendors, POL could be subject to oversights in vendor management which cause it to face and further reputational damage due to vendor shortcomings. This was confirmed during discussions with POL representatives (29-Oct-2020, 3-Nov-2020, 24-Feb-2021 and 09-Mar-2021), though no formal evidence has been supplied at this point in time.

2B. Since our initial analysis, the contractual management framework is being addressed and the changes required are understood.

- A team is in place, although the process of renegotiating the required and expected contractual controls to follow industry good practice for similar vendor contracts, and moving from the current service levels which are not tightly defined nor measurable needs vendor agreement and commercial agreement otherwise changes will rely on the good faith of vendors and not be enforceable. This is evidenced by review of the provided "Contract Management Framework Final 2020" and during discussions with POL representatives (29-Oct-2020 and 09-Mar-2021).

Recommendation

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.

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 the vendor management policy defined intervals (also please refer to recommendation 1Ai and observation 13A).

2Aiii. Within the boundaries of what can reasonably be achieved, 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.

2Aiv. Contract agreements should be discussed with relevant service areas (e.g. a business service that requires IT support should have the service levels and requirements approved by IT to ensure they align with existing/dependent services).

2Bi. Review the existing Contractual Management framework against the 'National Audit Office Good Practice Contract Management Framework' and update the existing POL framework accordingly.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

We note the inclusion of the following workstreams in the Horizon Improvements Programme (see *Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- WS #2: IT Target Operating Model
- WS #5: IT Controls

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.3.3 User identification, access management and reporting

There are **two** risk gradings in this section.

Rating	High	In-scope area mapping	PAM / RAM

Observations and impact

3A. The current POL approach to Identity and Access Management (IAM) has a low level of maturity based upon industry standard measures, characterised by little automation, undocumented processes, and limited oversight although Fast Fix improvements are underway - see 3Ai and 3G (below).

3B. Governance and administration is heavily decentralised and, in part, owned by third parties. POL has limited insight or visibility into suppliers with no contracted means of gaining this with Fujitsu. Please also see 3M – regarding Fujitsu/vendor IAM.

- The impact of observations at 3A and 3B is that POL is unable to provide sufficient assurance that user access, such as privileged access, is sufficiently well managed and the integrity of Postmasters' data is therefore protected. Moreover, the lack of a mature and consistent approach means that POL cannot currently demonstrate control over the risk of unauthorised or unaccountable access to critical infrastructure and systems, i.e. overall, POL cannot prove or verify who has or had access to what and why. This was confirmed during discussions with POL representatives (9-Nov-2020 and 17-Nov-2020) and further discussions throughout Feb-21 and March-21.

3C. Due to the decentralised model for identity within POL and the challenge presented by third party user maintenance, there is no consolidated source of truth for internal or third-party users (Fujitsu, Accenture, CC).

- 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.
- Without a single source of identity, correlation of users to system accounts is difficult as identity formats are inconsistent.
- Without a consolidated view of users, POL is unable to resolve the issues caused by the current decentralised approach, nor correlate or control third party user activity itself. This was confirmed during discussions with POL representatives (17-Nov-2020).

3D. Joiner-Mover-Leaver (user lifecycle management - "JML") governance is inefficient and inconsistent across POL with approval of access rights (certification), access approvals and reporting run separately for different user groups.

3G. POL defined Branch network roles such as Branch Managers, Auditor E, and Admin do not have any Segregation of Duties (SOD) rules in the system and allocation of roles is inconsistent. The creation process is paper based and does not check for SOD, and the recertification process does not check for adherence to the joiner processes.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

- This exposes franchise owners (Postmasters), 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), subsequent discussions in Feb, March and April-2021, and email received (26-Nov-2020,14:22) "RE: Global User Admin Access.msg".

Please also refer to Process: User journeys, approvals, and controls processes.

3H. User access review timings are not uniform; remediation tracking is not streamlined and mostly manual. Six-monthly access reviews are conducted by the Data Services Team for Global Users, which include Fujitsu users, and CFS (financial system), by emailing users' respective line managers. The response rates to the reviews are not satisfactory nor timely.

- The window of exposure to accumulated privileges/inappropriate access is between 6-12 months, assuming responses are obtained. This was evidenced during discussions with POL representatives (17-Nov-2020), various meetings in February and March and reviews of emails received (24-Nov-2020) "FW: Global User accounts - removal from stock units.msg".
- Although leaver checks are carried out weekly based on a report from HR, with remediation taking between 1 – 6 days, there is still a residual access exposure of 7 – 14 days. This was confirmed during discussions with POL representatives (17-Nov-2020).

3J. Reporting of PAM and APPSUP user account activity is provided by Fujitsu to POL ISMF on a monthly basis although this is not a contracted requirement for Fujitsu.

3K. The Fujitsu Security Report, which includes RA and APPSUP log details and joiner-mover-leaver activity, is being revised as a part of the Fast Fix programme to introduce: a Unique identification (UID) for users, PAM elevation occurrences with additional platform detail, and an agreed monthly delivery date for the report. This will enable users to be consistently viewed month to month and provide improved visibility of the systems they access. This was confirmed in discussions with POL and Fujitsu representatives at a series of meetings in March and April 2021.

3L. KeePass/generic privileged accounts (*see 11G, Section 4.4.6*) are not reported.

- The report whilst improving visibility is still limited in detail and scope and inhibits POL's ability to ensure Fujitsu manages its user in a timely manner. The lack of detail in the report may cause POL staff to not consider its content as having sufficient value and therefore not challenge its content.

3N. Although Fujitsu maintain logs for the various systems, the point is made by Fujitsu in their RA report to POL (*see Appendix 1: Documentation*) that, *"logs are extremely large and interspersed with other activity logging"*.

- The lack of ability to extract meaningful logs causes POL to be heavily reliant upon the monthly retrospective Security Report and inhibits POL's visibility of user activity. Fujitsu have previously suggested enhancing log reporting by deploying additional tooling, but this has been deemed cost prohibitive. This was confirmed during written exchanges with Fujitsu referred to at *Appendix 1: Documentation* although KPMG has been unable to test this with Fujitsu.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Recommendation
3Ai. POL has commenced a remediation programme (Fast Fix) to prioritise high-risk/Horizon Issues-related exposure points, review, remediate and improve, and document manual processes for governance to improve consistency, ensure appropriate approvals and traceability (auditability) of requests/actions taken. 3Aii. Continue 3Ai activities whist developing a roadmap to move from a primarily manually driven, undocumented approach to user lifecycle and access management to one which is optimised and ensures a consistent, auditable, and cost effective approach with strong policy, controls and accountability for identity and access management. 3Aiii. Execute against the roadmap to a risk-based approach, supported by a suitable IT controls framework *(see Section 4.4.7* *IT Controls* Framework*).* 3Bi. Establish strong policy, controls, and accountability within POL Horizon team and with vendors for identity and access management/governance for third-party users. *Please see Observation 3M regarding Fujitsu/vendor IAM observations.* 3Ci. Establish a single source of truth for identity of all users or by user type (employees, non-employees (third parties), service accounts etc.) and have reliable correlation between accounts and users. 3Cii. Examine the feasibility and implement a means of obtaining live user data from vendors to enable active management and visibility of users across the Horizon estate OR create a consolidated view for third party users (in particular Fujitsu) and consider use of a reporting tool to aid governance and understanding of third party users. *Please see Recommendation 3M regarding Fujitsu reporting.* 3Ciii. Please see *Section 4.10.3* Technology – Tools for IAM and GRC – which highlights existing tooling which should be considered as a part of this approach. 3Di. Establish central and unified JML processes, including immediate termination of rights for movers and leavers, with associated SLAs for users across Branches, global users, and third-party users. 3Gi. Review elevated access and identify toxic combinations. Establish strong SOD policies and a process to handle violations, exceptions and remediations. 3Gii. Planning is underway as a part of Fast Fix to ensure that POL creates and implements documented governance processes to ensure that roles are consistently and appropriately allocated to users, whilst developing a broader Identity and Access Management strategy. 3Hi. Identify all applications that impact the Horizon estate including CFS, re-define the frequency of access recertification (continued access rights) based upon level of risk, ownership, and SLA's for access remediation. 3Hii. Reduce manual intervention in the access recertification and remediation process through automation. 3Hiii. Identify Fast Fix components to reduce risk, such as increasing the frequency of access reviews and suspending users where there is no activity or where managers have not responded.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

3Ji. The provision of the report should be formalised within the existing Fujitsu-POL contractual framework.

3Ki. POL changes to address the observations are currently being discussed and should be seen as the minimum reporting requirement for POL. These include a Unique identification (UID) for users, PAM elevation occurrences with additional platform detail and an agreed delivery date for the report.

3Kii. ISMF should act upon the contents of the report to demonstrate the value of the proposed improvements and POL Internal Audit reviews should consider the extent to which reports have been challenged and appropriate actions taken.

3Li. Additional changes to reporting should include reporting of PAM account changes (i.e. changes in privileges) and use of KeePass/generic privileged accounts *(See Section 4.4.6 User journeys, approvals, and controls processes: Fujitsu HZ-managed* environment*).*

See 3N regarding log production and automation.

3Ni. Consideration should be given to improving the approach to log capture and analysis.

3Nii. As a part of the Identity and access management strategy being developed, specific to the Fujitsu estate, consideration should be given to session recording or key logging for specific activities. This enhanced visibility would alleviate the problem described by Fujitsu regarding logs.

Please see Recommendation (3K) regarding improvements to the current reporting process.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (*see Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- Fast Fix
- WS #2: IT Target Operating Model
- WS #7: Security
- WS #9: Tooling

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Rating	Serious	In-scope area mapping	PAM / RAM

Observations and impact

3E. The Governance (approvals) for Global users and CFS (POL's SAP system) are manually managed by approvers from historic lists. It is our understanding that Fast Fix improvements are being commenced to resolve this – see 3Eli.

- The impact of observations 3D and 3E is the approaches are 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 subsequent meetings in March and April-21 and review of email received (26-Nov-2020, 14:22) "RE: Global User Admin Access.msg".

3F. Within the POL domains there are limited policies and no guidance or controls that are sufficient to manage enablement/approval of users, including for elevated access, with activities being accepted common practice and/or relying on historic documents and lists.
Manual controls are being improved and documented through the Fast Fix programme whilst a broader Identity and access management strategy is developed.

- This results in a lack of meaningful governance, thus evidencing, of the approval processes and exposure to risk of inappropriate access. This was evidenced in conversations with POL Data Services Team 25th March 2021 and Horizon Live Service Team during February and March 2021.

3I. Postmasters have full access to Branch user management functions, such as create Horizon accounts, and management of passwords for these accounts independently of POL's Data Services Team. Elevation of user authority in Branches is not reviewed or controlled by POL. POL Branch user administration is inefficient and the expediency of an informal approach to allow a Branch to run effectively by retaining or sharing user accounts is a known issue with no current practical resolution. The team managing users report that over 90% of Branch leavers are not notified to POL.

- 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 POL-franchised Branches is the business owner, i.e. the Postmaster. This was confirmed during discussions with POL representatives (3-Nov-2020) and subsequent discussions in March and April-21.
- 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).

Please also refer to 'Section 4.4.5 User journeys, approvals, and controls processes' in respect of SmartID/Branch user process.

3M. Certification (user access rights governance) is a well-documented manual process (i.e. supported by spreadsheets and email requests). It is performed on a monthly basis. Access revocation is either by an Assignment Manager's instruction, as part of the monthly verification process, inactivity of more than 90

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

days or during a security spot check outside of the monthly certification (verification) process. Segregation of duties (checking a user's role doesn't conflict) is additionally managed as part of a second monthly check.

- The well-documented manual process relies upon human diligence for timeliness and thorough responses; thus, errors could occur, allowing inappropriate access. A window of 90 days for inactivity is an excessive risk exposure. This was confirmed during written exchanges with Fujitsu referred to at *Appendix 1: Documentation* although KPMG has been unable to test this with Fujitsu.

Recommendation

3Ei. Pending any automation process, POL is remediating this by updating the approvers lists and ensuring these are maintained on a quarterly basis.

3Fi. In line with the improvements at 3Ai and 3Aii, documentation, guides and training should be developed, including improving current manual controls and approver lists for all systems or processes that hold critical data. The current Fast Fix plan addresses this for areas including CFS and POL approvals for Fujitsu elevated activities – *see Appendix 5: Short-term Fast Fix tactical remediation* for a high-level view of the Fast Fix programme.

3Fii. Ensure all processes are appropriately monitored and reviewed in their manual and future automated states.

3Fiii. Improve current processes to introduce maker-checker (four eyes) controls where appropriate (i.e. as with the GLO user enablement.- planned Fast Fix).

3Ii. Postmasters should be reminded of the importance of good governance of their users and the process for mover/leaver notification should be reviewed.

3Iii. Educate Branch owners and staff on the risks and impact of shared (borrowed) user identities and logins.

3Iiii. Increase the frequency of user verification/inactivity to reduce the likelihood of leaver/shared account misuse.

3Li. and 3Mi. As a part of POL's assurance process, it is recommended that agreement is reached to test user cases which provide the greatest risk to Branch data. Due to Fujitsu's concerns around the potential risks exposed in disclosing personally identifiable information of its employees, this would need to be performed as a walk-through against a scripted process with obfuscated logs as evidence.

3Mii. The 90-day window for inactivity should be reduced to a maximum of 21 days after an account becomes dormant.

Please see the previous page regarding improvements to the current reporting process.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (see *Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- Fast Fix
- WS #1: Organisational Change and Comms
- WS #7: Security
- WS #9: Tooling

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.3.4 Compliance

There are **two** risk gradings in this section.

Rating	Serious	In-scope area mapping	Foundational

Observations and impact

4A. POL has a thorough approach to its Regulators and bodies it must comply with such as the Link Network (ATM's), though there is not sufficient collaboration in planning, monitoring and oversight of Horizon/broader POL IT compliance and risk management/3LoD.

