



Target Operating Model – Investigations

Group Litigation Order / Horizon IT
Post Office Limited

January 2021
V0.5 – Draft

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.

DRAFT FOR DISCUSSION PURPOSES ONLY



Contents

01	Executive summary
02	Setting the scene <i>Understanding the driver for change, vision and design principles.</i>
03	Current state assessment <i>An assessment of the current state of the investigations function with observations and recommendations.</i>
04	Building blocks <i>The details of what is needed to help re-build Postmaster trust.</i>
05	Moving forward <i>An implementation roadmap to affect the change blueprinted in this TOM.</i>
06	Appendix



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent member firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm via a third party, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential



DRAFT FOR DISCUSSION PURPOSES ONLY

Summary

Background

- This document details the assessment of processes for investigating transactional issues within Horizon at the Post Office Limited (POL) and the target operating model (TOM) with focus on Horizon investigation support to be provided by Horizon & GLO IT function. It has been authored by KPMG LLP (KPMG) in conjunction with extensive consultation with and input from stakeholders across POL such as investigation teams as well as the GLO / Horizon IT Director and his team.
- The design of the TOM has been driven by one primary need: to re-establish trust with Postmasters following the GLO and preceding years of prosecutions and convictions of Postmasters for offences such as theft and false accounting which were cleared.
- The report is divided into 5 sections: Setting the scene, Current state assessment, TOM for Horizon investigation support team, Indicative implementation roadmap and Appendices.

Summary

For more detail and rationale

Setting the scene

Drivers for change for Horizon investigation processes has been captured. Vision for Horizon investigation support team has developed along with design principles for developing the TOM.

Page 6

Current state assessment

The assessment of the current state of Horizon investigation processes has been performed through interviews with investigation teams within POL operations capturing findings and recommendations

Page 13

Building blocks

Services, processes, accountabilities and responsibilities, capabilities and metrics, organisational structure, and interfaces have been defined for Horizon investigation support team. Together they provide the architectural blueprint of what the Horizon investigation support team needs to look and operate like.

Page 23

Moving forward

Distinct initiatives have been defined based on recommendations following current state assessment and mapped into an indicative implementation roadmap

Page 46

Appendices

Detailed design requirements are included for processes, case triage, roles and responsibilities, transaction tolerance levels and technology

Page 51



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent member firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

Inputs and outputs

Various inputs and activities fed the creation of this report. They are summarised below

Inputs

- Lark Hill and Avondale Road investigation reports
- Overview of the IT architecture of Horizon
- Reference listing for message codes used in Horizon endpoint terminals
- Sample key logging documentation
- Sample ARQ data request form
- Sample BRT transaction corrections
- List of products handled by BRT
- List of BRT thresholds for discrepancy write-off
- Sample checklists used by investigations teams
- Lists of reports used by investigations teams
- Organisational charts

Activities

- Interviews with 10+ teams involved in investigation of transactional issues within Horizon as well as Fujitsu
- Workshops with the sponsor and Horizon Investigation Support team
- Assessed current process for investigating transactional issues within Horizon
- Captured current investigation process
- Developed detailed view of To-Be investigation processes
- Defined stakeholders, capabilities, roles and organisational structure
- Understood current tooling architecture and interfaces
- Developed specific recommendations in regards to data transfer, data consolidation and processing, data requirements for Fujitsu, case triage, use cases for data platform
- Prioritised proposed initiatives

Outputs

- Current state assessment of investigation processes
- Vision and Design principle for Horizon Investigation support team
- Case for change
- Key differentiators between future state and current state
- Current Process Map Level 1 (Visio)
- 'To-be' Data Driven Investigation Process Chart - Level 0, 1 and 2
- Recommendations for data transfer, data consolidation and processing, data requirements for Fujitsu, case triage, use cases for data platform
- TOM building blocks for Horizon Investigation support including services and processes, accountabilities and responsibilities, capability requirement and metrics, org structure and interfaces
- Indicative implementation roadmap
- Current data sources by investigation team



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent member firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential



L02

Setting the scene

Understanding the driver for change, vision and design principles.

 © 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent member firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

6

What is Horizon?

Horizon is the Post Office core Branch computer system

Horizon can be described as a set of technologies which allow POL branches to sell POL products and services to consumers, reconcile branch accounting positions and pass information to third parties including clients of POL and external service providers. It consists of two primary functions: The range of products sold at the POL branches consist of Postal Orders items which are provided only through a POL branch and products such as stamps, mail, foreign currencies which can be purchased elsewhere.

1. **Branch.** Technology which is present in the Branches such as computer terminals and peripherals (e.g. key pads, printers) which allow users to sell products to consumers, allow Postmasters to set up branch users of the system and perform basic accounting and reporting functions. The hardware present in the branch is managed and supported by Computacenter.
2. **Network Infrastructure.** The branch access network is provided by Computacenter whilst the distribution network providing connectivity between branches and the Horizon back end is provided by circuits operated by Verizon. Distribution to client and external third parties is provided by a combination of Verizon and Fujitsu managed circuits. The Core network operating in and between datacentres is provided and managed by Fujitsu.
3. **Back end.** Technology which allows the branches to connect to the main Horizon back end functions and those back end functions themselves which provide access to reference data, and the main accounting reconciliation processes and the interfaces between third parties. These elements of the platform are managed and supported by Fujitsu:
 - i. Extract Transform and Load (ETL) services which provide batch output services between the Horizon platform and third party clients (e.g. British Gas etc.);
 - ii. Extract Transform and Load (ETL) services which move data within the Horizon Platform itself for reconciliation purposes;
 - iii. Extract Transform and Load (ETL) services which take data from third parties (such as reference data and paystation data) and push this into the Horizon Platform;
 - iv. Generic Web Services which allow interrogation of third party services (such as bank authorisation services) and post data to third parties such as actual payment transaction data; and
 - v. Automated Payments Advance Data Capture (AP-ADC) A facility which allows the Post Office to make configuration changes, add products, change customer journey's and orchestrate calls to Generic Web Services without having to involve Fujitsu in the change and testing cycles. This facility uses a proprietary programming and configuration structure.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

Vision

Postmaster experience and trust is at the heart of this TOM's vision

POL's vision for Horizon & GLO IT TOM is:

"To improve the Horizon user experience and Postmaster service, by re-establishing a level of trust and confidence in Horizon – specifically with regards to platform security, data integrity and supplier management."

POL's vision for Horizon investigation support team is:

- "To improve and ensure the use of data and data driven processes in investigating transactional issues within Horizon to drive to more robust investigation outcomes for both Postmasters and POL supported by appropriate technology."



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties. Nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential



Case for change

The need for change is clear. Post Office must re-establish trust with Postmasters.

Context

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

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

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

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

Subsequent actions

In response to the Judgement in October 2020 POL engaged KPMG to help them design TOM for a newly formed GLO / Horizon IT team.

Desired outcome

The desired outcome of this activity is an exceptionable blueprint from which change could enacted to rebuild trust with Postmasters.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm. KPMG International and its member firms are not liable for the actions or omissions of any member firm. All rights reserved.

Document Classification: KPMG Confidential



DRAFT FOR DISCUSSION PURPOSES ONLY

Design principles

The selected overarching design principles for Horizon & GLO IT have been applied to the investigations TOM. They are as follows.

Overarching Design Principle	Design criteria for investigations
Enable data driven decision making	<ul style="list-style-type: none"> • Ensure consistency and auditability of investigation process • Every investigation is conducted using a standard methodology and is carefully documented
Improve Horizon user experience for Postmasters	<ul style="list-style-type: none"> • Ensure that the Postmasters are as satisfied with the investigation service as possible – speed, communications, quality of outputs of the investigation process – as well as fairness of dispute resolution process
Use technology to POL's advantage	<ul style="list-style-type: none"> • Enabling technology is in place to support investigation processes to reduce chances of manual errors and detect and prevent issues from happening



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

Current state and to-be state comparison

Below are key areas of change between current, near future and long term target states for the investigation process.

	Theme	Change	Impact
Near Future (within 6 months)	Investigation Triage Step	Introduction of a Triage step at the beginning of the investigation to evaluate the investigation cases, assessing whether it should be pursued, prioritised and escalated to the appropriate team.	Allows the investigation teams to be more efficient, limit time spent on smaller issues and focus on more contentious matters. The priority issues can be focused on, driving faster and more effective resolution of cases.
	Horizon Investigation Support Team	Introduction of the dedicated investigation team to support the financial investigation teams to perform data driven investigations and drive for the development of industry practice approaches.	By working with the financial investigation teams, the Horizon Investigation within Horizon & GLO IT function will help to instil industry practice data driven investigation processes. Being heavily involved with the Lessons Learned process will help to identify new issues, new data sources and how the existing process need to change.
	Lessons Learned	Introduction of the 'Lessons Learned' step after investigations.	Mechanism to underpin and encourage positive change to investigation workflows, analysis processes, and, later, to technology driven investigation Business Logic when Data Platform is introduced.
	Validation Procedures	Introduction of Validation steps to ensure data integrity (Digital Fingerprint) when receiving data from Fujitsu and other third parties.	Following industry practices when handling data helps to ensure that the data and potential evidence is admissible in court.
	Dynamic Investigation Workflow	Introduction of consistent investigative workflow approach driven by the Case Management tool, instead of checklists. Each Investigation team would have their process workflow specific to the type of work they do.	Allows for automation of the collection of the data sources required and generation of a template report. Drives good practice across the investigation teams and allows for an auditable and consistent approach.
Long Term (1+ years)	Single Source of Truth (Data Platform)	Taking an active part in the development of the 'Data Platform' initiative within POL, drafting use cases for the investigative reports.	Data Platform can reduce the reliance of the POL on Fujitsu by having the data available and managed by POL. This would become the key place to extract raw data in the first instance (in its initial form) but, with time, would allow for the BI layer to sit on top that would provide the data insight to the investigation teams.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

11

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

What is an operating model?