It is noted that POL is the Appointed Representative (AR) of directly regulated firms for the distribution of banking and insurance products. This does not include banking framework services. This does not mean POL are regulated in this space, though it is accepted that demonstrating 'compliance in spirit' is recommended and its Regulated providers should direct POL on how this should be interpreted.

- Compliance is well managed at a business level. However, the interpretation of requirements into IT/security controls is not sufficiently developed and therefore the ability of POL to manage its associated risks, including POL's Internal Audit teams ability to provide evidenced reporting is limited.

  This is particularly relevant where POL is an AR of directly regulated firms i.e. its third parties, where POL must satisfy the AR that they are 'compliant in spirit'. Without such, POL risk significant fines, damage to reputation and the possible withdrawal of 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 and March 2021).

Please see Section 4.4.7

IT Controls Framework.

Recommendation

4Ai. Compliance approaches should be embedded within the appropriate operating models/frameworks – Risk, IT operations, Internal Audit, etc. including where POL relies upon third party services.

4Aii. Review the IT risk management framework against identified and prioritised risks to establish if compliance expectations are appropriately reflected.

4Aiii. Establish clear responsibilities and plans for appropriately authorised individuals with pathways for escalation to leadership.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (see Appendix 6: Long-term remediation planning). We would expect our recommendations to be addressed across these workstreams:

- WS #5: IT Controls
- WS #7: Security
- WS #8: Internal Audit and Risk

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Rating	Complete	In-scope area mapping	Foundational
Observations and impact			
4B. Fujitsu and POL have recently agreed and signed a change notice within their contracts regarding our observation on issues regarding their GDPR regulatory requirement. • This was confirmed during discussions with POL representatives (April 2021). *Please see Section 4.7.1 Personal Identifiable Information (PII) at rest and in transit.*			
Recommendation			
4Bi. Update the Technical Risk Register maintained by POL to close off the risk. *Please see Section 4.7.1 Personal Identifiable Information (PII) at rest and in transit.*			
We note the inclusion of the following workstreams in the Horizon Improvements Programme (*see Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:			
N/A			

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.3.5 Test Governance

There are **two** risk gradings in this section.

Rating	Serious	In-scope area mapping	SDLC

Observations and impact

5A. A draft organisational Test Policy has been created and signed off by POL and is now with the third parties for review. A draft test framework has been created, and is under review with POL.

- The lack of a test policy was identified as a gap in KPMG's initial analysis in Q4 2020. An organisational test policy has since been produced. Once this is accepted by the third party suppliers, this must be embedded across Horizon test delivery.
- The test framework was also not in place; a draft framework is in the process of being built and reviewed by POL.
- This was evidenced during discussions with POL representatives (2-Nov-2020) and ATOS representatives (11-Nov-2020), and further sessions throughout Jan-21 and Feb-21.

5B. Test Governance is fragmented and is applied inconsistently.

- There is 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).
- Discussions between POL and FJ have commenced to determine how this gap can be resolved.

5C. Requirements traceability is incomplete or missing.

- 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), and ongoing conversations throughout Feb 2021 and Mar 2021.

Recommendation

5Ai. Finalise and embed the organisation wide Test Policy across Horizon test delivery, including third party test delivery.

5Aii. Finalise and embed the test framework, which outlines and determines the required test deliverables for each type of test engagement.

5Bi. Determine what is required to resolve the gaps, and agree to implement appropriate and effective test governance to ensure that all testing follows and adheres to POL's test framework.

5Ci. Traceability of requirements should be both mandatory and automated via an appropriate tool.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

We note the inclusion of the following workstreams in the Horizon Improvements Programme (see Appendix 6: Long-term remediation planning). We would expect our recommendations to be addressed across these workstreams:
• Fast Fix • WS #5: IT Target Operating Model • WS #9: Tooling

Rating	**High**	**In-scope area mapping**	SDLC

Observations and impact

5D. Lack of a clearly defined test environment and test data strategy.

- 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.
- The management of test data does not appear to be a high priority, and test data does not appear to be tightly controlled. The test data within the test environments is not kept up to date (i.e. reflective of Production), and does not seem to contain a representative mix of data points.
- 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), and ongoing conversations throughout Feb 2021 and Mar 2021.

Recommendation

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.).

We note the inclusion of the following workstreams in the Horizon Improvements Programme *(see Appendix 6: Long-term remediation planning)*. We would expect our recommendations to be addressed across these workstreams:
• Fast Fix • WS #5: IT Target Operating Model • WS #6: Data • WS #9: Tooling

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.3.6 SDLC Governance

There are **two** risk gradings in this section.

Rating	High	In-scope area mapping	SDLC

Observations and impact

6A. POL does not have a formal Programme or Project Software Delivery Lifecycle (SDLC) methodology

- Whilst POL does have a formal Portfolio Management Process, it does not have a standardised Project Management Lifecycle or a SDLC delivery methodology that specifically outlines the delivery approach to be used, how the programme or project will function, and how the change will be delivered by the programme or project. The decision on which programme delivery methodology to use has been delegated to the individual programmes or projects. The impact of this approach is that no project will align in its approach, and each project will be structured differently. This also increases the complexity of project governance, as each project has different quality gates, milestones, delivery structures and ways of managing third parties. This was evidenced during discussions with POL representatives (29-Oct-2020, 2-Nov-2020, 3-Mar-2021).

Initial discussions have commenced between POL stakeholders as to what tooling requirements are required to manage the SDLC lifecycle.

Recommendation

6Ai. Formalise and implement a standardised SDLC methodology which describes how POL expects technical change delivery to occur. This methodology should adhere to accepted universal standards of software delivery. Whilst third parties can, in their responsible components, follow their own internal processes, once the change moves under POL's control, the change should be governed under this standardised methodology.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (see Appendix 6: Long-term remediation planning). We would expect our recommendations to be addressed across these workstreams:

- WS #5: IT Target Operating Model
- WS #9: Tooling

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Rating	Serious	In-scope area mapping	SDLC

Observations and impact

6B. Documents do not adhere to POL standard templates, and the quality of the documents varies greatly. Sign-offs for documentation also vary.

- 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".

Recommendation

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.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (*see Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- WS #5: IT Target Operating Model
- WS #9: Tooling

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.4 Process

The following pages detail our observations as they pertain to Horizon process.

4.4.1 Risk management authority

Rating	High	In-scope area mapping	Foundational

Observations and impact

7A. POL's approach to risk assessment and management is insufficient for a business of its complexity and community importance.

Although Risk Registers exist at a central, project and technical level, these are not sufficiently developed. Risks identified do not reflect the business priorities and are poorly managed.

- This inhibits the ability of POL's ISMF and management to advise, challenge and respond to risks. This could lead to high-impact risks not being identified and open risks not being addressed resulting in misalignment with POL's risk appetite, exposing POL to potential regulatory criticism and future reputational damage. This was confirmed during discussions with POL representatives (3-Nov-2020) and March 2021, and review of evidence provided (26-Nov-2020) "20201104 Security Risk.xlsx".

Please also see Sections:

4.4.2 Risk management at Three Lines of Defence (3LoD),

4.4.7

IT Controls Framework, *and*

4.10.2 Business Continuity Plan (BCP) / Disaster Recovery (DR).

7B. POL is migrating from its Archer risk management framework tool to ServiceNow as part of a platform consolidation process. It is building risk registers to track monitor, identify dependencies, aggregate risks, and highlight potential impact on the new platform, building a strategic risk management tool. This is a positive step to platform consolidation.

- The migration needs to be built upon by POL's Horizon team to ensure the shortcomings of the former Archer platform are not replicated, where only high-level and generic risks were recorded, and little value was seen in the platform.

  Successful implementation will enable an approach where controls, risks and remediation are all managed through one platform enabling management of internal controls to provide complete and accurate reporting metrics leading to efficient and effective strategic and operational decisions being made by POL leadership. This was confirmed during discussions with POL representatives (3-Nov-2020), subsequent discussions in March-21, and review of evidence provided "20201104 Security Risk.xlsx" (26-Nov-2020).

Recommendation

7Ai. Risks should be evaluated and managed on the basis of the likelihood and impact to the business.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

7Aii. POL should ensure that IT/security and general risks are commonly manged where appropriate across the HZ and general POL domains.

7Aiii. Establish a clear process for risk and dependency management with defined roles and responsibilities.

7Aiv. Re-evaluate risk management processes to identify gaps and remediate accordingly.

7Bi. Build upon the migration and leverage the ServiceNow platform capabilities to enable a single pane approach across all relevant teams and improved collaboration.

7Bii. Ensure Risks, Assumptions, Issues and Dependencies (RAID) are developed to reflect the current and evolving risk landscape, and are tracked and maintained.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (*see Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- WS #5: IT Controls
- WS #7: Security
- WS #8: Internal Audit and Risk
- WS #9: Tooling

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.4.2 Risk management at Three Lines of Defence (3LoD)

Rating	High	In-scope area mapping	Foundational

Observations and impact

8A. POL The annual Service Organisation Controls Report ISAE3402 (SOCR) obtained from Fujitsu reviews high level infrastructure controls and does not provide reasonable assurance for Fujitsu managed controls over Horizon as the report does not provide assurance over the design and operating effectiveness of the controls.

We also noted that Internal Audit currently reviews the SOC report ISAE3402 informally. See also 8B.

- Lack of assurance over the design and operating effectiveness of the controls regarding Fujitsu managed controls in respect of Horizon can result in lack of effective management of Fujitsu as a vendor, resulting in regulatory criticism, potential fines, reputational damage and possible further litigation against POL (3-Nov-2020, 5-Nov-2020 and 2 March 2021).

8B. Third LoD Internal Audit assurance activities are based on thematic reviews. These reviews do not call out or specifically include assurance over controls around Horizon which can result in a lack of risk management activities and appropriately scoped reviews of in-house and outsourced controls around Horizon.

- This could result in, insufficient management of Fujitsu 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 and 2-March-2021).

Recommendation

8Ai. Internal Audit should formalise the reviews of the Service Organisation Controls Report ISAE3402 (SOCR) obtained from Fujitsu and ensure the evidence of reviews are retained for audit trail purpose. 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.

8Aii. Internal Audit should consider obtaining SOC 1 / SOC 2 reports from Fujitsu in order to get comfort over the design and operating effectiveness of the controls.

8Bi. IA should review their strategy and approach and consider whether thematic approach is adequate around Horizon and also consider revisiting the IT Controls framework to ensure if it drills down to the granular level of applications.

8Bii. As part of the collaborated efforts between second and third LoD , third LoD to continually monitor emerging risks regarding the Horizon estate and supporting resources, conduct business monitoring, risk assessments and refresh audit plans accordingly and formalise the communication with risk and 2nd LoD.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

Document Classification: KPMG Confidential

POL00337564

We note the inclusion of the following workstreams in the Horizon Improvements Programme (*see Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:
• WS #8: Internal Audit and Risk

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.4.3 Contractual Arrangements

Rating	High	In-scope area mapping	Foundational

Observations and impact

9A. 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 have the ability to apply the latest business needs or re-evaluation of the required service levels against the contracts.

- This has caused significant gaps between business needs and vendor provided services resulting in vendors not meeting with POL's expectations or needs to deliver a service to its Postmasters and customers, and leading to contractual and Horizon performance issues. This was confirmed during discussions with POL representatives (29-Oct-2020 and subsequent discussions 29-Jan-2021, 24-Feb-2021, 09-March-2021).

Recommendation

9Ai. Determine the key issues and gaps within the service delivery, and address these core issues within the vendor contract.

9Aii. Implement POL process to assure and present challenge to Fujitsu and other relevant vendors as a part of the revised operating model. It is recognised that the post holder in the POL Horizon IT function is providing more challenge to Fujitsu, however this will require more formality to ensure vendors provide what is required.

9Aiii. Implement appropriate and required SLAs to ensure that Fujitsu meets POL's expectations when delivering support service regarding Horizon. This will require contractual re-negotiations between POL and Fujitsu to implement.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (see Appendix 6: Long-term remediation planning). We would expect our recommendations to be addressed across these workstreams:

- WS #2: IT Target Operating Model

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.4.4 Product Management

Rating	Serious	In-scope area mapping	SDLC

Observations and impact

10A. Initially there was no Product Owner for Horizon; a Product Owner has now been assigned (from Feb 21).

- Up until the appointment of the GLO-/IT director there was no single person responsible for ownership and formalised coordination of the Horizon platform - i.e. with responsibility across change, operations, strategic vision, business support, etc.
- Updates are made based on requests by Business Product managers with limited oversight from POL IT on sequencing and prioritisation.
- These items were evidenced by discussions with POL representatives (22-Oct-2020 and 28-Oct-2020).
- A Product Owner has now been assigned, and is taking overarching ownership of the platform.

10B. Level of involvement from architects is limited.

- Late or inadequate engagement of a Solution Architect have resulted in poor documentation (including design documentation) thereby resulting in design issues/gaps. This was evidenced by discussions with POL representatives (22-Oct-2020).
- Effort is now taking place to rectify this gap, and improve architect involvement. Documentation is being reconstituted.

Recommendation

10Ai. The Product Owner now needs to take formal ownership of the Horizon Platform, with sign-off responsibility and accountability for change being delivered into the platform.

10Aii. With the Product Owner assigned, the next main action is to develop a Product Lifecycle for the Horizon platform.

10Bi. Mandate early and continuous engagement of enterprise and solution architects for any change across Horizon.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (see *Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- Fast Fix
- WS #2: IT Target Operating Model
- WS #3: Horizon System Improvement

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.4.5 User journeys, approvals, and controls processes

There are **three** risk gradings in this section.

Rating	Serious	In-scope area mapping	PAM / RAM

Observations and impact

11A. Multi-factor authentication (MFA) is used by support staff but its use is not extensive, and consideration may be given to enhancing POL and Postmaster staff authentication with its use. The current username and password approach in a number of areas could be elevated as there is a concern regarding the assurance of user identity and thus security.

- The current approach can allow the impersonation of users, compromising auditability and security. This was confirmed during discussions with POL representatives (19-Nov-2020, during Feb-21 and March-21).

11D. Though SMARTIDs are owned by POL employees, logon information is shared via the Branch managers' email addresses and password management for Branch staff is solely administered by Branch managers.

- 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 and 26th March 2021).

Please also see Governance 3I - User identification, access management and reporting.

Recommendation

11Aii. Consider enabling MFA for users where there is the potential for credential theft, and assess the benefits for extending this to Branch user access.

11Di. A more thorough review of the current SmartID processes is recommended to ensure any exposures to sharing of personal login data is limited and that it cannot be subsequently exploited.

11Dii. Examine the feasibility of implementing maker checker (four eyes) controls (manual or automated) for all Joiner Mover Leaver (JML) actions undertaken by Postmasters.

11Diii. Assess the practicality of defining and implement segregation of duties for elevated access roles such as Branch manager and implement if feasible.

11Div. Establish strong controls over Branch manager access. Ensure adequate logging, monitoring, and reviewing is enabled.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (see Appendix 6: Long-term remediation planning). We would expect our recommendations to be addressed across these workstreams:

- WS #7: Security
- WS #9: Tooling

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Rating	High	In-scope area mapping	PAM / RAM

Observations and impact

11B. Joiner Mover Leaver (JML) process for SMARTID/Branch login is insufficiently governed by Postmasters and POL with leavers in particular not being well managed and leaver detection largely based on inactivity.

- There is a lack of in-house POL controls or oversight on creation and use of Branch staff accounts. This was confirmed during discussions with POL representatives (17-Nov-2020).
- Dormant SmartID account policy is not efficient, based upon a 60 – 90 days' inactivity window. This was confirmed during discussions with POL representatives (17-Nov-2020 and further discussions in March and April 2021).

11C. It is known that inactive SMARTIDs are actively transacting.

- The current SmartID process has known gaps, though the overall process enables POL to tie an individual's National Insurance number to a user account, and prevent multiple simultaneous logins with the SmartID.
- However, it 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 ".

11E. For the staff of a Post Office. leavers' accounts remain available and are "useful" where staff replacements are waiting for their own accounts.

- 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) and in subsequent conversations in March and April 2021.

Recommendation

11Bi. JML processes for SMARTID must be defined, periodically reviewed, and updated as necessary.

11Bii. Immediate termination of leavers is recommended for SMARTIDs as they provide critical access to Horizon and Branch hub.

11Biii. Assess current operations and identify opportunities for automation to improve efficiency and reduce human error.

11Biv. Consideration should be given to the practicality of an interim solution using, say Branch Hub, to raise tickets for leavers.

11C. Refer to 11Bii.

11Ei. Check and address devolved policies and contracts, training and understanding for:

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

- Employment contracts for staff,
- Regulations and processes in particular for Postmasters (Direct and Franchisee), and
- Internal Audit reviews of these at a Branch level.

Consider these in the viewpoint of franchisee enablement and within the Postmaster Journey workstream (see Section *4.11*).

11Eii. Refer to 11Bii.

We note the inclusion of the following workstreams in the Horizon Improvements Programme *(see Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- WS #1: Organisational Change and Comms
- WS #7: Security
- WS #9: Tooling

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Rating	Minor	In-scope area mapping	PAM / RAM

Observations and impact

11F. Post-Covid, two POL staff members can create, amend, and delete GLO Branch users and the setup does not have a four-eyes (maker-checker) approach to protect the individual and POL as a good governance process.

- The lack of process assurance for user setup exposes the unobserved and un-checked actions of the operatives to future examination and is a risk exposure for POL which could be easily resolved with an improved maker-checker process. This was confirmed during discussions with POL representatives (17-Nov-2020 and during March and April 2021) and email received (18-Nov-2020) "FW: Post Office Limited Horizon discussions - follow up check".

Please see Section 4.3.3

Recommendation

11Fi. Implement a maker-checker (four-eyes) process as an interim solution as part of Fast Fix.

11Fii. If staff move back to an office-based environment re-examine the process to maintain the proposed four eyes approach.

11Fiii. Ensure that the interim fix is established within future automation.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (*see Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- Fast Fix
- WS #5: IT Controls
- WS #7: Security

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.4.6 User journeys, approvals, and controls processes: Fujitsu HZ-managed environment

There are **four** risk gradings in this section.

Rating	High	In-scope area mapping	PAM / RAM

Observations and impact

11G. Generic privileged accounts are maintained in a KeePass environment. In addition, emergency access group privilege accounts are used for scenarios where the Fujitsu POA security team must forcefully gain access due to account lock out.
These are manually maintained and, although the process is reported by Fujitsu as "documented", POL visibility regarding their use and detail of underlying activity are limited.

- Such accounts have extensive rights and ability to change data and their use can be highly impactful. Anonymised users or group accounts should be closely managed and reported upon with approvals and effective escalation processes for emergency situations. This was confirmed during written exchanges with Fujitsu referred to at *Appendix 1: Documentation* although KPMG has been unable to test this with Fujitsu.

Recommendation

11Gi. POL and Fujitsu should review the documented approach between the organisations and reporting approach for these specific account types as a priority for good governance.

11Gii. Due to the impactful nature of such accounts, POL and Fujitsu should consider a documented approval process that is auditable, similar to that being agreed for APPSUP.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (see *Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- Fast Fix
- WS #5: IT Controls
- WS #7: Security

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Rating	Serious	In-scope area mapping	PAM / RAM

Observations and impact

11H. The process of creation, validation (certification) and revocation appears to be well documented and managed, based upon the information provided. Workflows have been provided to illustrate creation, approval, revalidation, and activity monitoring within the Fujitsu Europe Business Management System. Although these processes are manual, as described, they appear to be repeatable and documented, providing a level of assurance over them having some degree of maturity.

- Whilst the process appears well-documented and managed, the lack of process automation relies upon human diligence for check-in-check-out, password rotation and limited time usage, thus errors can occur. This was confirmed during written exchanges with Fujitsu referred to at *Appendix 1: Documentation* although KPMG has been unable to test this with Fujitsu.

11I. The primary HZ user store is the Fujitsu AD system which controls and defines all access and connectivity controls. These include the mandating of multi factor authentication for remote access and appropriate role limitations in order to preserve appropriate segregations of duty. Rules are well documented.

Unix, Oracle, and Windows platforms plus the service databases (Oracle and SQL) have administrative staff assigned to them. These assignments (roles) are controlled by AD-driven groups (also termed "teams" by Fujitsu) within the Fujitsu HZ domain. Access management is based upon documented rules and role models and appear to be well designed and appropriately maintained for what is a primarily manually managed approach. The access controls afforded by user group membership are further managed on a use-case basis, such as user access to a location or device.

- KPMG has been unable to test the provided accessibility matrix to ensure there are no technical or procedural gaps in the controls.
- The use of manual controls is an exposure and with no automation there is no likelihood of prevention or alerting for bad actors. This was confirmed during written exchanges with Fujitsu referred to at *Appendix 1: Documentation* although KPMG has been unable to test this with Fujitsu.

Recommendation

11Hi. The practicality of investment in a privileged access management (PAM) tool seems low within the current contractual arrangement and lifecycle of the Horizon platform. If this is the case, consideration should be given to improvements in reporting and POL IA assessments to partially alleviate the lack of automation and improve POL's visibility of process.

11Ii. As a part of the POL risk management and assurance process it is recommended that agreement is reached to test use cases which provide the greatest risk to Branch data. Due to concerns around the potential for disclosure or misuse of personally identifiable information raised by Fujitsu on behalf of its employees, this would need to be performed as a walk-through against a scripted process with obfuscated logs as evidence.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

We note the inclusion of the following workstreams in the Horizon Improvements Programme (*see Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:
• WS #7: Security • WS #8: Internal Audit and Risk

Rating	**Minor**	**In-scope area mapping**	PAM / RAM

Observations and impact

11J. A role known as APPSUP is used for non-balance impacting actions, such as stock unit associations, month end rollovers, or monthly tidying of dispatch reports. The APPSUP role provides full data read/write privileges on Oracle systems. This is subject to an approval process which includes both POL and Fujitsu managers and is currently being improved and documented to create a clear, evidence pack from request to completion within the Fast Fix programme.

- The process and changes being enacted are critical to evidencing agreed changes, which if unapproved may be deemed to be to the Postmaster's detriment. The approach will demonstrate POL has provided appropriate oversight with a consequence that the audit trail is operationally complete. This was confirmed during written exchanges with Fujitsu referred to at *Appendix 1: Documentation* and conversations with POL and Fujitsu representatives involved in the improvements

Recommendation

11Ji. This process should be completed, maintained, and integrated into future automation processes as a priority

11Jii.The agreed process should be agreed under a Change Notice to ensure it is binding on Fujitsu.

11Jiii. The currently proposed remediation should be communicated to Postmasters, Investigations, and other appropriate POL/Fujitsu staff as it sets a reassuring standard of process integrity and auditability.

11Jiv. The agreed approach should be considered for adoption in other similar use cases, such as KeePass (*see 11G, section 4.4.5*.).

We note the inclusion of the following workstreams in the Horizon Improvements Programme (*see Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:
• Fast Fix • WS #1: Organisational Change and Comms • WS #7: Security • WS #8: Internal Audit and Risk

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Rating	None	In-scope area mapping	PAM / RAM
Observations and impact			
11K. The Fujitsu Transaction Correction Tool has been retired and its function replaced by the APPSUP process and is therefore not covered within the KPMG report. It should also be noted that the POL Branch Reconciliation Team (BRT) operates a transaction correction process which is used to correct SAP account balances and is not a part of the Fujitsu-operated processes.			
Recommendation			
11Ki. POL should seek written confirmation regarding the Transaction Correction Tool's retirement.			
We note the inclusion of the following workstreams in the Horizon Improvements Programme (*see Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:			
• N/A			

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.4.8 IT Controls Framework

Rating	High	In-scope area mapping	Foundational

Observations and impact

12A. Work has started to address the scope and granularity of the IT Controls and framework which is not implemented in a way which enables a meaningful and granular view, thus the controls framework does not actually apply robust and effective controls to IT processes across delivery, operations, change management and vendor management. The initial work covers 15 prioritised Horizon-orientated elements as a start-point for a more extensive programme and incorporates COBIT and NIST-based control points.

- The lack of an efficient IT Controls Framework, supported by a clear identification of IT risks and a similarly risk-based POL Internal Audit process 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, subsequent discussions in March and April 2021) and a subsequent review of the extracted controls "Copy of Risk and Control Matrix.xlsx".
- Investigations and rectification efforts have now commenced.

Recommendation

12Ai. Update and extend the IT controls framework to include the required relevant control processes, documentation, and objective control descriptions to implement effective controls across the IT landscape within POL, including vendor supported applications. Design the controls accordingly to ensure the controls are granular, well understood by the staff performing Control Self Assessments (CSA), and are applicable to POL.

12Aii. Once the IT Controls framework is matured, POL IA should update its process to perform independent and periodic Internal Audits.

12Aiii. 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.

12Aiv. Enhance the IT Control reporting schedules, and ensure the reporting contains the required information to accurately determine the effectiveness and completeness of the controls.

12Av. Develop and implement the Controls Process Management document, and ensure adherence.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (see *Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- WS #5: IT Controls
- WS #8: Internal Audit and Risk

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.4.9 Testing

There are **two** risk gradings in this section.

Rating	High	In-scope area mapping	SDLC

Observations and impact

13A. POL does not perform appropriate or comprehensive User Acceptance Testing.

- 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).
- Discussions have commenced to determine how this issue will be resolved. No key decisions have been finalised at this point.
- Investigations regarding the usage of the Model Office environment to support UAT effort are underway; however, the Model Office environment is part of the Production infrastructure, and as such there are limitations to what testing can actually be performed in this environment.

13B. The test environments are not properly managed and utilised, with single environments in use by multiple projects and test phases. Test data within the environments is not refreshed.

- 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).
- Using obsolete test data can result in code conflicts, data issues and other code configuration issues which could invalidate certain test results.
- Additionally, test analysts from different teams could attempt to use the same test data resulting in data conflicts.
- 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).
- This has further been expanded upon via conversations with the Fujitsu test manager (2-Mar-20210, where it was noted that POL only has access to one test Horizon environment. This is also detailed in the "COMMGTREP4166v1.0 - TESTING-QA" report supplied by Fujitsu (1-Feb-2021).

13E. There is no end-to-end regression in place, and the Horizon regression testing is performed in an ad hoc and unplanned manner. There is no coordination of regression testing across POL, Fujitsu and ATOS, and when regression testing is executed, it is restricted only to the area of responsibility of the third party (i.e. Fujitsu will only regression test Horizon at the system test level, ATOS rarely execute regression at all). Fujitsu does have a regression suite of tests; however, these are only executed as part of a project, and they are not executed independently.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

- Without appropriate and regular regression testing in place 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).

Recommendation

13Ai. A UAT phase should be Introduced as standard for all Horizon change. UAT should be conducted within its own non-Production environment, post the completion of functional testing.

13Bi. 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.

13Ei. Establish an appropriate regression approach which covers the end-to-end business processes, as well as integration and functional components. Expand the regression suite to cover all required functionality which requires regular regression. This regression approach should include a regular (monthly) execution cycle for the regression suite.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (*see Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- WS #1: Organisational Change and Comms
- WS #2: IT Target Operating Model
- WS #9: Tooling

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

Document Classification: KPMG Confidential

POL00337564

Rating	Serious	In-scope area mapping	SDLC

Observations and impact

13C. POL does not have an owner for Non-Functional Testing (NFT), and there is no overarching NFT approach.

- 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).

13D. POL do not have a standard set of Non-Functional requirements (NFRs) covering the Horizon platform.

- 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).

Recommendation

13Ci. POL to identify a NFT subject matter expert (SME) to take ownership of all non-functional testing, and govern third party delivery of NFT.

13Di. Develop / identify a standard set of Non-Functional requirements which apply across the Horizon platform.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (see *Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- Fast Fix
- WS #2: IT Target Operating Model

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.4.10 Change management

There are **two** risk gradings in this section.