An operating model describes how a function organises and governs its capabilities and assets to deliver its strategy. By considering six key components, we ensure that a holistic solution is built which considers all aspects of an organisation



This model has been used to inform the building blocks found in Section 4.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent member firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential



L03

Current state assessment

An assessment of the current state of the investigations function with observations and recommendations.

 © 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm via a third party, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

13

DRAFT FOR DISCUSSION PURPOSES ONLY

Current state assessment

Findings and recommendations have been captured in the following areas: governance and reporting, processes, people and training, source information and data and systems and tools

Area	Theme	Observations	Recommendations
Governance & Reporting	There is a lack of centralised co-ordination of investigations and assurance of investigation processes	<ul style="list-style-type: none"> Currently there is no apparent centralised co-ordination of investigations within POL, including no clear/consistent reporting lines to the Board, or consistent Board level accountability and/or oversight. As a consequence, the Post Office risks a lack of consistently applied processes, project management rigour and subject matter expertise to ensure efficient investigations across the firm. In particular, this is likely resulting in: <ul style="list-style-type: none"> Potential duplicative data requests, such as to Fujitsu; Potential over collection of data across multiple vendors (with corresponding data costs) and with little or no re-use of data or work product; Lack of knowledge management shared across teams/departments; and Higher investigation costs. 	<ul style="list-style-type: none"> Introduce a centralised investigations function, with clear reporting lines to board level
	There is a lack of understanding of Postmasters' needs from a technology perspective	<ul style="list-style-type: none"> One of the root causes of stock discrepancies is the non user-friendly interface of Horizon terminals. Changes to Horizon do not take into account Postmasters' needs There is no single owner of the development changes required from Horizon, hindering improvement. Having a holistic view of the Postmasters' requirements and being able to prioritise them can help to achieve best results from Horizon efficiently. 	<ul style="list-style-type: none"> Introduce a Horizon System Product Owner Role to improve understanding of Postmasters' needs and ensure prioritisation of initiatives for the benefit of this primary user group
	There is no consistent approach to risk management for investigations	<ul style="list-style-type: none"> There does not appear to be consistent centralised approach to conduct risk management activities and to assist the investigations teams to identify, manage or remediate investigations processes related risks. This has resulted in limited oversight of high level, strategic, operational, emerging and known risks for investigation processes An example of a higher level risk could be an introduction of a new product that is not integrated into Horizon systems which could result in data validation and following data driven investigation process difficult to achieve. 	<ul style="list-style-type: none"> Risk management should fit in to a structure which ensures consistent alignment with Horizon risk team and Enterprise Risk Management (POL Central Risk team). This point has been subject to further investigation and guidance from the audit stream and is raised in sub-themes 8 and 9 of the Post Office_ Interim Report v2.1.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent member firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

14

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

Current state assessment (cont.)

Area	Theme	Observations	Recommendations
Governance & Reporting (cont'd)	There does not appear to be consistent monitoring of KPIs for investigation teams	<ul style="list-style-type: none"> While certain investigation teams do appear to have some KPIs tracked, these appear to be monitored on an individual unit basis, rather than centrally. Without consistent and accurate KPIs, it is difficult to understand which investigation teams are performing better/worse, and where the focus for budget spend and process improvements should be. 	<ul style="list-style-type: none"> Develop KPIs and MI for investigations teams Introduce centralised review and monitoring of KPIs and MI
	There are no independent third parties involved in investigations	<ul style="list-style-type: none"> Investigations are primarily conducted internally by POL and Fujitsu. There may be a risk of a perceived conflict of interest or self-review. This may affect Postmasters' trust in POL in regards to the outcome of investigations. 	<ul style="list-style-type: none"> For high-profile cases or disputes, consider the use of an independent third party investigation or review team, or an organisation trusted by Postmasters, such as the National Federation of Sub-postmasters (NFSP)
Processes	There is a lack of documentation of processes and methodologies to be used by investigative teams and Postmasters	<ul style="list-style-type: none"> Teams do not appear to have consistently documented methodologies which cover their work, in part because of the variety of products and situations that are investigated. Some teams follow checklists, but they readily acknowledge that these include steps not applicable to some investigations. There is an inherent business risk that the loss of key experienced personnel may lead to significant process knowledge gaps if the knowledge transfer does not happen. It tends to be more difficult to benchmark performance and consistency in the absence of formally documented procedures. It is also more difficult to identify process efficiencies in the absence of formal processes, as each team member may conduct their work differently. If work performed is not readily auditable or consistent, it could potentially result in a lack of consistency or fairness in approach and outcome. Limited validation of data inputs appears to be carried out by investigation teams that we have spoken to. Data sourced from third parties is not consistently logged / uploaded into POL case management systems making it more difficult to investigate or review older cases. Whilst knowledge base for Tier 1 investigators exist and they do their best to advise Postmasters during the support call, access to knowledge base and detailed instructions for Postmasters is not utilised to its full potential. If the training material for Postmaster on how to achieve common Horizon tasks does not exist, it increases the effort of investigating common issues. 	<ul style="list-style-type: none"> Document investigation methodologies, including review and redesign of existing checklists, where required Greater use of workflow tools within Dynamics to drive investigation steps for specific teams Implement data validation steps Enforce logging / uploading of all case related data and evidence into the case management system Provide and encourage the development, maintenance and use of detailed instructions for Postmaster on how to execute common tasks to help promote good practice – this should be part of an end-to-end instruction knowledge base for all elements of Horizon which contributes to an effective operating model.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent member firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

15

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

Current state assessment (cont.)

Area	Theme	Observations	Recommendations
Processes (cont'd)	There is limited evidence of 'lessons learned' being captured and shared within and between investigations teams	<ul style="list-style-type: none">Without 'lessons learned' or other type of 'post-incident activity' it is very difficult to understand the variety of cases, report on them (MI) and crucially improve for the future.Post-incident activity helps drive development of more efficient investigations and improvement of the Horizon system. Development of new investigative techniques or improved detection models is hindered without this crucial step.	<ul style="list-style-type: none">Introduce post-incident activity ('lessons learnt'), documented and shared, as a step of every investigation.
	The methodology for triaging investigations does not appear to be documented.	<ul style="list-style-type: none">There are not clear triage processes in place to identify and escalate the most high risk or high profile cases.At present, where limited triage is in place, it is largely based on product type and case age.Without a formally documented methodology for prioritising investigations, it potentially results in investigations not being tackled in the most appropriate order.It also leaves the investigations team open to a lack of consistency in response times.	<ul style="list-style-type: none">Document triage methodology, setting criteria for assignment and escalation of investigations.
	De minimis criteria are not applied to investigations leading to a high number of investigation cases and delay in resolution	<ul style="list-style-type: none">At present, POL do not apply de minimis levels to determine whether investigations will be pursued. This means that investigations are pursued, even where the financial value in question is less than the cost of the investigation. This can lead to a backlog of cases, longer resolution times, and higher investigation costs.Whilst the BRT (Branch Reconciliation Team) used product-based 'low value tolerances' to determine if discrepancies are automatically written off, these are not intended to be used in the context of investigations. These only consider monetary values, rather than any associated risks.POL should also consider the risks and implications involved when opting not to undertake a thorough investigation, similar to a cost-benefit analysis.Applying a de minimis level, below which POL would not investigate, could help to reduce workload and cost, and allow greater focus on priority cases.	<ul style="list-style-type: none">Introduce de minimis criteria for investigations at case triage stage.
	There is no documented mechanism for resolving disputes with Postmasters.	<ul style="list-style-type: none">Currently POL does not have a documented process in place to resolve disputes with Postmasters in situations when investigations do not find evidence of Horizon being at fault, or where Postmasters do not accept the findings of an investigation.	<ul style="list-style-type: none">Develop process for resolving disputes with PostmastersIntroduce a 'Review Committee' for disputed cases which are high risk or high profile. This would consist of GLO leadership, Legal Risk, and other key stakeholders able to make a business decision on how to proceed.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

16

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

Current state assessment (cont.)