Rating	Serious	In-scope area mapping	SDLC

Observations and impact

14A. KPMG initial analysis identified that the POL change control process was immature and had gaps; POL has updated and improved the process across Q1 2021.

- Not all change was governed by the change control process; some change was previously redirected to project work, some was not seen until after the change is implemented, some change did occur without passing through this process.
- 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. A formal framework is now being developed, and is Work in Progress.
- Horizon change can come via non-IT projects; this change is sometimes unknown and does not pass through the change control process. This has now been updated, and all change is expected to be controlled by the change control process.
- This has been recognised as a core area which requires rectification, and a new change delivery process is being implemented, with the aim of drastically improving change management.
- 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, 14-Jan-2021, 9-Feb-2021, 20-Apr-2021).

14B. Impact assessments of Horizon changes are irregular and inconsistent.

- 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.
- Discussions are ongoing between POL and the third party suppliers on how this gap can be resolved.
- This was evidenced during discussions with POL representatives (27-Oct-2020, 30-Nov-2020), and there have been additional discussions in Mar 2021.

14D. The Design Authority is being re-implemented and re-established.

- The Design Authority was deprecated when the architectural capability was outsourced to ATOS (2014).
- Actions are being taken to re-constitute the Design Authority, with the appropriate terms of reference in place.
- 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), and ongoing discussions in Q1 2021.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Recommendation
14Ai. Finalise and implement the new change control process, and ensure the appropriate governance and controls are in place to manage change. 14Aii. Uplift the Change Management Framework to ensure any decisions regarding change (e.g. approvals, risks, costings, estimates, etc.) have a formal, objective basis, and are no longer subjective. 14Aiii. Ensure that the change control process and framework is adopted and adhered to by all third parties and change delivery streams, including any potential internal change workstreams. 14Bi. Enforce appropriate impact assessments, performed by POL experts and architects and technical staff. 14Di. Ensure that the re-constituted formal Design Authority, and ensure all change is appropriately routed through this group for review and analysis.
We note the inclusion of the following workstreams in the Horizon Improvements Programme (*see Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:
• WS #2: IT Target Operating Model • WS #11: Remediation Management Office

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Rating	High	In-scope area mapping	SDLC

Observations and impact

14C. 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.

- 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 thought. Additionally, without clear challenge there is no incentive for the third parties to provide more in-depth and accurate information.
- As part of the update and improvement to the change management process, the deliverables from third parties will be reviewed, and uplifted as required. Discussions with the third parties have commenced.
- 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", during discussions with POL representatives (27-Oct-2020), and in ongoing discussions with POL throughout Q1 2021.

14E. There is no central change repository, which holds records of all change (historic and on-going).

- Changes, particularly to reference data and AP-ADC scripts, are not always persisted in a centralised repository which would allow 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.
- As the Change Management process is updated and matured, Service Now will become the repository for change, containing the required change records.
- This was evidenced during discussions with ATOS representatives (7-Dec-2020) and during discussions with POL architects in Mar 2021.

Recommendation

14Ci. Enforce document standards, and challenge any documentation without an appropriate level of detail.

14Ei. Set up a formal change repository, and require all change to be recorded and captured into this repository.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (*see Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- WS #2: IT Target Operating Model

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.4.11 Known Error Logs (Historic)

Rating	None	In-scope area mapping	KEL (historic)

Observations and impact

15A. Historic KELs documentation lacks adequate details (particularly technical details regarding the issue, the cause and how it was resolved). This has since been rectified, with technical details now supplied by Fujitsu.

- Without adequate details supplied, there is uncertainty and lack of a consistent means of confirmation 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).
- With the submission of the Historic BEDs report "COMMGTREP4169 BED Report v1.0" (23-Feb-2021), and the ongoing technical workshops, substantial progress has been made by POL to resolving the Historic KELs, with 45 of the 62 now closed, and the remaining are to be tested. Further progress is being made with respect to the testing of the outstanding KELs, with Fujitsu and POL working together collaboratively to plan the testing.

Recommendation

15Ai. Continue with the current effort to close out these Historic KELs.

We note the inclusion of the following workstreams in the Horizon Improvements Programme *(see Appendix 6: Long-term remediation planning)*. We would expect our recommendations to be addressed across these workstreams:

- Fast Fix
- WS #2: IT Target Operating Model

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.5 Capability

The following pages detail our observations as they pertain to Horizon capability.

4.5.1 POL Horizon capabilities

Rating	Serious	In-scope area mapping	SDLC Foundational

Observations and impact

16A. The Horizon IT function has grown to 20+ experienced technical delivery individuals, with the objective of ensuring that POL has the capability to both govern and deliver change into Horizon, as well as fully understand the platform from a technical sense.

There remains a heavy reliance upon a number of vendors to manage Horizon, as the team still has capability gaps to fill (e.g. BAs, development, release).

- There are still key person dependences in place, where a single SME has knowledge of a specific component or process (e.g. AP-ADC scripts and Reference Data). There is a risk that if this SME is "lost" then the knowledge is likewise lost.
- There are still overarching gaps in the HMR's team's knowledge, especially considering the depreciation of POL technical documentation and knowledge since the ATOS outsource in 2014. Whilst this is being recovered and rectified, the scale and scope of effort is large, and will require an extended period of time to resolve.
- This was confirmed during discussions with POL representatives (16-Oct-2020, 29-Oct-2020 and 11-Nov-2020), with additional discussions throughout Q1 2021.

Recommendation

16Ai. Implement and embed the newly designed and launched target operating model for Horizon, and ensure this is supported by a complementary model in the broader organisation and by the vendors.

16Aii. 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.

16Aiii. The need for improvement in skills and capabilities 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.

16Aiv. 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.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

We note the inclusion of the following workstreams in the Horizon Improvements Programme (see *Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- Fast Fix
- WS #1: Organisational Change and Comms
- WS #2: IT Target Operating Model
- WS #3: Horizon Systems Improvements

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.6 Culture and product

The following pages detail our observations as they pertain to Horizon culture and conduct.

4.6.1 Culture and understanding around roles and responsibilities

Rating	Serious	In-scope area mapping	Foundational

Observations and impact

17A. In our initial investigation we observed that there was an apparent lack of defined, understood or acknowledged job roles, impacting upon incumbents' understanding of responsibilities and accountabilities in relation to Horizon.

The new Horizon Operating Model has defined roles and responsibilities and individuals have been appointed to these roles.
The culture that is being embedded within the Horizon team needs to be supported by a broader shift in culture POL-wide.

- The previous lack of a Horizon-orientated Operating Model and lack of understanding referred to above impacted the timeliness and effectiveness of POL's reaction to the Horizon Issues. POL stakeholders have observed that POL has had an insufficiently collaborative and questioning culture. This has been especially noticeable regarding implementing change to react to the Horizon Issues. 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, and subsequent discussions in January to April 2021).

17B. A new Target Operating Model (TOM) has been introduced which includes roles and responsibilities. Historically there has been a lack of knowledge to challenge vendors within supplier relationship, thus vendors have not been held to account and performance reporting has been misaligned. Incumbents will need to manage vendors at a relationship, performance and contract basis within their new roles and be confident in the support of their stakeholders.

- Vendors will continue to act or revert to a status quo unless the TOM is fully adopted and sustained. SLAs and lines of communication within a model that protects POL's interests and hold vendors to account must be agreed and enforced. This is confirmed by discussions with POL representatives during October and November 23-Oct-2020, 29-Oct-2020, 30-Oct-2020, 3-Nov-2020, 10-Nov-2020 and subsequent discussions including 09-Mar-2021).

Recommendation

17Ai. All component workstreams that support the target Operating model and are illustrated at *Appendix 5: Short-term Fast Fix tactical remediation* (Fast Fix) and *Appendix 6: Long-term remediation planning* (Long Term Remediation) need to be aligned with those of the Postmaster Journey and underpinned by POL's Culture and Change programme to deliver and sustain the required outcomes, and building for the Strategic Platform Modernisation.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

17Bi. Cultural and operational changed in the ways of working for incumbents should be supplemented by appropriate training, plus a communications strategy to ensure vendors and POL staff are clear on the new approach.
We note the inclusion of the following workstreams in the Horizon Improvements Programme (see *Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:
• WS #1: Organisational Change and Comms • WS #2: IT Target Operating Model • WS #11: Remediation Management Office

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.7 Data

The following page detail our observations as they pertain to Horizon data.

4.7.1 Personal Identifiable Information (PII) at rest and in transit

Rating	Serious	In-scope area mapping	Foundational

Observations and impact

18A. POL distributes banking and insurance products, which includes payment cards - as such Payment Card Industry Data Security Standard (PCI DSS) compliance is a requirement of the card scheme (e.g. VMC - Visa Master Card). POL is not PCI-DSS compliant and there is an active remediation programme in place to address the none-compliance. Horizon contains Personal Data (in this case payment card information), which is not encrypted at rest or in transit.

- Given continued PCI-DSS non-compliance, or insufficient remedial progress, POL risk action being taken by the card scheme (VMC), which may result in fines or their card scheme being withdrawn for use by POL.
- -Given the lack of encryption the risk of payment card information being viewed or obtained by unauthorised users is higher than it ordinarily would be if encryption was in place. In the event of unauthorised access POL risks being subject to Regulatory action (from the Information Commissioner's Office) under the Data Protection Act (DPA) 2018 (e.g. lack of appropriate technical controls). This could be a fine, leading to reputational damage. This was confirmed during discussions with POL representatives (16-Oct-2020 and 12-Nov-2020)."

Recommendation

18Ai. Continue to completion the PCI compliance in-flight project.

18Aii. Add PCI DSS non-compliance to the Central, Project and Technical Risk registers.

18Aiii. Introduce DPA compliance monitoring for processes which include Personal Data across Horizon, including the AWS environment. Ensure appropriate organisational and technical controls are present for the protection of payment card information.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (see *Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- WS #6: Data
- WS #7: Security
- WS #8: Internal Audit and Risk

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.8 Systems

The following page detail our observations as they pertain to Horizon systems.

4.8.1 Key dependencies

Rating	Serious	In-scope area mapping	Foundational

Observations and impact

19A. Migration to AWS as part of the Belfast Exit is in-flight however POL still have a significant number of decisions to make (i.e. whether to stay with Fujitsu to manage Horizon or not, integration or migration of legacy product services onto AWS).

Since this observation was originally made in Nov 2020, there has been a great deal of movement with Belfast Exit, however there are still some core decisions which will impact Horizon yet to be finalised (for example - how will the test environments function, what will be done with the applications not being migrated to AWS, what happens with the applications now they are in AWS (refactor / rebuild / improve), etc.).

- 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).

Recommendation

19Ai. Review interdependencies and the core contracts surrounding the migration to ensure no potential conflicts or future complications materialise.

19Aii. Ensure that the current POL - Fujitsu contract is fit for purpose to accommodate the in-flight migration and future states.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (*see Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- WS #6: Data
- WS #7: Security
- WS #2: IT Target Operating Model

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.9 Supplier and performance management

The following pages detail our observations as they pertain to Horizon supplier and performance management.

4.9.1 Vendor performance management

There are **two** risk gradings in this section.

Rating	High	In-scope area mapping	Foundational

Observations and impact

20A. Key Performance Indicators (KPIs) are too high-level, without well-defined service performance metrics, which is self-reported by Fujitsu and no subsequent independent assurance activities being undertaken by POL. It should be noted that there is currently no contractual obligation for detailed reporting.

- High-level and non-accountable performance reviews do not provide sufficient evidence of vendors' performance to the required standards, with no improvement expectations from stakeholders. This leads to the Service Management Report (SMR) being accepted as is with no challenge from POL.
- The results of the metrics from the Fujitsu provided SMR do not include sufficient technical analysis regarding any issues or problems which had arisen during the reported month.
- Lack of overall visibility and governance of the Horizon service, which could lead to performance metrics not being met and result in operational issues.

  This was confirmed during discussions with POL representatives (29-Oct-2020 and 9-Nov-2020, and ongoing discussions in February and March 2021) with subsequent review of the provided Service Management Report "SMR Pack - September 2020".

Recommendation

20Ai. Develop service performance management frameworks for the current and future target operating models. Ensure there is inclusion of relevant forum(s) with Fujitsu presence for POL to discuss and present relevant challenges on reported metrics in order to maximise service performance for Horizon.

20Aii. Review and update the defined expected KPIs and thresholds to meet with POL defined Horizon risk appetite. This will require contractual re-negotiations between POL and Fujitsu to implement.

20Aiii. In parallel with 20Aii, working in collaboration with Fujitsu, revise the SMR to include relevant and detailed technical analysis to ensure that POL is made aware of Horizon related issues and problems that are being or have been resolved.

20Aiv. In the short-term, POL should be seen to be consuming and acting upon the requested inputs from Fujitsu and other key vendors to demonstrate the importance/value of the requested improvements.

20Av. Stakeholders should be engaged in discussions regarding investments required to achieve the outputs desired from vendors and such decisions formally agreed.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

We note the inclusion of the following workstreams in the Horizon Improvements Programme *(see Appendix 6: Long-term remediation planning)*. We would expect our recommendations to be addressed across these workstreams:
• WS #2: IT Target Operating Model

Rating	**Serious**	**In-scope area mapping**	Foundational

Observations and impact

20B. Horizon service performance is overseen through different governance routes such as the Information Security Management Forum (ISMF) and Service Management Report (SMR)

- 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".

Recommendation

20Bi. In collaboration with second LoD, service managers, compliance team and ISMF review the existing end to end vendor performance management process for Fujitsu. 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. This will require contractual re-negotiations between POL and Fujitsu to implement.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (see *Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:
• WS #2: IT Target Operating Model • WS #7: Security • WS #8: Internal Audit and Risk

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

Document Classification: KPMG Confidential

POL00337564

4.10 Technology

The following pages detail our observations as they pertain to Horizon technology.

4.10.1 Tool support for change delivery

Rating	Serious	In-scope area mapping	SDLC

Observations and impact

21A. There is no universally required project management tooling in place, and some projects are managed via spreadsheets and email, whereas other projects are using an implementation of Jira just for the delivery of that project.