Area	Theme	Observations	Recommendations
People & Training	There do not appear to be formal channels for knowledge sharing, or identifying additional training requirements	<ul style="list-style-type: none"> With KPIs not centrally tracked, methodologies not documented, and investigation prioritisation not consistent/clear, it is difficult to rapidly identify where knowledge gaps and deficiencies might lie. Learnings do not appear readily shared between teams as standard e.g. we understand that the sharing of Tier 3 (CIRT) to Tier 2 (BSC T2) learning points is a very recent development. The majority of training appears 'on-the-job' rather than formally taught, which could promote the recurrence of legacy issues. In order to increase the capability investment in training, key milestones and defined career paths are required. Leveraging in-house knowledge can help to establish suitable training content to minimise the training costs. 	<ul style="list-style-type: none"> Introduce lessons learned as a key part of investigations Introduce formalised knowledge sharing opportunities between colleagues in investigation teams and broader POL teams Define career progression, identify and invest into key training required for the operations investigation teams, aligning with POL's response plan to the Findings on culture and people development.
	Product related investigation expertise varies among team members	<ul style="list-style-type: none"> The investigation processes are complex as it requires a product specific investigation approach depending on transactions performed by a branch Investigations processes will vary based on the requirements of these individual products 	<ul style="list-style-type: none"> Leverage product specialists for investigation purposes Review and document investigative processes for specialist products
	There is a lack of forensic data driven investigation capabilities within investigation teams within Operations	<ul style="list-style-type: none"> Existing investigation teams have good knowledge of the POL's finance systems and transaction processes, however there is a need to complement their investigations with specialist forensic data investigation capabilities to follow data driven investigation processes. Anecdotal evidence suggests that the majority of the current investigations team were not actively recruited into the team based on previous investigations experience or training. There is a risk of potential capability gaps. 	<ul style="list-style-type: none"> Introduce Horizon Investigators Conduct capability assessment in investigation teams to identify any potential capability gaps Introduce investigation team training and development initiatives, aligning with POL's response plan to the Findings on culture and people development.
Source Information & Data	There does not appear to be centralised co-ordination or collaboration between teams for data requests to third parties	<ul style="list-style-type: none"> Different investigation teams do not appear to collaborate with regards to requests for external data sources (such as Credence licences or specific Fujitsu data requests) which may lead to the duplication of data costs. 	<ul style="list-style-type: none"> Introduce centralised coordination of requests to external data suppliers



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

17

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

Current state assessment (cont.)

Area	Theme	Observations	Recommendations
Source Information & Data (cont'd)	There is a need to get information from multiple data sources to conduct investigations making the process open to human errors and labour intensive	<ul style="list-style-type: none">Investigation teams require data from a wide variety of systems and data sources, a number of which are not Horizon-driven (e.g. Puzzle, Playstation, Banking data, Camelot).Sourcing of data from multiple unconnected systems and the need to manually manipulate data make this process prone to human error, reducing confidence in investigation outputs.Accessing data older than 12 months must be raised via ARQ (via Security Team to raise to Fujitsu). The request also comes at a cost to business.The response time on ad hoc data requests from Fujitsu may vary depending on who makes the request.Establishing clear process for the data exchange with Fujitsu will help to reduce response times to obtain data as a business.<ul style="list-style-type: none">Agreeing contractually Fujitsu's obligation to provide the data, e.g. via an SLA.Consider tiered SLA: P1-Urgent, P2-Normal, P3-Low Priority	<ul style="list-style-type: none">Introduce "single source of truth" for data - Data Platform – to help to support integration of data sources reducing chances of human errors.The automation within Data platform can help generating dedicated reports for the investigations teams.Introduce the Data Platform to reduce the reliance on Fujitsu, allowing POL to store information as required internally.Establish clear process for the data exchange with Fujitsu.
	There is limited availability and use of the Key Logging functionality	<ul style="list-style-type: none">Key Logging data is considered useful for investigations, but is only retained by Fujitsu for 180 days, which may not be long enough for typical investigations.There is an inconsistent approach to Key Logging information, with some teams using it regularly, with others not using it at all.There is a lack of a defined process for obtaining Key Logging information.The scope of the Key Logging function is limited, as it was originally designed as a debugging tool. Currently the function only logs Horizon User Interactions, Pin Pad and Counter Printer. Keystrokes, such as monetary values entered, are not recorded.Logs containing this information reside on EPOS terminals which require an ad-hoc process to capture and preserve logs on a case by case basis.If the scope of the Key Logging data recorded is widened, POL should be aware of any GDPR compliance requirements applicable to the data.	<ul style="list-style-type: none">Integrate the Key Logging information into existing investigative stepsNew, more robust and defined process for storing and providing Key Logging information to POL investigations, governed by an SLA.Request an expansion of the scope of Key Logging data and data retention period from Fujitsu.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm via a third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

18

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

Current state assessment (cont.)

Area	Theme	Observations	Recommendations
Systems & tools	Horizon user functionality is inherently deficient	<ul style="list-style-type: none"> The Horizon interface is not user friendly, especially for certain transactions (e.g. lottery or cash handling), leading to high volume of user errors, manual workarounds and transaction corrections <ul style="list-style-type: none"> The review of stamp stock processes conducted in July-August 2020 suggests that Postmasters are required to settle the value of shortfalls by converting the stamp shortage into a cash loss by posting "balancing sales" through Horizon. Such sales are not distinguishable in the total sales due to the way they are processed on Horizon The analysis performed by POL in Nov 2020 suggests that in P08 2019-P07 2020 POL has issued 133,716 transaction corrections. 82% of those transaction corrections come from top 5 products – Cash Rems from branch (48%), Camelot (24%), ATM Retracts (3%), Suspense including Cash/Bureau Suspense (3%) and Bureau (3%) Some teams expressed frustration that there have been no improvements to Horizon at its core functionality. Reporting functionalities remain limited, without significant data insight. 	<ul style="list-style-type: none"> Identify user pain points and improve Horizon functionality Introduce Data Platform with advanced Data Analytics logic and dedicated investigative reports
	There are limited controls and safeguards for cash handling in place within branches	<ul style="list-style-type: none"> Cash-related issues are the primary driver for Transaction Corrections. It seems that there are no automated controls and safeguards in relation to cash handling within branches, e.g. no intelligent/smart cash till, no reliable CCTVs monitoring the till. CCTV can't be / isn't commonly used in investigations, as ownership of systems lies with individual Postmasters. Whilst some investigators said this was used in investigations, in practice it relied on Postmaster reviewing footage themselves and providing a written / verbal "confirmation" of events. The use of CCTV is not standardised in branches. CCTV is not designed to monitor tills to evidence cash fraud or genuine mistakes, and its use cannot be enforced in branches. Data privacy concerns were also expressed, as the CCTV footage is primarily for the use of Postmasters themselves. Reduction in cash-related issues would reduce the amount of TCs required and improve the Postmaster experience. Intelligent/smart tills are available in the market that could report the cash position directly to Horizon making reconciliation more efficient and reliable. Additionally, cash counting machines could be used as a low cost alternative to reduce the high volume of Transaction Corrections. 	<ul style="list-style-type: none"> Consider implementation of CCTV, intelligent / smart tills, or cash counting machines, to reduce volume of cash-related issues



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

19

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

Current state assessment (cont.)

Area	Theme	Observations	Recommendations
Systems & tools (cont'd)	Limited and not 'fit for purpose' core investigation tools (Credence, HORice)	<ul style="list-style-type: none">The core tools used by various investigation teams are limited in functionality and data retention.Data retention periods are quite short (max. 12 months HORice or 3 months Credence).Credence data is updated overnight, so Credence provides data on a one day delay.HORice is only a 'borrowed' tool, although it is a core tool used by various investigations teams. POL's right to use it is limited and not protected/guaranteed contractually.There is no means to verify the correctness of the data from these systems.There is a lack of consistency between teams - various teams use different tools and choose them based on their preference.Lack of reliable tools with readily available investigation reports with the data insight leads to inefficient investigation processes and could result in inconsistent outcomes.Data Platform/Lake project (lead by Ruk Shah) has already been started but was put on hold. Data retention of the various information stored in Data Platform will be complex (including requirement for Legal Hold), but is an important point to consider.	<ul style="list-style-type: none">Use of POL owned 'single source of truth' database to allow for complete data to be stored and retrieved as a self-serve basisImprove functionality and widen usage of existing tools (e.g. FREDD-O) to produce dedicated reports for the investigation purposes in the short term
	There is an inconsistent use of telephony systems across teams	<ul style="list-style-type: none">Anecdotal evidence suggest that there is an inconsistent use of POL's telephony system (Puzzle) to record calls made to Postmasters within Postmaster facing teams. Therefore evidence of Postmaster engagement, or evidence of advice given/not given to Postmaster, may not get recorded. This could leave POL without critical evidence points at a later stage, particularly if Postmasters' state they were following advice/instruction given by POL.According to Puzzle SME there are no policies in place mandating POL staff to use the system for calls to branches calls but POL staff are guided to use Puzzle during the training	<ul style="list-style-type: none">Mandate use of telephony systems (such as Puzzle) across Postmaster facing teams
	There is a lack of security monitoring tools on EPOS terminals	<ul style="list-style-type: none">Horizon remains the only key source of information for the EPOS terminalsWithout other monitoring tools it may be difficult to validate the potential issues with Horizon.According to POL representative, there appears to be no security monitoring tools (such as Endpoint Detection and Response) functionality which would allow an additional layer of visibility of Horizon terminals.	<ul style="list-style-type: none">Introduce security monitoring to allow for identification of critical infrastructure failure, and issues with Horizon terminals



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

20

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

Current state assessment (cont.)

Area	Theme	Observations	Recommendations
Systems & tools (cont'd)	Investigations are typically reactive, rather than proactive	<ul style="list-style-type: none">The Post Office has a largely reactive response to investigations, with matters being managed in silos, often in an ad hoc manner. As a result, there can be a mis-alignment of capabilities to tasks.There is no trend and pattern detection, leading to potential scenarios where multiple calls about a similar issue are raised to different analysts, but no one to connect events and address a root cause.There are pockets of excellence which use advanced analytics model for proactive investigative work:<ul style="list-style-type: none">The internally developed analysis tool FREDD-O is a rich and centralised source of data (importing data from Credence, CFS, HORice, Dynamics, etc) but appears to be underutilised by teams outside of the Branch Analysis Team.This risk-based model identifies high-risk branches, allowing to prioritise investigations into them and have a defensible approach.FREDD-O is currently used for detailed analysis of branches individually, though could potentially support analytics of issues that are raised or impact multiple branches to systematically identify widespread issues.Data validation steps were limited to the formatting steps only.While the model is advanced, FREDD-O does not use real time data limiting its ability to dynamically investigate more recent events.	<ul style="list-style-type: none">Introduce predictive or proactive tools to identify high risk transaction or branches e.g. consolidated reporting on Helpdesk queries (covering IT and Business support) including Data Analytics designed to identify the issues/trends at scale.Introduce centralised issues log having a streamlined process for tracking issues - 'single source of truth'.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

Current state assessment (cont.)

Area	Theme	Observations	Recommendations
Systems & tools (cont'd)	Insufficient access security controls within the Case Management System (Microsoft Dynamics)	<ul style="list-style-type: none">The existing case management system used by the investigation teams (Dynamics) is setup in such a way that allows all members of an entire business unit to access all cases and the sensitive information contained therein.It is understood that the historic and closed cases can be used as a reference by other investigators and other investigative teams in order to keep track of the interactions with Postmasters, or to aid identification of recurring issues. Immediate access to old cases is required in order to provide prompt response and good level of service to Postmasters.Access to the system should be controlled on a timely need-to-know basis and should be auditable. Both of which can be achieved if Dynamics system is implemented with these principles from the beginning.We were advised by Dynamics SME that auditing and monitoring of access to cases and attached sensitive information is not possible within the current Case Management system (Dynamics) used by the investigation team.The current system (Dynamics) is managed by Fujitsu, meaning that Fujitsu have full administrative access to the confidential information (which is not audited). In addition, it is worth noting that any new development requirements requiring additional development costs.Not having sufficient access security controls and auditing controls conflicts with POL's intent regarding the Judgement and openness with Postmasters.As standard industry practice, access controls should consider all user types and their levels of access (read only, write) with time bound controls for elevated levels of capability or activity, such as administrators or high-value approvals.At an application level we would expect to see workflows based around categories of user:<ul style="list-style-type: none">Creators and case workers being able create/modify the case, until they pass the responsibility to another investigator / team;Triage decision makers with approval rights as a limited group individuals;System administrators who are not part of a standard workflow with access to cases by request (say supervisor-type delegator).Full activity auditing within the application logs for all workflow and user activitiesThe controls should form part of a broader identity and Access Management strategy ensuring the right person gains access to the right resource at the right time in a well-managed and reportable manner.	<ul style="list-style-type: none">Review the current Dynamics approach to assess whether application access security controls and workflows can be improved to provide acceptable controls and reporting.If this is not feasible, consider introducing a different case management system.Assess the data security and privacy of information stored within the case management system. Verify if the Auditing is not possible to be enabled with the Dynamics.Introduce additional training around data protection and strengthen the confidentiality policy for the investigation teamsIf additional access controls and restrictions are introduced, consider adding a step to produce brief sanitised summaries of cases at the conclusion of an investigation to be used as reference for any future investigations (knowledge base). Any sensitive or confidential information should be removed. These should be saved within the system and identify the root cause, proposed resolution and outcome for the Postmaster.Align to the recommended identity and Access Management (including elevated access) approach.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

22


Document Classification: KPMG Confidential



L04

Building blocks

The details of what is needed to help re-build Postmaster trust.

 © 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent member firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

23

Building blocks

The model introduced on page 12 has informed the selection of the following building blocks.

A. Services

- Outlines proposed core services provided as part of investigation process.

B. Processes

- Outlines proposed core processes delivered as part of investigation process. Details are found in Appendix 1 and 2.

C. Accountabilities and responsibilities

- Outlines proposed accountabilities and responsibilities for Investigation support team within Horizon and GLO IT function.

D. Capabilities and metrics

- Captures capabilities required to deliver Investigation activities in scope of Horizon & GLO IT function and related performance metrics as well as differences in capabilities between CIRT and Investigation support team

E. Roles and responsibilities

- Describes the role of Investigation support team within GLO / IT Horizon and organisational structure needed to execute the services, processes and capabilities. Details are found in Appendix 3.

F. Interfaces

- Details proposed interfaces for the Horizon & GLO IT function with internal and external stakeholders in regards to investigations

G. Technology and Data

- Summarises technology needed and required changes for processes for obtaining data for the investigations function. Details are found in Appendices 5 and 6.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm. KPMG International and its member firms are not liable for the actions or omissions of any member firm. All rights reserved.

Document Classification: KPMG Confidential





Services

Outlines proposed core services to be delivered by the investigations function.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

25

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

Investigation Services - target state

We have defined activities comprising the resolution of transactional issues related to Horizon in four service steps below. The processes supporting each service are outlined in Building block B

Services	Process Objective	Description
Plan Investigations	<ul style="list-style-type: none">To decide on a strategy to resolve customer disputes related to transactional issues within Horizon and design the approach	<ul style="list-style-type: none">The Plan Investigations process determines how the organisation resolves disputes raised by Postmasters in regards to transactional issues within Horizon from start to finish, end-to-end and what capabilities need to be developed as well as sets standards for internal investigation processes. Its ultimate goal is to make the organisation think and act in a strategic manner
Execute Investigations	<ul style="list-style-type: none">To make sure that investigations are delivered in line with set out standards and procedures	<ul style="list-style-type: none">The Execute Investigations process includes specific steps that the organisation needs to undertake to investigate cases
Review Investigations	<ul style="list-style-type: none">To make sure that IT services are delivered effectively and efficiently	<ul style="list-style-type: none">The Review Investigations process includes specific steps that the organisation needs to undertake to improve efficiency and effectiveness of its investigation activities
Prevent Investigations	<ul style="list-style-type: none">To reduce volume of Horizon transactional issues	<ul style="list-style-type: none">The Prevent Investigations process includes monitoring of new requests from Postmasters to identify trends and address them in a proactive manner



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

LB

Processes

Outlines proposed processes for the investigations function. Details are found in Appendix 1 and 2.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

Horizon investigation processes - target state

The table below captures target state processes comprising services delivered by POL to resolve disputes with Postmasters, related to Horizon. They will be used to describe responsibilities and accountabilities.

Services=>	1. Plan investigations	2. Execute investigations	3. Review investigations	4. Prevent investigations
Processes=>	1.1 Develop HZ investigation & dispute resolution strategy	2.1 Triage case	3.1 Review investigation activity	4.1 Analyse helpline activity
	1.2 Set processes & standards	2.2 Initial review	3.2 Define CSI	4.2 Take preventative actions
	1.3 Plan capacity	2.3 Investigate inc. lessons learnt	3.3 Manage CSI delivery	
		2.4 Investigate high profile cases inc lessons learnt	3.4 Assure processes	
			3.5 Develop capability	
			3.6 Manage knowledge	



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

28

DRAFT FOR DISCUSSION PURPOSES ONLY

Horizon investigation processes - target state (cont.)

The table below describes Level 2 processes within each Level 1 process.