- There seems to be no overarching tool in place to facilitate the delivery of a) project change or b) test management, which causes inefficient control and coordination of change management. Similarly, there is no coordination of metrics, MI, and reporting, and so the governance of each project will be different, and more complex, than if there was a prescribed tool which had to be used for project 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).

Recommendation

21Ai. Whilst POL has IBM DOORS and Microfocus ALM present, these tools have not been in use several years, and have degraded. Re-licensing may be expensive, and these tools may no longer suit POL's approach. 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.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (see *Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- WS #2: IT Target Operating Model
- WS #9: Tooling

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.10.2 Business Continuity Plan (BCP) / Disaster Recovery (DR)

Rating	High	In-scope area mapping	HNGA

Observations and impact

22A. Whilst there is a Business Continuity Policy in place, the next level plans do not exist.

- The BCP document is high level, and outlines the purpose and scope of the required business continuity approach, and this is as expected, and is acceptable. However, the next level of detail, which should be contained in the business continuity plans for each business unit, seem to be unavailable or not yet created. The impact of the missing plans is that the business units do not have a structured and detailed approach to BCP, and do not have the expected components in place to determine how business continuity will be handled. This was evidenced by conversations with the BCP manager and the DR manager (3-Mar-2021, 15-Apr-2021, 16-Apr-2021).

22B. There is no consideration for resilience at the architectural level.

- Designing for business and technical resilience is not included in the architectural effort of change. This has an impact of making resilience an afterthought, and the solution (when implemented) may not have the required components in place to support the expected resilience requirements. This was evidenced by conversations with the BCP manager and the DR manager (3-Mar-2021, 15-Apr-2021, 16-Apr-2021).

22C. POL has no Business Impact Assessments (BIA) in place. BIAs are a standard component of a BCP, and inform the overall BCP approach and structure.

- Without BIAs in place, the business cannot determine what the business and financial impacts are when a system goes offline for a period of time. BIAs also help determine the prioritisation for each system, enabling appropriate recovery planning to be put in place. This was evidenced by conversations with the BCP manager and the DR manager (3-Mar-2021, 15-Apr-2021, 16-Apr-2021).

22D. There is no clear linkage between the BCP approach and the DR approach

- It would be expected for the BCP and DR approaches to be linked, and be working together to ensure both the business and technology aspects of business continuity are maintained, however this is not the case, and the two areas are currently operating independently. This is known to the BCP and DR leads, and they have identified this as a risk, and are working to resolve this problem. This was evidenced by conversations with the BCP manager and the DR manager (3-Mar-2021, 15-Apr-2021, 16-Apr-2021).

22E. The DR approach is to repeat the same tests year on year, with no updates for results and changes to the systems.

- The DR events are appropriately run year on year. However, each event simply repeats the tests of the previous year, without detailed analysis across any changes which have occurred within the year, or analysis to changes to the surrounding systems. Furthermore, the feedback mechanisms within the DR testing are not fully utilised, and the outcomes of the tests are not fed back into the next year's planned testing. This was evidenced by conversations with the BCP manager and the DR manager (3-Mar-2021, 15-Apr-2021, 16-Apr-2021).

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Recommendation
22Ai. Develop and finalise the individual business continuity plans for each business unit. These plans then need to be implemented. 22Bi. POL should develop a standardised and universally accepted approach to resilience, which is well documented and applies across third party delivery. This will ensure that third parties, when delivering solutions into POL, have to adhere to common and understood resilience requirements. 22Bii. Include the resilience requirements in the architecture and design of a solution (generally these are part of the non-functional requirements). This should include a review by the BCP and DR managers. 22Ci. The BIAs need to be created, validated, and signed off as soon as possible. Once complete, and accepted, the BIAs can then drive the BCP and DR strategy across POL and the third parties. 22Di. The BCP and DR approaches need to work in conjunction, and in support of each other. This is a goal of both the BCP and DR managers, and they are actively working towards establishing a proper working structure. 22Ei. The DR testing has to consider system and structural change, adapting to reflect what those changes were, and how they could potentially change the resilience of the landscape. 22Eii. The tests being executed for DR year on year should be updated to reflect points of failure, changes to the risk profile, changes to scope and changes to responsibilities (e.g. ownership of systems, etc.)
We note the inclusion of the following workstreams in the Horizon Improvements Programme (see *Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:
• WS #3: Horizon System Improvements • WS #7: Security

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Rating	Serious	In-scope area mapping	HNGA
Observations and impact			
22F. Both the BCP manager and DR manager are coordinating teams of one (themselves). Based on the volume of work, and the complexity of the landscape, larger teams would be expected. • For a corporation the size of POL, with the number of third parties, and based on the complexity of the technical landscape, KPMG would expect to see each area to have a team of 5-8 people. This was evidenced by conversations with the BCP manager and the DR manager (3-Mar-2021, 15-Apr-2021, 16-Apr-2021).			
Recommendation			
22Fi. Both the BCP and DR teams should be expanded with the required SMEs and experts to facilitate the delivery of the full scope of work required in both these areas.			
We note the inclusion of the following workstreams in the Horizon Improvements Programme (*see Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:			
• WS #7 Security			

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.10.3 Tools for IAM and GRC

Rating	Serious	In-scope area mapping	Foundational

Observations and impact

23A. There is insufficient usage of technology and tools for IAM and risk management.

- POL has access to ForgeRock, Microsoft Identity Manager, ServiceNow, TRACtion and Archer (being migrated to ServiceNow), tool sets although their capabilities are not fully leveraged nor used in an integrated way, which if they were could:
  - alleviate, streamline, and automate manual processes,
  - provide a single view of users/identities,
  - improve governance and reporting, and
  - reduce risk exposure.
- There is no privileged access management software implemented at present. This was confirmed during discussions with stakeholders ((3-Nov-2020, 9-Nov-2020, 10-Nov-2020 and further discussions in February, March, and April 2021)

Recommendation

23Ai. Assess existing tools and processes and create a strategic roadmap to leverage or consolidate current tooling.

23Aii. Consider additional Commercial Off the Shelf (COTS) tools to introduce new capabilities, in particular privileged access, and supplement or replace existing tools not fit-for-future/end of life tools to achieve additional efficiency and controls.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (*see Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- WS #7 Security
- WS #9 Tooling

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.10.4 AP-ADC Scripts allow uncontrolled change

Rating	High	In-scope area mapping	SDLC

Observations and impact

24A. Automated Payments – Advance Data Scripts (AP-ADC) are used to make changes in Production & Reference Data.

- An initial review of the function and use of the AP-ADC scripts has illustrated the extent to which they represent a significant part of the HZ environment. Moreover, their existence is shown to compromise DR, as the DR approach does not consider AP-ADC changes which have been implemented, and the DR environments do not always include the latest AP-ADC changes. Additionally, changes implemented via AP-ADC are generally not tested from a holistic or an end-to-end perspective. When the scripts have an impact wider than expected this may be missed until the script is in Production, and then problems may occur. Note that the AP-ADC scripting capability was originally the responsibility of POL; this function was then outsourced to ATOS in 2014. Recently (April 2021), this functionality was insourced back into POL from ATOS.
- This was confirmed during discussions with POL representatives (14-Dec-2020) with subsequent review of the provided 'AP-ADC script reference manual' (20Nov2020).
- A separate report focusing on AP-ADC scripts has been produced which provides a series of recommendations.

Recommendation

24Ai. The "AP-ADC script and Reference Data assessment v1.4" report discusses the AP-ADC scripts in detail, and offers several recommendations to rectify the issues identified.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (*see Appendix 6: Long-term remediation planning*). *We would expect our recommendations to be* addressed across these workstreams:

- WS #3: Horizon System Improvements

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

Document Classification: KPMG Confidential

POL00337564

4.10.5 Usability and User Interface Design

Rating	Serious	In-scope area mapping	SDLC

Observations and impact

25A. Usability is not considered during solution design, and there does not appear to be a clear focus on the interface design and structure.

- Modern payment and retail systems have a focus on smooth and intuitive screen design that supports the user journeys and process flows, whereas this does not seem to be the case with Horizon. The screen interface has an "old school terminal" feel which is complex and confusing, and still has elements which are no longer part of the POL product offering. In a worst case scenario, poor screen design can lead to user confusion and error, which then require backend rectification and assistance to be provided to the user.
- This was confirmed during discussions with POL representatives (4-Feb-2021), and with a subsequent review of the provided user interface design tools.

Recommendation

25Ai. Implement appropriate user design, following standard usability protocols. Tidy up the screens and improve the user interaction with the platform.

We note the inclusion of the following workstreams in the Horizon Improvements Programme (see *Appendix 6: Long-term remediation planning*). We would expect our recommendations to be addressed across these workstreams:

- WS #3: Horizon System Improvements

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

4.11 Further observations

Observations have also been made during our review of the Horizon architecture. It is our understanding that these observations are being addressed by current POL activities. However, as they have the potential to cause problems which align with the concerns of the Horizon Judgement, we have included them for awareness, and they may have an impact on the Horizon Remediation Programme or potentially the wider POL organisation. This list is not exhaustive.

4.11.1 "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 workarounds and has potential to be a vector for fraudulent transactions. There are several strands of remediation which will aim to address this.

4.11.2 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 but 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. This observation has been taken forward by GLO into the Postmaster engagement workstream.

4.11.3 Enfranchisement

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 but 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. This observation has been taken forward by GLO into the Postmaster engagement workstream.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

05

Appendices

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

Document Classification: KPMG Confidential

POL00337564

5 Appendices

5.1 Appendix 1: Documentation

5.1.1 Document list - PAM/RAM

During this review we inspected 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 Horizon analysis V0.3a Horizon description (1) ARC030 Horizon Solution Architecture Outline ARCSECARC0003V6po UEM-012b - POL IT Landscape v1.5 (002) 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
Weekly leaver checks and access remediation of leavers	Evidence for the Global user access accounts	POL

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Title	Description	Source
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	Update on IT General Controls review	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	Table of Risks identified and Controls in place to mitigate them	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
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 Fujitsu	POL
Fujitsu-Post Office ISAE3402 FINAL report - 1 April 2018 to 31 December 2018	SOCR performed by EY, provided to POL by Fujitsu	POL
Fujitsu-Post Office ISAE3402 FINAL report - 1 April 2019 to 31 December 2019	SOCR performed by EY, provided to POL by Fujitsu	POL
JML - Final Report	Joiners, Movers and Leavers thematic Internal Audit conducted by POL IA in 2020	POL
Internal 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	Fujitsu
COMMGTREP4165 – RA Report	Fujitsu Report – Remote Access and Privileged Access	Fujitsu
COMMGTREP4228 RA Report Follow up responses	Fujitsu report – Remote Access Report - Follow up responses	Fujitsu

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

5.1.2 Document list – KELS, SDLC, HNGA

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 ToR 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
SMR Pack September 2020	Fujitsu monthly Service Management Report pack	Fujitsu
Monthly service review meeting minutes and actions 09.09.2020	Minutes and actions from monthly service review meeting	Fujitsu
20200220_POL_BCMS Board Paper	Business Continuity Gap Analysis – Audit, Risk and Compliance Cttee Report	POL

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Title	Description	Source
05.02_RCC_9.5 (ii) Business Continuity Management Policy v2.6	Business Continuity Management Policy 21 June 2020	POL
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
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	Computacenter Change Request Sample	POL
CHG0037838	Verizon Change Request Sample	POL

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Title	Description	Source
CHG0037846	Verizon Change Request Sample	POL
CHG0037898	Verizon Change Request Sample	POL
CHG0036991	Computacenter Change Request Sample	POL
CHG0036992	Computacenter 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
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

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Title	Description	Source
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
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/Fujitsu
Knowledge Base - cardc2117L.151119.pdf	Knowledge Base Article	POL/Fujitsu
Knowledge Base - dsed1614M 060420.pdf	Knowledge Base Article	POL/Fujitsu
Knowledge Base - GelderR488Q 131120.pdf	Knowledge Base Article	POL/Fujitsu

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

KPMG

Post Office Limited

KPMG LLP

Title	Description	Source
Knowledge Base - jsim1429l 151119.pdf	Knowledge Base Article	POL/Fujitsu
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/Fujitsu
Current Architecture and Forums.ppt	Current Architecture and Forums details	POL
Computacenter Service Report March 21	Post Office Service Review Pack	Computacenter
RADC2012001++1-SUB-RFLCommon V0.12.xls	Screen construction / design for the SUB-RFL change	POL
RADC-2012-012 Add Prize Draw MenuHierarchyFront v423.xlsm	Screen construction / design for the Add Prize Draw change	POL
COMMGTREP4169 BED Report v1.0	Fujitsu Report – Bugs Errors and Defects Historic	Fujitsu
COMMGTREP4167 HNGA Robustness v1.0	Fujitsu Report – Service Delivery Metrics	Fujitsu
COMMGTREP4184 BED Report v1.0	Fujitsu Report - BED Current Process	Fujitsu
COMMGTREP4227 Testing QA Report	Fujitsu Report – Follow-up Responses	Fujitsu
Fujitsu – SYSMAN4_Event Overview	Process document – Event Collection Process	Fujitsu
COMMGTREP4166 v1.0 Testing-QA	Fujitsu Report – Testing and QA process	Fujitsu
COMMGTREP4168v,1.0 SDLC	Fujitsu Report – SDLC processes	Fujitsu
COMMGTREP4226 SDLC Report	Fujitsu Report – SDLC Report – Follow up responses	Fujitsu

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

5.2 Appendix 2: Contributors

During this review we spoke to several individuals. They are listed below.