Services	Processes L1	Processes L2
1. Plan investigations	1.1 Develop HZ investigation & dispute resolution strategy	Develop strategy and framework for responding to Postmasters queries in regards to transaction corrections and resolving disputes
	1.2 Set processes & standards	Set investigation processes and standards (including SLAs for dispute resolution)
	1.3 Plan capacity	Assess expected demand for investigation activities Plan resources for conducting investigations
2. Execute investigations	2.1 Triage case	Review and prioritise cases and allocate to a relevant team
	2.2 Initial investigation	Attempt to resolve Postmasters queries using knowledge articles
	2.3 Investigate inc. lessons learnt	Including validations steps, lessons learnt identification
	2.4 Investigate high profile cases inc lessons learnt	Including validations steps, lessons learnt identification
3. Review investigations	3.1 Review investigation activity	Review current and complete investigation cases
	3.2 Define CSI	Identify scope of Continual improvement initiatives
	3.3 Manage CSI delivery	Manage delivery of Continual improvement initiatives and drive change
	3.4 Assure processes	Assess quality of complete investigation cases against set standards Identify gaps in investigation standards and feedback
	3.5 Develop capability	Develop / update capability development programs and materials Run training sessions
	3.6 Manage knowledge	Update knowledge articles
4. Prevent issues	4.1 Analyse helpline activity	Monitoring (near real-time) of cases raised by Postmasters with the Helpline in regards to Horizon Identify root cause and trends
	4.2 Take preventative actions	Define and plan preventative actions Execute preventative actions



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

29

Document Classification: KPMG Confidential



Process accountabilities and responsibilities

Outlines proposed accountabilities and responsibilities for investigations processes.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

30

Document Classification: KPMG Confidential

Responsibilities & accountabilities - current state

Below are the processes introduced in building block B and mapped against teams with current responsibility and accountability. There is currently no teams with responsibility and no accountability. Only the operations team is currently accountable and responsible.



Key

Accountability & responsibility

Responsibility w/o accountability

DRAFT FOR DISCUSSION PURPOSES ONLY

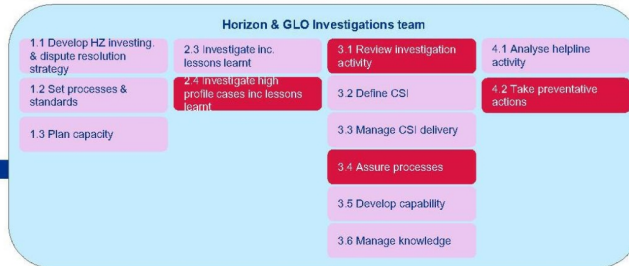
Responsibilities & accountabilities - target state

Below are the processes introduced in building block B and mapped against the target state responsibility and accountability, by team.



Key

Accountability & responsibility
Responsibility w/o accountability



The proposal is that the Horizon / GLO IT team takes ownership of a number of investigation processes as well as support Operations on other processes.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent member firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

32

LD

Capabilities and metrics

Captures capabilities required to consistently and reliably manage the instigations function.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

Capability requirements and metrics

Based on the scope of services and processes to be undertaken by Horizon & GLO IT function, by colleagues who will form Investigation Support Team, capability requirements and performance metrics have been proposed

Investigation Support Team's purpose

To improve and ensure the use of data and data driven processes in investigating transactional issues within Horizon to drive to more robust investigation outcomes for both Postmasters and POL supported by appropriate technology

Required capabilities

Forensic accounting

Investigation expertise

Investigation process design

Investigation assurance

Change mgmt

Metrics*

- Average # of open investigation cases
- % of investigation cases complete within SLA with Postmasters
- % of cases resolved to the satisfaction of both parties
- Average time to complete investigation
- Average time to respond to Postmasters

* Subject to availability of SLAs and processes for measuring KPIs



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

Capabilities and experience by investigation team - target state

This slide outlines differences focus, capabilities and desired experiences for each investigation team

Team	Description & focus	Capabilities	Desired experience & expertise
BSC Tier 1	<ul style="list-style-type: none"> Complaint and enquiry handling by phone Use of knowledge articles to identify solutions Provide timely responses to client queries Identification of issues and red flags 	<ul style="list-style-type: none"> Customer query handling 	<ul style="list-style-type: none"> Knowledge of POL products and systems
BSC Tier 2	<ul style="list-style-type: none"> Case investigation for less complex cases Identification and escalation of complex cases 	<ul style="list-style-type: none"> Investigation expertise Case triage 	<ul style="list-style-type: none"> Ability to assess risk and conduct triage Use of common data analysis steps Knowledge of POL products and systems
CIRT	<ul style="list-style-type: none"> Case investigation for medium complexity cases Identifying and liaising with key stakeholders (internal and external) 	<ul style="list-style-type: none"> Investigation expertise 	<ul style="list-style-type: none"> Significant experience of POL systems / processes Extensive knowledge of POL products and systems Experience of conducting investigations within POL Some experience of enhanced use of POL data
Horizon / GLO Investigators	<ul style="list-style-type: none"> Case investigation for high complexity cases Dispute resolution for contentious cases Sharing of investigations industry practice Investigations assurance and review Identification of investigations process improvements Identifying and liaising with key stakeholders (internal and external) 	<ul style="list-style-type: none"> Forensic accounting Investigation expertise Investigation process design Investigation assurance Change management 	<ul style="list-style-type: none"> Senior investigators with experience and training in a variety of corporate settings Use of a variety of IT and finance systems Ability to lead complex, high risk investigations Data analysis skills and techniques Understanding of legal processes and evidence Handling of sensitive or confidential information



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

35

Document Classification: KPMG Confidential



Roles and responsibilities

Describes the investigations function roles and responsibilities needed to execute the services, processes and capabilities. Details are found in Appendix 3.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

Investigation roles

The Investigations Support Team's work will involve assisting investigations teams in two key areas

Investigations Support (60%)

- The team will provide SME support to investigations teams, focusing on the use of data driven evidence, processes and technologies.
- This includes leading the most complex, sensitive or high profile investigations, and providing advice and support to investigators during their investigations.
- The team's key specialism will lie in identifying where additional data analysis can be used to resolve cases, or where new data sources or techniques can add value to an investigation.
- The team will take responsibility for investigation cases from assignment to the team to resolution or handover to the Review Committee

Driving Change (40%)

- The team will have responsibility for driving change to Horizon and investigations processes, with a particular focus on how greater or more effective use of data can improve effectiveness, efficiency and outcomes of Horizon based investigations.
- They will work with investigation teams to understand what further data requirements they may have, where data insight can add value to their investigations, and liaise with the relevant stakeholders to ensure these requirements can be met. This may include internal work to make better use of the data or systems already in place or working with external stakeholders to obtain high quality or more user-friendly data.
- This will include establishing the Lessons Learned process, which would allow industry practice data driven investigations techniques to both be shared with investigators, as well as adopted into the processes that drive investigations.
- They will lead change activities relating to investigations and the systems used in investigations, which would include liaising with internal and external stakeholders to make these changes happen
- They will keep abreast of the latest technology and investigation fraud techniques and disseminate that knowledge across investigation teams



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm. KPMG International and its member firms are not liable for the actions or omissions of any member firm. All rights reserved.

Document Classification: KPMG Confidential



DRAFT FOR DISCUSSION PURPOSES ONLY

Key investigation team roles

The key investigation roles proposed are as follows. Details are provided in Appendix 3.

Role	High level description	What issues does this address?
Head of Security, Risk & Investigations	<ul style="list-style-type: none">Leads the team, reporting into GLO/Horizon IT Director with dotted line reporting into Operations. Represents the team when dealing with high profile investigations, including providing evidence in court.Provides oversight of the team's work and provides challenge and feedback to the wider investigations teams (including defining and monitoring key KPIs for investigation teams).Raises awareness of the importance of data driven investigations internally.	<ul style="list-style-type: none">Clear reporting lines to board level / leadershipMore centralised monitoring of key KPIs for investigation teams.Limited practice of data driven investigations internally.
Branch Accounting Investigator	<ul style="list-style-type: none">Provide accounting expertise to investigations, both in leading certain key investigations and supporting complex ongoing investigations, including providing evidence in court.Identify and recommend improvements to accounting and financial data and its use in investigations.Identify root causes for common discrepancies, and develops plans to reduce occurrences of these.Review investigations and share lessons learnt to investigative teams	<ul style="list-style-type: none">There is currently limited formal accounting knowledge within a number of teams.There is limited practice of data driven investigations internally.This can reduce the occurrence of common discrepancies in branch accounts.There are no central sharing of lessons learned between investigations teams.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

38

DRAFT FOR DISCUSSION PURPOSES ONLY

Key investigation team roles (cont.)

Role	High level description	What issues does this address?
Data investigator	<ul style="list-style-type: none">Leading the most high profile data-intensive investigations, including providing evidence in court.Lead data mining activities to identify common issues and themes in investigationsLeads develop of investigations use cases for the Data PlatformLead review / quality assurance of completed investigations, ensuring processes have been followed correctly and lessons learned shared	<ul style="list-style-type: none">Greater use of data driven evidence and investigation techniquesGreater detections of patterns and trends within data and issues raised.Current data and processes are not shaped to meet the requirements of investigators.There is currently no formal centralised review of investigations work, or central sharing of lessons learned. This supports the standardisation of investigation procedures.
Data investigations Analyst	<ul style="list-style-type: none">Reviewing completed investigations, ensuring processes have been followed correctly and share lessons learned.Supports the work of the data investigator.	<ul style="list-style-type: none">There is currently no formal centralised QA of investigations work, or central sharing of lessons learned or. Supports the standardisation of investigation procedures.
Technical Data Insights Lead	<ul style="list-style-type: none">Design and develop data tools and platforms for use within the business with initial focus on investigationsThis person will work closely with investigations support team but will sit within Horizon & GLO IT Architecture team	<ul style="list-style-type: none">At present, some parts of the process are siloed with no central coordination of a number of tools, such as FREDD-O or the BiT tool.This role will allow central coordination to make better use of the tools and data in place, and identify additional requirements from across the business.Through the work of this person, current tools can be made "fit for purpose".This can increase the adoption of data driven insight across investigations cases.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential



Interfaces

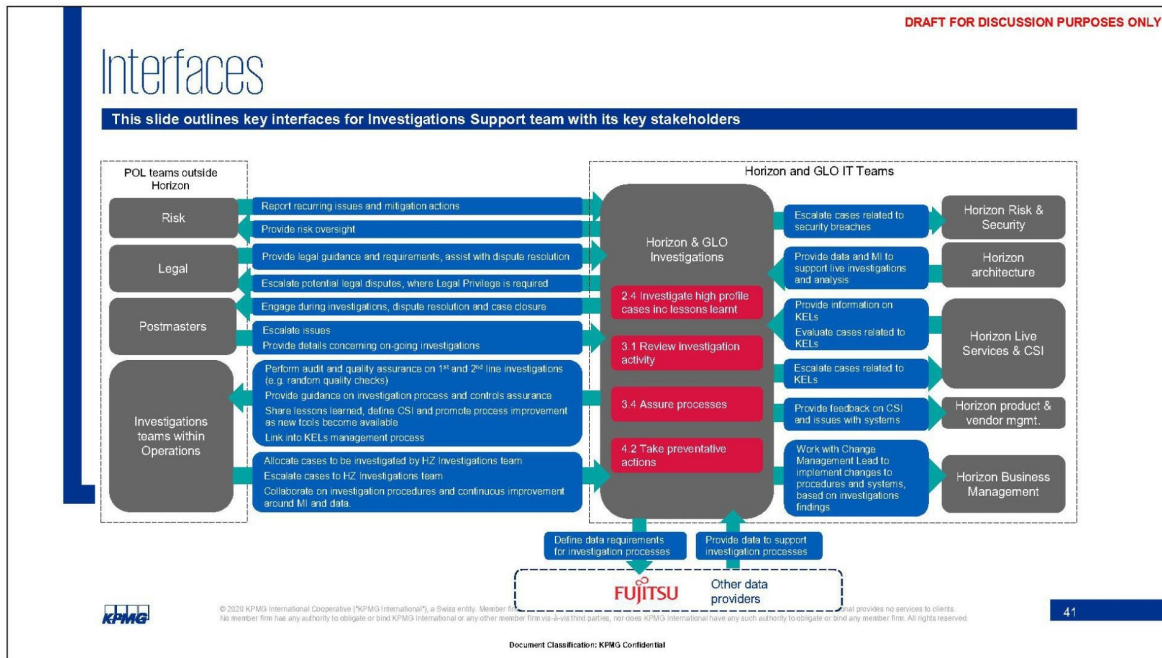
Details proposed interfaces for the investigations function with internal and external stakeholders.

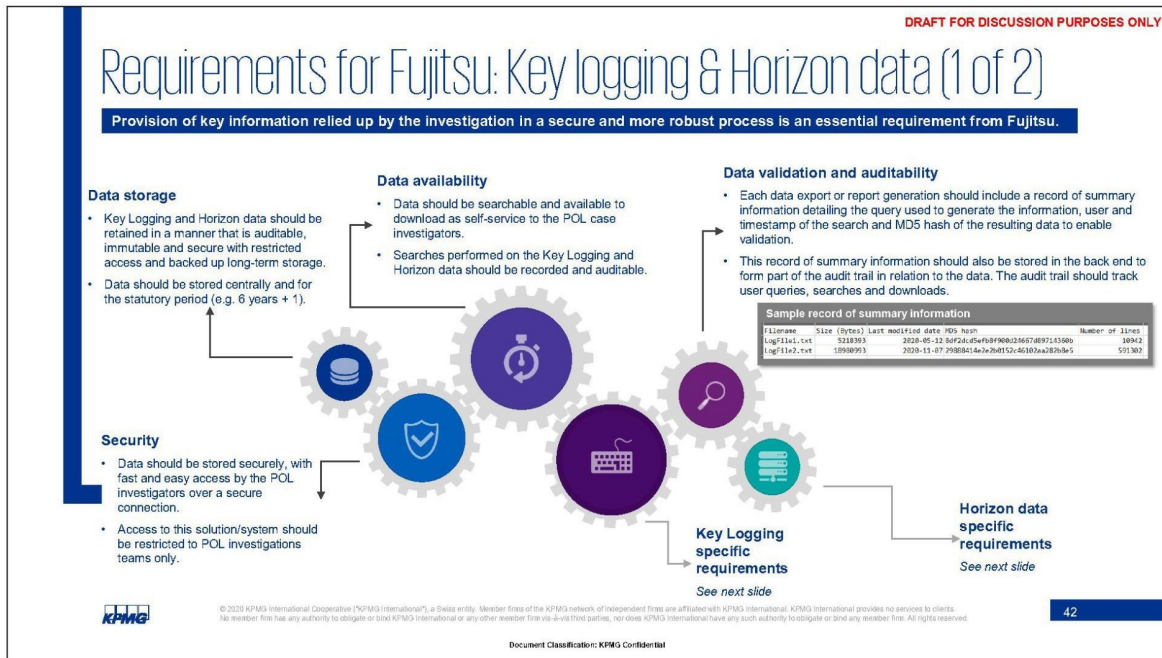


© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

40

Document Classification: KPMG Confidential





DRAFT FOR DISCUSSION PURPOSES ONLY

Requirements for Fujitsu: Key logging & Horizon data (cont.)

This slide outlines specific requirements for Fujitsu in regards to Key Logging and other Horizon data.

Key Logging requirements

- The Key Logging function should include all available auditable data including keystrokes typed by Postmasters in accordance with GDPR regulations.
- Key Logging information should be documented in a central knowledge base that is easily accessible to POL investigators. The knowledge base documentation should include message code information and GUI examples to provide investigations with additional context of user journey (see sample* below).
- Data should be readily available and accessible to support POL's investigation capability within 24 hours.
- Key Logging data should be searchable via GUI conditions or queries, e.g.

```
(session-id:"191000" OR date:[20201025 1100 TO  
20201025 1105]) AND message-code:"MSG10600"
```

*Sample knowledge base entry

MSG10601 is an alert message that indicates that a card has been inserted.
See GUI example:

Card Inserted MSG10601
Wait.
Press Cancel to cancel the transaction.

Horizon data requirements

Short term

- Horizon database to maintain integrity of data records to show creation of the records and maintain full audit of any subsequent changes. And for the information to be available to POL investigation teams.
- Greater integration of new products into Horizon database. For example, Camelot interaction with Horizon is very limited.
- Reports should be designed and tailored with investigation teams in mind.
- Horizon CBA usability for Postmasters and counter users should be improved, including greater ability to review recent transactions so that Postmasters can resolve issues quicker and more efficiently.
- Ensure that POL access to Horizon data is contractually agreed/guaranteed.

Long term

- Integration of Horizon data and Post Office data platform allowing for almost real-time data exchange including data validation and secure transfer – feed into data platform.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

43

LG

Technology and Data

Summarises technology needed and required changes for processes for obtaining data for the investigations function. Details are found in Appendices 5 and 6.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

Technology and data requirements

Changes to technology and processes for obtaining data are required to address findings from the current assessment of the investigation processes

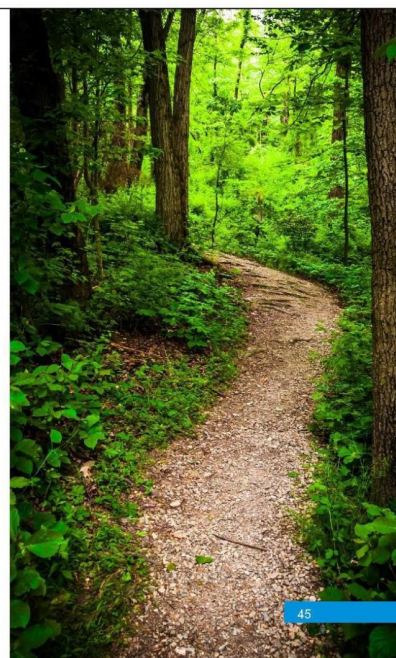
We have developed further level of detail on the following areas of recommendations, with these being captured in Appendices 5 and 6:

- **Introduction of data platform**
 - Benefits that data platform bring with data consolidation and business logic to drive the data insight
 - Requirements for data imports, security, visualisation, processing and reporting
 - Examples of investigation use cases for data platform
- **Process for obtaining data in the near future**
 - Recommendation for immediate changes for requesting, receiving and storing data from Fujitsu
- **Changes to ARQ process**
 - The proposed immediate and medium term changes aiming to streamline and enhance the data request and transfer ARQ processes with Fujitsu for obtaining Key Logging and Horizon data.
- **Data Sources Catalogue**
 - The Data Sources Catalogue lists the data sources and reports used by investigations team within POL. The catalogue captures the use case for each sources and can be used as a reference guide for investigators to identify reports which may be valuable to their investigations.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm. All rights reserved.