Name	Title	Area of Focus
Adrian Eales	CTO, Retail	Horizon walkthrough
Andrew Kenny	Service Centre Manager	Demonstration of the Tier 2 team usage of HORice when conducting investigations
Adam Malach Tony Hogg	Head of Cyber Security Advisory Head of Cyber Operations IT Security	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 Martin Godbold Paul Smith Dean Bessell Paul Kingham Charlotte Muriel	Historical Maters Horizon IT Director Horizon Service Lead Incident and Problem Manager Security Architect Access Control Specialist Historical Matters	Regular interaction on direction of travel, validation of hypotheses and emerging findings.
Dionne Harvey	Head of IT Contract Management	To understand the vendor relationship management aspect between POL and Fujitsu.
Sree Balachandran	Head of Postmaster Experience, Product and Vendor Management	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	Data Services Lead	Overview of the process for management of global user accounts, Privileged Access Management, Remote Access Management
Dave King	Head of Security Architecture, CISO	Walk through privileged Access Management/PAM/RAM process(es) for Horizon at Fujitsu

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

KPMG

Name	Title	Area of Focus
		Walk through break-glass procedure including approvals, monitoring, audit log reviews etc.
Shaun Turner	Learning Technologies Manager	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
Aatish Shah	IT Governance and Reporting Manager	IT Change Framework: POL IT controls and the framework in place around these controls
James Brett	Senior Test Manager (ATOS)	Discuss the testing which ATOS is responsible for delivering
Luke Harrison	Digital Workplace Lead	Further develop understanding of the IT landscape (e.g. IT equipment, email, server, networking, etc) of the Post Office Limited and Branches
Sally Rush	GLO Solutions Specialist	Understand the current documentation and processes for data management in Horizon
Rob Wilkins	IT Cloud Services Director	Understand the Horizon move to Amazon Web Services
Gary Walker	Service Management & Enterprise IT Director	Understand the Release management process, Change delivery, Operations overview
Ian Sage	PM for AWS migration	Discussion of how the Belfast Migration programme is governing change
Ben Owens	Head of Cloud Services	Introduction to the testing being performed across change occurring on Horizon, and how the testing is governed and controlled including the test approach for the Belfast migration.
Jonathan Acres Diogo Vidinhas	IT Audit Manager Senior Audit Manager	To understand the POL environment from IA's perspective and evaluate Internal Audit's involvement with risk management around Horizon and Fujitsu
Rebecca Barker	Deputy Head of Risk, Risk Business Partner	Understand the role/records/actions under POL's Risk Management function

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Name	Title	Area of Focus
	Group CIO, Group COO	
Stephen Browell	Fujitsu	Discussion of ways of working with Fujitsu including access to documentation and resources
Katrina Holmes	Head of Branch Operations Engagement	Horizon change mgmt., testing and incident management
Stuart Banfield	IT Service Transition Lead - Retail	Horizon change processes
Harry Vazanias	Contractor	Discussion of change management, gaps, and problems in IT org structure and SDLC management
Joseph Moussalli	SPO	Discussion on how the PCI programme is being governed
Tony Jowett	CISO	Governance around Horizon and the IT controls framework
Steve Page	Lead Solution Architect	Library of architecture documentation on Horizon and an overview of the Horizon data flow
Saira Burwood George Cross	Head of SPO Portfolio Governance Manager	Walkthrough of the portfolio process; Discussion on detailed programme and project management; Governance of third-party delivery
Cherise Osei	Change and Service Catalogue Manager	Walkthrough and discussion of the POL change management process
Gareth Clark	Head of Transformation Portfolio	Portfolio management within IT
Matthew Warren	Head of Reference Data Services	Discussion of how ATOS are involved with POL change
Harshwardhan Soman	Test and Release Manager	Collaborative development of testing capability
Johnny Lansdale	Business Continuity Manager	Understanding of BCP process

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

KPMG

Post Office Limited

KPMG LLP

Name	Title	Area of Focus
Jon Davies	Asset and Configuration Management Lead	Understanding of ITIL service management processes
Kathryn Wearne	Head of Service Operations	Incident and Problem Management, Change Management, Operations, Service Desk
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	Case Review Analyst	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

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

KPMG

Post Office Limited

KPMG LLP

Name	Title	Area of Focus
Matt Quincey	Service Manager for Accenture and Verizon	IT Systems
Drew Mason	Network Monitoring and Support Analyst	Branch analysis and loss prevention, FREDD-O
Ketul Patel	Network Delivery Director	Key logging and network analysis
Ruk Shah	Group MI and Analytics Director	Data Platform
Maria Opaniran	Project Manager, SPO	Data Platform
Dean Whitehead	Service Centre Support Manager	Dynamics and Puzzel
Laura Tarling	Case Review Analyst	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
Clare Hammond	Senior Data Protection Manager	Compliance controls
Jonathon Hill	Compliance Director	Compliance controls

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

5.3 Appendix 4: Glossary

Throughout the report we refer to several terms and use acronyms. They are defined below:

Term	Definition
AP/ADC	Automated Payments/Advance Data Capture
APPSUP	Application Support – a user role which provides full data read/write privileges on Oracle systems.
ATOS	3rd. Party Supplier of IT Services
AWS	Amazon Web Services
BCP	Business continuity plan
BEDS	Bugs Errors Defects - Fujitsu terminology – synonymous with Known Error List (KELS)
BIA	Business impact assessment
BRDB	Branch Database
CAB	Change Advisory Board
CFS	POL's Finance System
CIJ	Common Issues Judgement
CMMi	Capability Maturity Model Integration - a process level improvement training and appraisal programme, administered by the CMMI Institute
COBIT (IT)	Control Objectives for Information and Related Technology
CSA	Controls Self-Assessment
DR	Disaster Recovery
EPOS	Electronic point of sale
FCA/PRA	Financial Conduct Authority / Prudential Regulation Authority
GDPR	General Data Protection Regulation
GLO	Group Litigation Order
HIJ	Horizon Issues Judgement
HIJF	Horizon Inquiry Judgement Findings

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Term	Definition
HITJ	Horizon IT Judgement
HNG-A	Horizon Next Generation – Anywhere. This is the replacement for the HNG-X counter using Windows 8.1
HORice	Interrogation and Reporting tool – designed to interface with Horizon
IAM	Identity and access management
ISMF	Information Security Management Forum
JML	Joiners Movers Leavers
KELs	Known Error Lists
LoD	Lines of Defence – a risk management model designed to assure the effective and transparent management of risk by making accountabilities clear
KPI	Key performance indicator
MFA	Multi-factor Authentication
PAM	Privileged Access Management
PM	Postmasters
POL	Post Office Limited
RA	Remote access
RACI	Responsible, Accountable, Consulted, Informed matrix
RAID	Risks, assumptions, issues, dependencies
SDLC	Software Development Lifecycle (Development, Change Management, Testing etc)
SLA	Service Level Agreement
SME	Subject Matter Expert
SOCR	Service Organisation Controls Report
SoD	Segregation of Duties
SMR	Service management report
SPM	Strategic Platforms Modernisation (Project to consider options for replacement of Horizon system)

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Term	Definition
ST	System Testing
SIT	System Integration Testing
SV&I	Solution Validation and Integration
TOM	Target Operating Model
ToR	Terms of Reference
TUPE	Transfer of Undertakings (Protection of Employment)
UAT	User Acceptance Testing
UX	User Experience
XML	Extensible Mark-up Language

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

5.4 Appendix 5: Short-term Fast Fix tactical remediation

This screen shot has been extracted from the Horizon Improvements Programme V1.0. It depicts the range of work currently ongoing to address HIJs, with a planned delivery date of '1.0 – Initial fix' in before the end of May 2021.

Note, Fast Fix activity stated in March 2021, but planning is shown from April here taken from latest reporting.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

KPMG

Post Office Limited

KPMG LLP

DRAFT FOR DISCUSSION

Fast Fix - POAP

0.1 – Requirements / issue definition
1.0 – Initial fix in short term to address critical issues, mainly process based but likely to have some tech enablement
2.0 – Medium term interim build to reinforce 1.0 remediation with improved solution
3.0 – Longer term integrated operating model solution

Rapid fix implemented — Rapid fix
Interim report / plan / review — Longer term

Workstream	Fast fix	Sub-workstream	Key deliverables/ milestones
			Apr-21: 05/04 · 12/04 · 19/04 · 26/04 — May-21: 03/05 · 10/05 · 17/05 · 24/05
Organisational Change			0.1. Stakeholder mapping and analysis, with targeted interventions for short term workstreams drafted
IT TOM		Hz governance / IT change	1.0 - New process & job description to support governance and core change control needs drafted 1.0 - Critical KPI / Metrics dashboard v.10
Horizon System Improvement		Enterprise architecture	1.0. High level design draft for deployment of AppDynamics on Horizon issued Design of platform to integrate longer term solution. No quick fix 0.1 - Data platform functional and non-functional requirements 0.1 - Draft of strategy for instrumentation and monitoring of Horizon platform produced Design of platform to integrated longer term solution. No quick fix
	7	Horizon HNGA software issues	0.1 - Agree scope for HNGA software issue improvements 0.1. Reference data recommendations to improve process, source code management and testing to mitigate most frequent issues complete (0.1) Design for interim reference data and APADC solution (target to deliver June 2021)
	13	Horizon help improvements	0.1 - Horizon help improvements requirements and HLD designed for technical solution 1.0 - Horizon help priority improvements
	5	Current KELS	1.0 & 2.0 - updated process (complete) 3.0 – ServiceNow implementation
	6	Historic KELS	1.0 - Resolution of/ confirm testing all historic KELs 1.0 – Model office testing (TBC) 1.0 – Rig testing (TBC – target end Jun 2021) 2.0 - Creation of regression suite pack for periodic reconfirmation. 3.0 – Validation/ Testing of regression pack (Target end July 2021)
	9	Test HNGA under load	1.0 - NFT approach and framework to implement the appropriate tooling. New process for NFT, new tooling for testing and monitoring within Hz to do it with. 2.0 – Create NFT scripts and NFT environment. 3.0 – Execute NFT and resolve issues. 0.1 - DR & BC policy in progress
	10	SDLC / QA	1.0 – New processes developed and documented to manage SDLC delivery with change, requirements management, build, design, test, release and operations management processes. PMs as central voice drafted and process updates implemented 2.0 Implementation of new processes as per 1.0
	8	Inform errors to PMs	1.0 – Communications to Postmasters on defects sent using current technology (in place) 2.0 - Establish feedback loop for SPMs to measure effectiveness of process & improvements
Investigations	1	Horizon dispute mechanism	1.0 Tactical solution with updated process and name in Horizon (to replace 'Settle centrally', driven by ref data) for dispute mechanism 2.0 Solution extended to include 2 extra 'buttons' within Horizon terminal
	2	Keystroke logging	1.0. Tactical solution to capture, store and preserve postmaster interaction data to go live 2.0 Requirements-driven capture of user interaction activity at the counter
	3	Direct access to transactional data	1.0 – Process change tactical solution for sourcing ARQ data from Fujitsu by POL staff, including roll out of user training and communications to go live 2.0 Requirements and design of investigations Data Platform
	4	Sharing of transactional data	0.1 – Agreed options and recommendation for tactical data sharing solution, including SPM and POL communication developed and disseminated 1.0 Investigation reports shared with Postmasters 2.0 Requirements for sharing of data with Postmasters
	14	Investigation of Postmaster transactional concerns	1.0 – New investigations TOM, with changes to process, org structure, technology enablement through MS Dynamics 2.0 - Development of Wider technology enablement of investigations process increases transparency of process for Postmasters, refinement of KPIs and WoW under the new organisational structure (target Sep 2021)
IT Controls		Controls tactical fix	0.1 – Wave 1 lessons learnt report 1.0 - Training and implementation for selected IT controls re. third party risk management. 3.0. 6 monthly evolution of IT assurance to include programme support and establish an effective second line IT risk function
		Enhanced IT controls roadmap	0.1 – Draft enhanced IT controls roadmap produced and lessons learnt report
Data		Data governance	1.0 - Horizon Information Asset Register (IAR) v1 drafted 2.0 Operationalising use or IAR within data governance processes 1.0 - Data governance policy framework v1 drafted
Security	12	PAM/ RAM	1.0 – Remediation and improvements, including FJ Transaction Correction, BRT, SmartID and GLO as a priority. IDAM manual remediations 1.1 Continuation of manual-process improvements
Internal Audit and Risk	15	Independent audits	POL IA team to complete their review of POL HIJ actions by July
Tooling		ServiceNow	0.1 - Tactical Proof of Value (POV) ServiceNow Dispute resolution & Change Management 1.0 - Tactical MVP ServiceNow Dispute resolution 0.1 - POL ServiceNow Healthscan 1.0 - Tactical MVP ServiceNow Change Management

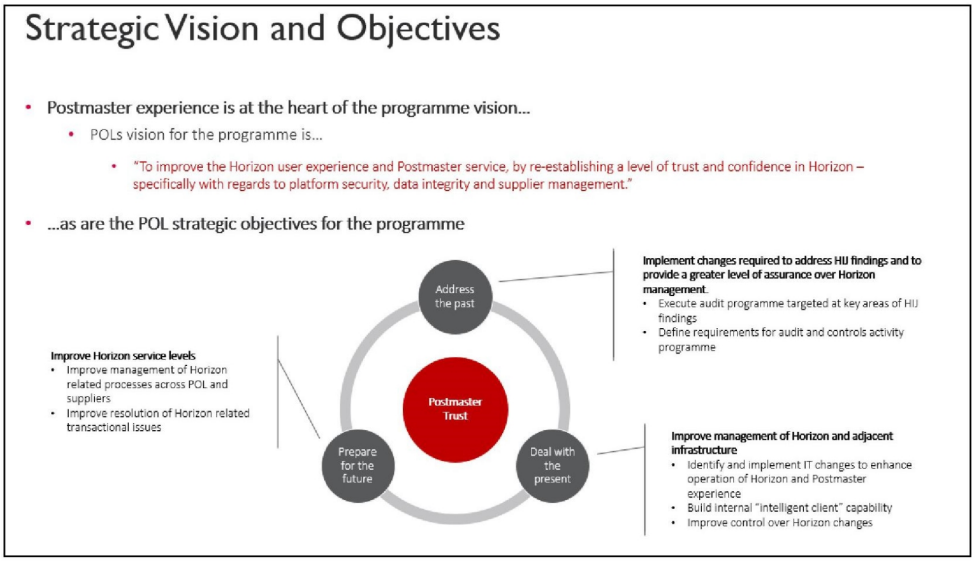
© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

5.5 Appendix 6: Long-term remediation planning

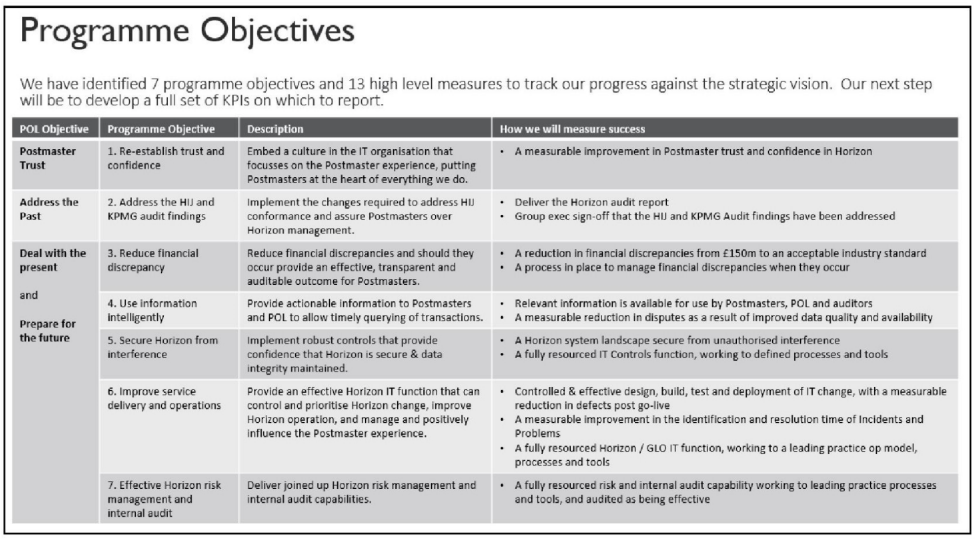
5.5.1 Strategic vision and objectives

This screen shot has been extracted from the Horizon Improvements Programme V1.0. It depicts the programme strategic vison and overall objectives.