Document Classification: KPMG Confidential





L05

Moving forward

An indicative implementation roadmap to affect the change blueprinted in this TOM.

 © 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent member firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

46

Moving forward

An indicative implementation roadmap has been created capturing recommendations from the current state assessment

The current state assessment outlines a number of recommendations.

We have combined recommendations into initiatives which we have mapped into an indicative roadmap.

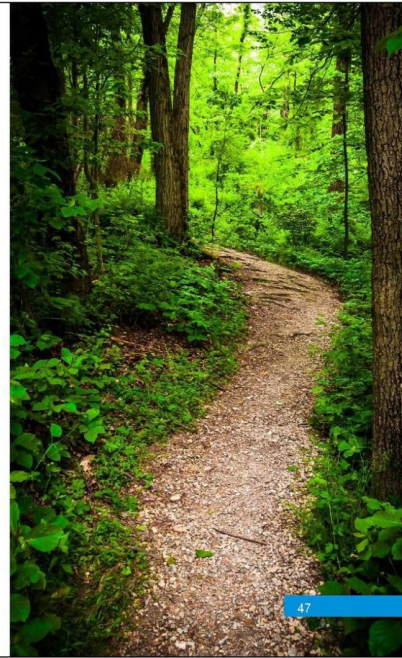
The following slides describe a proposed implementation roadmap and high level scope of initiatives.

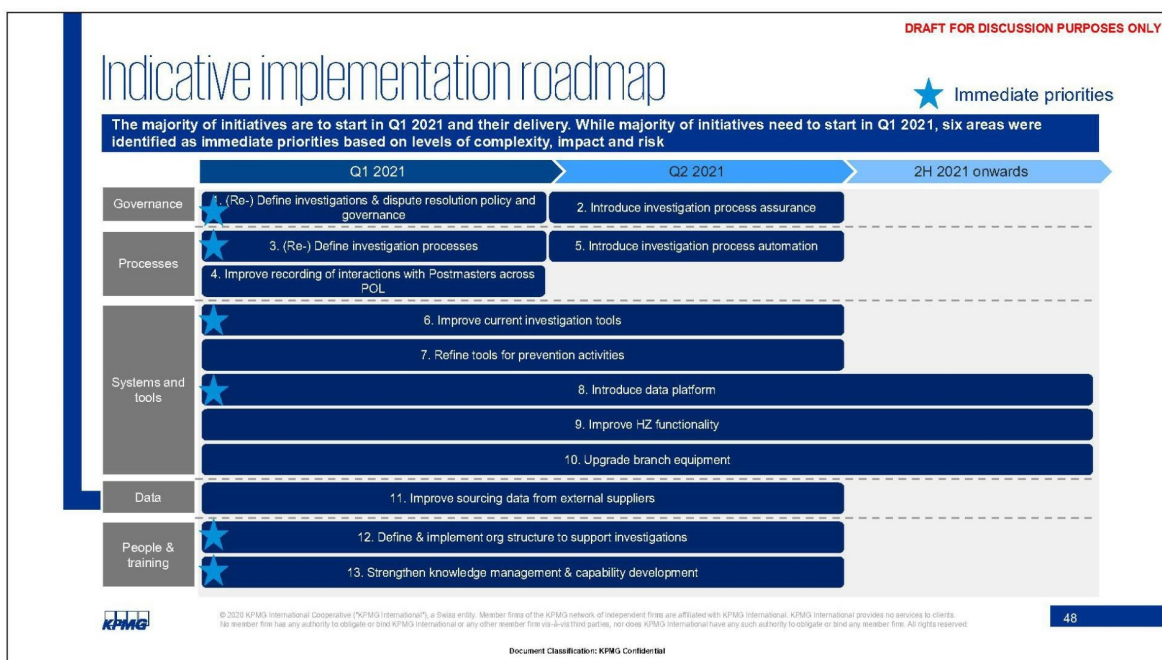
Given the criticality of findings, it is recommended to start implementation of the majority of the initiatives as soon as possible.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm. KPMG International and its member firms are not liable for the actions or omissions of any member firm. All rights reserved.

Document Classification: KPMG Confidential





DRAFT FOR DISCUSSION PURPOSES ONLY

Scope of initiatives

The following two slides outline high level scope of each initiative and their dependencies

Work package	Scope	Dependencies
1. (Re-) Define investigations & dispute resolution policy and governance	<ul style="list-style-type: none">Develop and implement policy framework for investigating and resolving disputes with Postmasters in regards to transactional issues within HorizonIntroduce a Review Committee for disputed cases which are high risk or high profile. This would consist of GLO leadership, Legal and other key stakeholders and make a business decision on how to proceed.For high-profile cases or disputes, consider the use of an independent third party investigation or review team, or an organisation trusted by Postmasters, such as the National Federation of Subpostmasters (NFSP)Define and implement performance management framework for managing investigations and dispute resolution	<ul style="list-style-type: none">KPI availabilityBuy in from POL GE
2. Introduce investigation process assurance	<ul style="list-style-type: none">Introduce assurance framework for investigation processes including setting policies and standards, quality control and continuous feedback loop into policies and standards	<ul style="list-style-type: none">#1 and #3 completionBuy-in from investigation teams
3. (Re-) Define investigation processes	<ul style="list-style-type: none">Design streamlined investigation processes for investigating Horizon transactional issues in line with industry practices including<ul style="list-style-type: none">Document existing investigation methodologies, including review and redesign of existing checklists, where requiredIntroduce triage steps with clearly defined methodology, setting criteria for assignment and escalation of investigationsIntegrate the Key Logging information into existing investigative stepsIntroduce greater use of data validation processesMandate the recording of all case data and evidence to case management systemIntroduce post-incident activity ('lessons learned'), documented and shared, as a step of every investigation.Improve leverage product specialists for investigation activitiesIntroduce de minimis criteria at case triage stage	<ul style="list-style-type: none">Union negotiationsBuy-in from investigation teams
4. Improve recording of interactions with Postmasters across POL	<ul style="list-style-type: none">Mandate use of telephony systems across Postmaster facing teams to build evidence of interactions in case of issues in the future	<ul style="list-style-type: none">Buy in from wider POL
5. Introduce investigation process automation	<ul style="list-style-type: none">Drive use of workflow tools within the case management systems to improve adherence to investigation processes	<ul style="list-style-type: none">#3 completion



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent member firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

49

DRAFT FOR DISCUSSION PURPOSES ONLY

Scope of initiatives (cont.)

Work package	Scope	Dependencies
6. Improve current investigation tools	<ul style="list-style-type: none">Introduce centralised issues log having a streamlined process for tracking issues to enable proactive approach to issuesIntroduce access security controls to the case management system (Dynamics), with auditability, access control and monitoring built inIf this is not feasible, considering introducing a different case management system which allows for more granular control	<ul style="list-style-type: none">Buy in from wider POL
7. Refine tools for prevention activities	<ul style="list-style-type: none">Improve functionality and widen usage of existing tools (e.g. FREDDO-O) to produce dedicated reports for the investigation purposes in the short term	<ul style="list-style-type: none">Buy in from wider POL
8. Introduce data lake and data platform	<ul style="list-style-type: none">Introduce predictive or proactive tools based on data lake to identify high risk transaction or branches e.g. consolidated reporting on Helpdesk queries (covering IT and Business support) including Data Analytics designed to identify the issues/trends at scale	<ul style="list-style-type: none">CAPEX availability
9. Improve HZ functionality	<ul style="list-style-type: none">Introduce of the Horizon System Product Owner Role to improve understanding of Postmasters' needs and ensure prioritisation of initiatives for the benefit of this primary user groupIdentify Horizon user pain points and improve Horizon functionalityIntroduce security monitoring to allow for identification of critical infrastructure failure	<ul style="list-style-type: none">CAPEX availability
10. Upgrade branch equipment	<ul style="list-style-type: none">Consider implementation of CCTV, intelligent/smart tills or cash counting machines to reduce volume of cash-related issues	<ul style="list-style-type: none">Buy-in from POL GECAPEX availability
11. Improve sourcing data from external suppliers	<ul style="list-style-type: none">Introduce centralised coordination of requests to external data suppliersEstablish clear processes and SLAs for the data exchange (including key logging information) with data suppliersRequest an expansion of the scope of Key Logging data and data retention period from Fujitsu	<ul style="list-style-type: none">Contractual agreements with suppliers
12. Define & implement org structure to support investigations	<ul style="list-style-type: none">Introduce a centralised investigations function, with clear reporting lines to board level, as well as Horizon investigation Support Team as a third line support	<ul style="list-style-type: none">Union negotiationsBuy-in from investigation teams
13. Strengthen knowledge management & capability development	<ul style="list-style-type: none">Conduct capability assessment in investigation teams to identify any potential capability gapsIntroduce formalised knowledge sharing opportunities between teams at different investigation tiersIntroduce investigation team training and development initiatives	<ul style="list-style-type: none">Buy-in from investigation teams



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

50

Document Classification: KPMG Confidential



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm via a third party, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

51

LA1

Detailed design – processes



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

A1: Introduction

Our review has identified a lack of documentation of processes and methodologies to be used by investigations team within POL.