5.5.2 Programme objectives

This screen shot has been extracted from the Horizon Improvements Programme V1.0. It depicts the specific programme objectives.



Programme Objectives

We have identified 7 programme objectives and 13 high level measures to track our progress against the strategic vision. Our next step will be to develop a full set of KPIs on which to report.

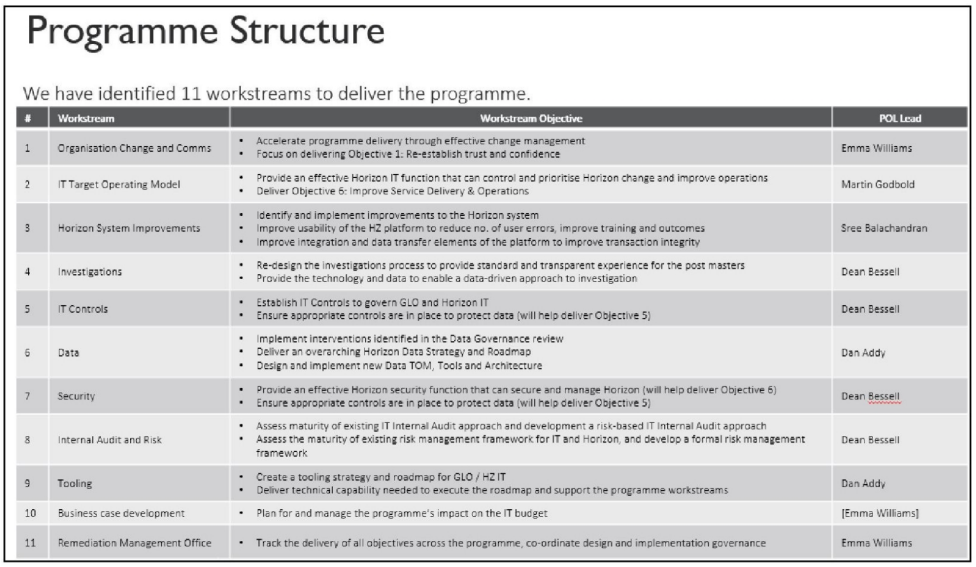
POL Objective	Programme Objective	Description	How we will measure success
Postmaster Trust	1. Re-establish trust and confidence	Embed a culture in the IT organisation that focusses on the Postmaster experience, putting Postmasters at the heart of everything we do.	• A measurable improvement in Postmaster trust and confidence in Horizon
Address the Past	2. Address the HIJ and KPMG audit findings	Implement the changes required to address HIJ conformance and assure Postmasters over Horizon management.	• Deliver the Horizon audit report • Group exec sign-off that the HIJ and KPMG Audit findings have been addressed
Deal with the present and **Prepare for the future**	3. Reduce financial discrepancy	Reduce financial discrepancies and should they occur provide an effective, transparent and auditable outcome for Postmasters.	• A reduction in financial discrepancies from £150m to an acceptable industry standard • A process in place to manage financial discrepancies when they occur
	4. Use information intelligently	Provide actionable information to Postmasters and POL to allow timely querying of transactions.	• Relevant information is available for use by Postmasters, POL and auditors • A measurable reduction in disputes as a result of improved data quality and availability
	5. Secure Horizon from interference	Implement robust controls that provide confidence that Horizon is secure & data integrity maintained.	• A Horizon system landscape secure from unauthorised interference • A fully resourced IT Controls function, working to defined processes and tools
	6. Improve service delivery and operations	Provide an effective Horizon IT function that can control and prioritise Horizon change, improve Horizon operation, and manage and positively influence the Postmaster experience.	• Controlled & effective design, build, test and deployment of IT change, with a measurable reduction in defects post go-live • A measurable improvement in the identification and resolution time of Incidents and Problems • A fully resourced Horizon / GLO IT function, working to a leading practice op model, processes and tools
	7. Effective Horizon risk management and internal audit	Deliver joined up Horizon risk management and internal audit capabilities.	• A fully resourced risk and internal audit capability working to leading practice processes and tools, and audited as being effective

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

5.5.3 Programme structure

This screen shot has been extracted from the Horizon Improvements Programme V1.0. It depicts the programme structure currently being set up across 11 workstreams.



Programme Structure

We have identified 11 workstreams to deliver the programme.

#	Workstream	Workstream Objective	POL Lead
1	Organisation Change and Comms	• Accelerate programme delivery through effective change management • Focus on delivering Objective 1: Re-establish trust and confidence	Emma Williams
2	IT Target Operating Model	• Provide an effective Horizon IT function that can control and prioritise Horizon change and improve operations • Deliver Objective 6: Improve Service Delivery & Operations	Martin Godbold
3	Horizon System Improvements	• Identify and implement improvements to the Horizon system • Improve usability of the HZ platform to reduce no. of user errors, improve training and outcomes • Improve integration and data transfer elements of the platform to improve transaction integrity	Sree Balachandran
4	Investigations	• Re-design the investigations process to provide standard and transparent experience for the post masters • Provide the technology and data to enable a data-driven approach to investigation	Dean Bessell
5	IT Controls	• Establish IT Controls to govern GLO and Horizon IT • Ensure appropriate controls are in place to protect data (will help deliver Objective 5)	Dean Bessell
6	Data	• Implement interventions identified in the Data Governance review • Deliver an overarching Horizon Data Strategy and Roadmap • Design and implement new Data TOM, Tools and Architecture	Dan Addy
7	Security	• Provide an effective Horizon security function that can secure and manage Horizon (will help deliver Objective 6) • Ensure appropriate controls are in place to protect data (will help deliver Objective 5)	Dean Bessell
8	Internal Audit and Risk	• Assess maturity of existing IT Internal Audit approach and development a risk-based IT Internal Audit approach • Assess the maturity of existing risk management framework for IT and Horizon, and develop a formal risk management framework	Dean Bessell
9	Tooling	• Create a tooling strategy and roadmap for GLO / HZ IT • Deliver technical capability needed to execute the roadmap and support the programme workstreams	Dan Addy
10	Business case development	• Plan for and manage the programme's impact on the IT budget	[Emma Williams]
11	Remediation Management Office	• Track the delivery of all objectives across the programme, co-ordinate design and implementation governance	Emma Williams

5.5.4 Plan on a page across all workstreams

This screen shot has been extracted from the Horizon Improvements Programme V1.0. It depicts the plan on a page of 24 months of activities across the proposed 11 workstreams.

Note: Additional artefacts also exist, such as a RAID log, Resource Plans and Governance structure.

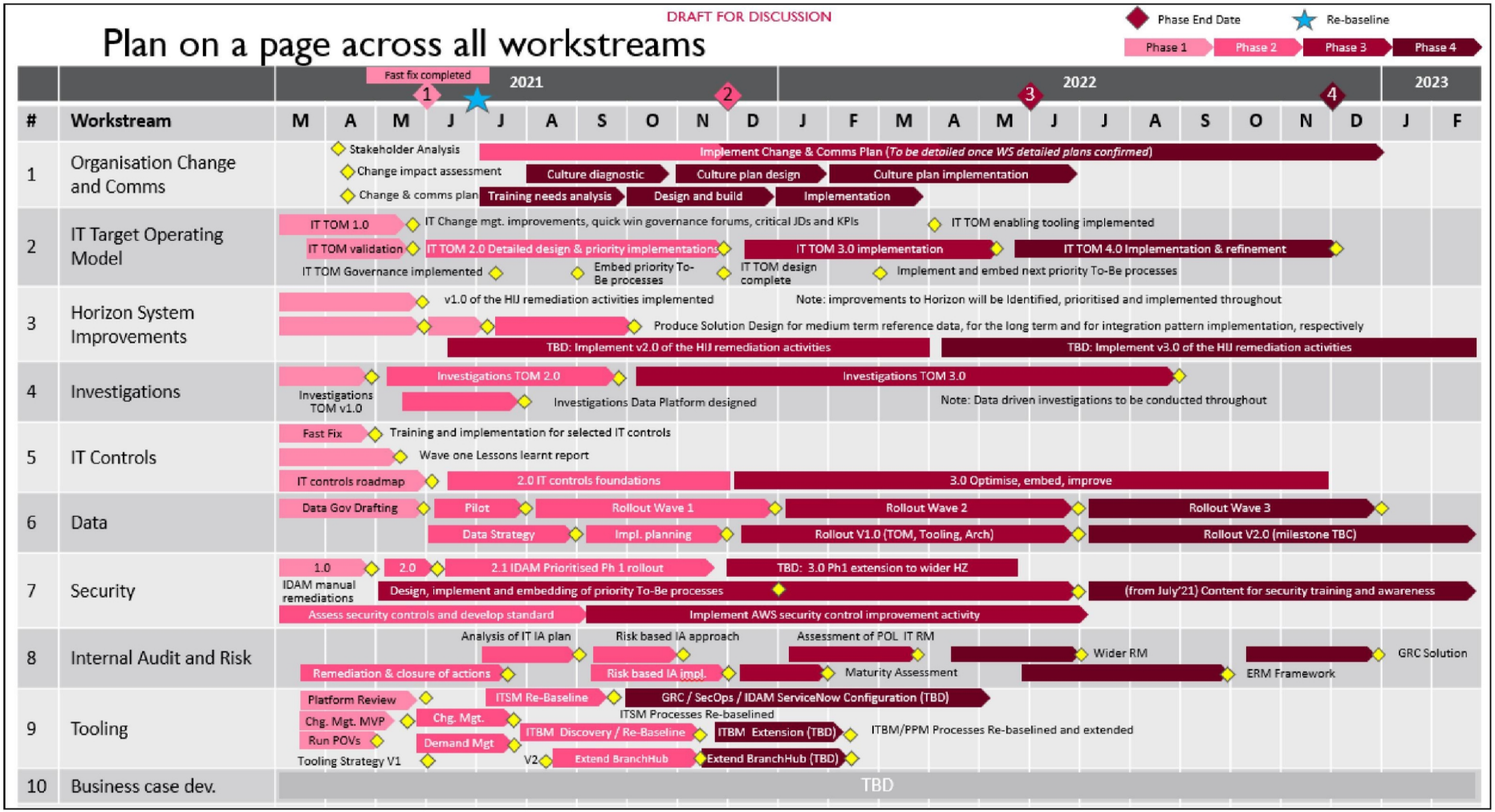
© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

KPMG

Post Office Limited

KPMG LLP



© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

Document Classification: KPMG Confidential

POL00337564

5.6 Appendix 7: Engagement Terms of Reference

The following screenshots are taken from our contract with POL. This sits under the following contract reference: 2019/S 079 190249.

Engagement requirements

This engagement has two requirements:

A. In support of the Post Office's response to the inquiry, the Post Office wish to offer an interim report into progress they have made to address previously identified failings.

Specifically, the Post Office require assistance across six areas:

i. Privileged Access Management
ii. Software Development Lifecycle, Testing and Quality Assurance
iii. Known Error Logs – historic
iv. Known Error Logs – current
v. Remote Access
vi. Horizon Next Generation (HNGA) Robustness

The six areas and expected evidence are included in the table below.

Area	Requirement	Expected Evidence
Privileged Access Management	To clearly know who has what privileged access at any given time.	• PAM capability overview covering People, process and technology • Evidence of the PAM related processes within FJ working – to include processing of Movers • Routine Reporting on PAM • Evidence sampling of PAM system in Fujitsu • Evidence of corrections to PAM when things are seen to have gone wrong
SDLC, Testing, QA	To understand how changes progress from requirements analysis through development, testing and into early live support. Clearly demonstrate how such changes become fully live under mainstream support arrangements.	• SDLC, Testing and QA capability overview covering people, process and technology. • Evidence of the process working and not working. • Evidence of handling of any exceptions. • Evidence of decisions made along the process • Evidence of go/no go decisions and how they have been made • Evidence of where things have not followed process and what has been done to correct them.
KELS – historic	For each historic KEL prove that the KEL condition no longer exists	• Data needed to proves the KEL has been fixed – will differ in each case
KELS Current	Understand how Fujitsu notice that something is not right	• KELS Process overview within FJ covering people process and technology • Evidence of reporting and decision making around KELS e.g. minutes of meetings, reporting
Horizon Remote Access	How does remote access into work both in the past and now that people are working from home? Covers branch equipment and BRDB.	• Who in FJ has the tools and capability and how do FJ manage this • What are the specific tools and capabilities. • How is the access given and taken away from people? • How is it monitored. • Evidence of all of the above
HNGA robustness	Evidence of functional and non-functional robustness of HNGA	• Evidence of performance and stress testing • Evidence of measures for transactional integrity • Evidence of infrastructure resilience • What are the processes/controls/measures for ensuring that integrity is not breached • Ability to replicate fault conditions for targeting improvements

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

KPMG

Post Office Limited

KPMG LLP

B. Given the judgements the Post Office also wish to establish a cyber and forensic capability. They require assistance in developing a capability focused operating model.

Supplier approach

The Supplier will approach meeting Authority requirements in four phases:

1) Phase 1 – Discovery

The Supplier will work with the Authority to uncover all materials and stakeholders needed to complete subsequent phases, and with the support of the Authority schedule meetings with the stakeholders.

The supplier will draft both high level and detailed plans to manage the timetable that will be used to define the programme timeline. These plans will be agreed with the Authority.

2) Phase 2 – Review of Horizon

A review will be conducted against a criterion agreed between the Supplier and Authority, such as standards as specified in the contract between the Post Office and Fujitsu or any other standing instructions.

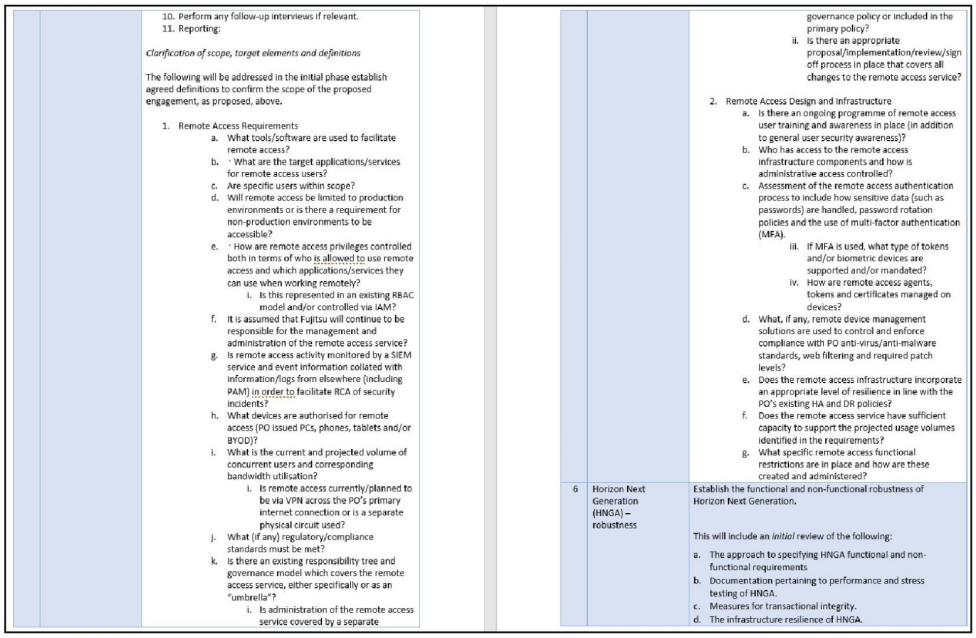
Note: At the time of agreeing this Contract the Authority contract with Fujitsu has not been made available to the Supplier. As such it has not been possible to agree the criterion against which the Supplier will review.

The Supplier will a conduct review of the six areas of Horizon identified in Requirement A. Specifically, this will involve:

#	Area	Description
1	Privileged Access Management (PAM)	Establish who has what privileged access to Horizon at any given time. This will include an *initial* review of the following: a. The processes and technology involved in the management of privileged access. b. The detail/description of the roles that are assigned privilege access and how those approvals are vetted/controlled at a technical level. c. The frequency of privileged level access, specifically those accesses that are granted to the Horizon production environment. d. The purpose of the PAM usage on a case by case basis. e. The audit trail of which activities were carried out and management of any activities that could affect counter transactions data. f. Records of corrective action taken by Fujitsu when failings in the process have been identified. The Supplier will fulfil this task by performing the following actions: *Proposed Approach* The following high-level approach is supported by the details, below (Scope and Definitions AND Target Elements). 1. Establish scope of privileged access 2. Establish baseline for privileged access review 3. Agree report deliverable structure and content (i.e. a 'product description'). 4. Request relevant documentation for privileged access – both Horizon and anything underlying if different (if in scope) 5. Request relevant documentation for PAM management. 6. Review documentation. 7. Arrange meetings with relevant key personnel to discuss relevant topics and clarify any items. 8. Perform interviews. 9. Perform analysis. 10. Perform any follow-up interviews if relevant. 11. Reporting. *Clarification of scope and definitions* The following will be addressed in the initial phase to establish agreed definitions to confirm the scope of the proposed engagement, as proposed, above. Specifically, within the statement "Establish who has what privileged access to Horizon at any given time." Further clarification is required to confirm: 1. Within the scope, how is "Horizon" defined? 2. Within the scope, how is "Privileged Access" defined? 3. Within the scope, what is "at any given time" describing? *Target elements* The breadth of the review will be clarified to ensure that the above scope encompasses the correct target elements for the *initial* review: 1. Processes associated with management of privileged access and their scope. 2. Processes and technology, reviewed according to an agreed baseline, standard, policy or vendor guidelines. 3. The "reporting process" stated relates to what specifically? Is there an agreed approach that POL can provide that can be used as the template to perform the review against? 4. Clarification on the point "how privileged access is granted by Fujitsu" to understand the direction of the question and the underlying concern that raises the question. 5. We will review the corrective actions taken having clarified the perspective from which this is to be delivered.
2	Software Development Lifecycle (SDLC), Testing and Quality Assurance (QA)	Establish how: i) changes to Horizon progress from requirements analysis through development, testing and into early live support; and ii) how such changes become fully live under mainstream support arrangements. This will include an *initial* review of the following: a. SDLC, Testing and QA capabilities within the Post Office and Fujitsu. b. Where the capabilities have failed and why. c. How exceptions are handled. d. Where documentation of decisions has been made throughout the capability. e. Go live/ don't go live decisions and how they were made f. Where process was not followed, why and what was done to address the out of process step. The Supplier will fulfil this task by performing the following actions: • Reviewing and analysing the relevant documentation (e.g. test plans, progress reports, quality gate decision points, etc.). • Interviewing the test staff and test support staff (e.g. test manager, test practitioners, environment manager, release manager, PMO, etc.). • Analysing project boards, project decisions and meeting outputs. • Reviewing action logs. • Reviewing RAIDs. • Analysing defect management, and the decisions made around the acceptance of defects.
3	Known Error Logs (KEL) – historic	For each historic KEL establish whether the condition remains or not. This will include an *initial* review of the following: a. Each KEL end-to-end. The Supplier will fulfil this task by performing the following actions: • See 4 "Known Error Logs – current"
4	Known Error Logs – current	Establish how Fujitsu are made aware of an error. This will include an *initial* review of the following: a. The KEL process at Post Office and Fujitsu, across people, process and technology. b. Reporting and decision making around KELS e.g. minutes of meetings, reporting. The Supplier will fulfil this task by performing the following actions: • Reviewing and analysing the relevant documentation (e.g. KEL technical analysis, root cause, fix requirements, etc.). • Interviewing the staff responsible for decision-making regarding the KEL.
5	Remote Access	Establish how remote access into the Post Office network is conducted – both currently and pre- Covid – to include branch equipment and BRDB. This will include an *initial* review of the following: a. Who in Fujitsu has the tools and capability and how it is managed. b. The specific tools and capabilities at Fujitsu. c. How access granted and revoked and monitored. The Supplier will fulfil this task by performing the following actions: *Proposed Approach* The following high-level approach is supported by the details, below (Scope and Definitions AND Target Elements). 1. Establish the scope of the remote access service review. 2. Establish a baseline for the remote access service review based on current state, compliance requirements and any structural or functional enhancements discovered. 3. Agree report deliverable structure and content (i.e. a 'product description'). 4. Request relevant documentation for privileged access – both Horizon and anything underlying if different (if in scope) 5. Request relevant documentation for remote access management. 6. Review existing documentation. 7. Arrange meetings with relevant key personnel to discuss relevant topics and clarify any items. 8. Perform interviews. 9. Perform analysis.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564



10. Perform any follow-up interviews if relevant.
11. Reporting:

Clarification of scope, target elements and definitions

The following will be addressed in the initial phase establish agreed definitions to confirm the scope of the proposed engagement, as proposed, above.

1. Remote Access Requirements
   a. What tools/software are used to facilitate remote access?
   b. What are the target applications/services for remote access users?
   c. Are specific users within scope?
   d. Will remote access be limited to production environments or is there a requirement for non-production environments to be accessible?
   e. How are remote access privileges controlled both in terms of who is allowed to use remote access and which applications/services they can use when working remotely?
      i. Is this represented in an existing RBAC model and/or controlled via IAM?
   f. It is assumed that Fujitsu will continue to be responsible for the management and administration of the remote access service?
   g. Is remote access activity monitored by a SIEM service and event information collated with information/logs from elsewhere (including PAM) in order to facilitate RCA of security incidents?
   h. What devices are authorised for remote access (PO issued PCs, phones, tablets and/or BYOD)?
   i. What is the current and projected volume of concurrent users and corresponding bandwidth utilisation?
      i. Is remote access currently/planned to be via VPN across the PO's primary internet connection or is a separate physical circuit used?
   j. What (if any) regulatory/compliance standards must be met?
   k. Is there an existing responsibility tree and governance model which covers the remote access service, either specifically or as an "umbrella"?
      i. Is administration of the remote access service covered by a separate governance policy or included in the primary policy?
      ii. Is there an appropriate proposal/implementation/review/sign off process in place that covers all changes to the remote access service?

2. Remote Access Design and Infrastructure
   a. Is there an ongoing programme of remote access user training and awareness in place (in addition to general user security awareness)?
   b. Who has access to the remote access infrastructure components and how is administrative access controlled?
   c. Assessment of the remote access authentication process to include how sensitive data (such as passwords) are handled, password rotation policies and the use of multi-factor authentication (MFA).
      iii. If MFA is used, what type of tokens and/or biometric devices are supported and/or mandated?
      iv. How are remote access agents, tokens and certificates managed on devices?
   d. What, if any, remote device management solutions are used to control and enforce compliance with PO anti-virus/anti-malware standards, web filtering and required patch levels?
   e. Does the remote access infrastructure incorporate an appropriate level of resilience in line with the PO's existing HA and DR policies?
   f. Does the remote access service have sufficient capacity to support the projected usage volumes identified in the requirements?
   g. What specific remote access functional restrictions are in place and how are these created and administered?

6	Horizon Next Generation (HNGA) – robustness	Establish the functional and non-functional robustness of Horizon Next Generation. This will include an *initial* review of the following: a. The approach to specifying HNGA functional and non-functional requirements b. Documentation pertaining to performance and stress testing of HNGA. c. Measures for transactional integrity. d. The infrastructure resilience of HNGA.

Across the six areas additional lines of investigation may materialise as the review is conducted. As such *additional* review areas may be identified and agreed with the Post Office.

For the Supplier to maintain independence and manage potential conflicts of interest, Requirement A will exclude the following:

- Any review of financial controls in relation to financial reporting systems or systems that feed financial reporting systems.
- Any comment as to the effectives of Horizon to provide financial reporting.
- Any KEL that refers to financial reporting functionality, and or KELs that could be used to question the effectiveness of financial reporting systems.
- Any KEL that has a financial recording or reporting impact.

3) *Phase 3 – Review of Horizon - Report*

The Supplier will draft a report with its findings pertinent to the six areas outlined above. The report format will be agreed with the Supplier during the engagement, and may contain narrative documenting issues, findings, risks and recommendations versus the criterion outlined in Phase 2.

The report will be grouped into areas that will easily map to Horizon judgement matters, and the Supplier will provide this mapping.

The report will be KPMG-branded and may need to be disclosed in a public inquiry.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

		e. The processes/ controls/ measures for ensuring that integrity is not breached within HNGA. f. The ability to replicate fault conditions for targeting improvement activities.
		The Supplier will fulfil this task by performing the following actions: • Reviewing the Non-Functional Requirements, and establishing if they are fit for purpose and appropriately detailed. • Reviewing and analysing the relevant documentation (e.g. NFT / OAT plans, progress reports, quality gate decision points, volumetrics, data profiling and analysis, environment configuration, etc.). • Interviewing the test staff and test support staff (e.g. NFT manager, OAT manager, environment manager, release manager, PMO, etc.). • Analysing project boards, project decisions and meeting outputs. • Reviewing action logs. • Reviewing RAIDs. • Analysing defect management, and the decisions made around the acceptance of defects.

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

5.7 Appendix 8: Analysis, findings, and improvement recommendations – Horizon AP-ADC scripts and reference data solution

This document is an assessment of the reference data and AP-ADC scripting software which currently form part of the Horizon computer system.



AP-ADC scripts and reference data assess

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

KPMG

Post Office Limited

KPMG LLP

5.8 Appendix 9: Horizon IT Delivery Robustness Analysis – POL Horizon IT Maturity Assessment

This document is an assessment of the robustness of the Horizon IT capability. It assesses how Horizon IT Services are delivered against pre-defined maturity levels using KPMG's reference IT Maturity Assessment tool. The IT Maturity model is underpinned by industry standards such as ITIL, COBIT and CMMi and will be used to provide maturity scores for processes and capabilities supporting the Horizon platform.



IT Delivery Robustness Assessme

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

POL00337564

Post Office Limited

KPMG LLP

© 2021 KPMG LLP in the UK. All rights reserved. Published in the UK. KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page

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. This Report is provided in confidence and its circulation and use are limited – see Notice on cover page and page 1.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.