Over the following slides, we have set out proposed target states for investigations processes.

L1 investigation process – current state

- Maps out the existing processes and interactions between investigations teams from across POL

L0 investigation process – target state (short term)

- Describes the high level target state for investigations in the short term, highlighting the introduction of case triage steps, the introduction of a Horizon / GLO investigations team, and new defined processes for data collection, storage and validation.

L0 investigation process – target state (long term)

- Describes the high level target state for investigations in the long term, following the introduction of the Data Platform functionality, and the inclusion of data consolidation and processing processes.

L1 investigation process – target state

- Sets out the target state for the core investigations function, including how case triage fits into this process.

L2 investigation process – target state

- Provides target state process for investigating a case for the Horizon / GLO investigations team.

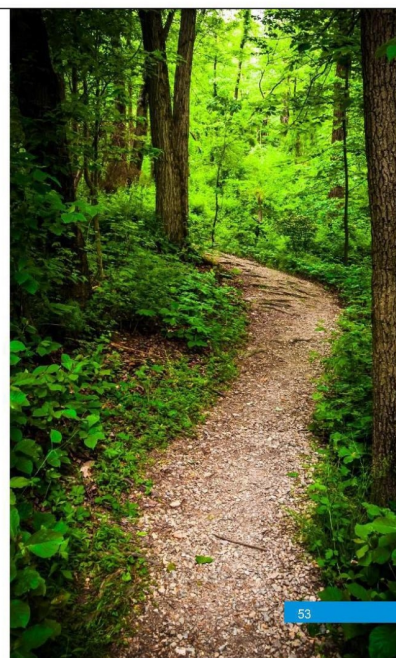
Secure data collection, storage and validation – near future

- Demonstrates the target state for requesting, receiving and storing data from both Fujitsu and other third party data providers – before the Data Platform is implemented.



© 2020 KPMG International Cooperative (“KPMG International”), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties. Nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

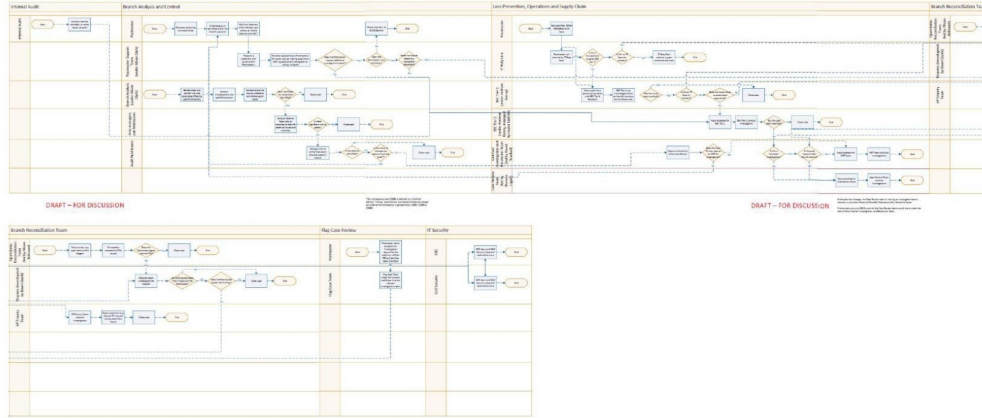
Document Classification: KPMG Confidential



DRAFT FOR DISCUSSION PURPOSES ONLY

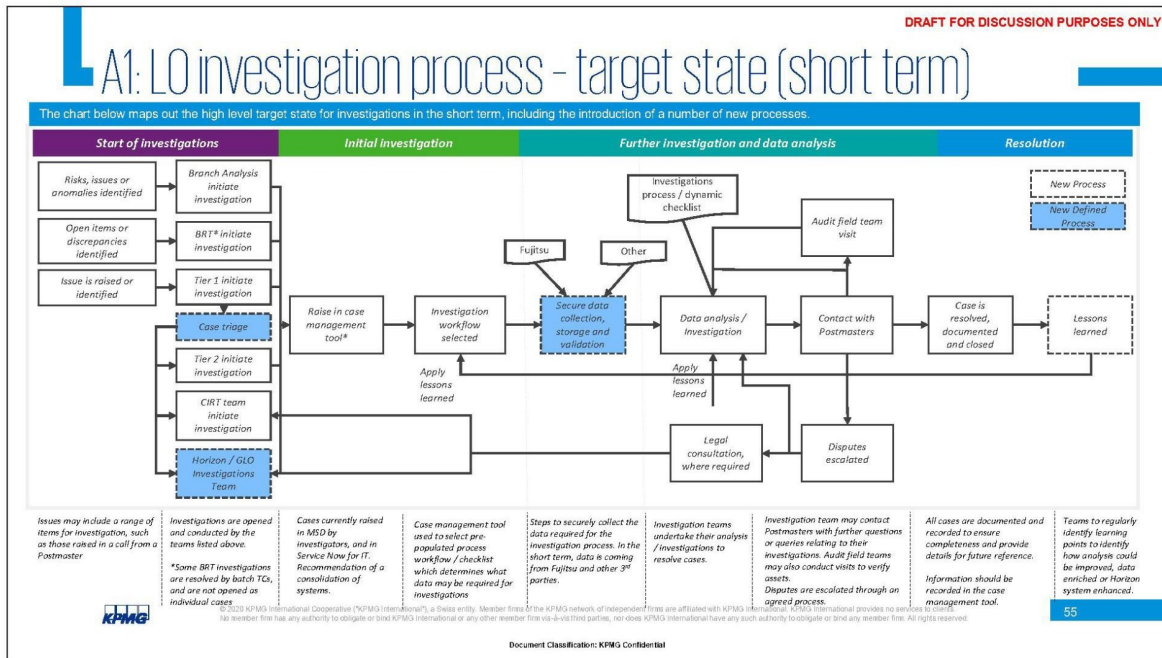
A1: L1 investigation process - current state

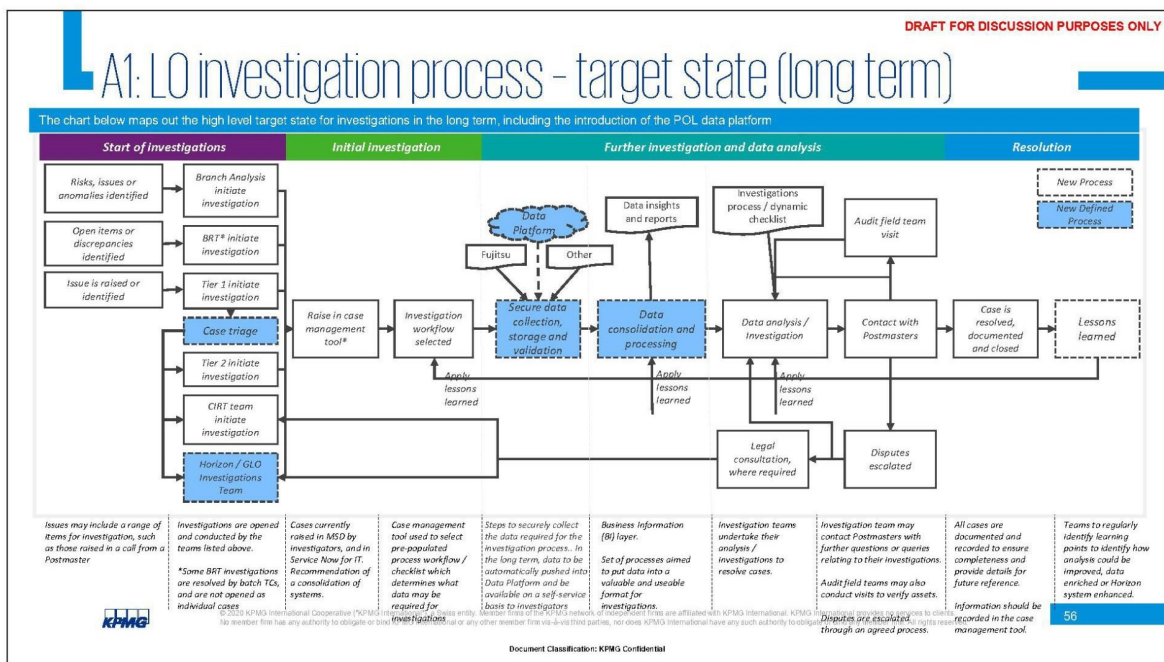
Current POL investigation processes at Level 1 and interactions between investigations teams from across POL have been mapped. The screenshot of the accompanying Visio document is below.

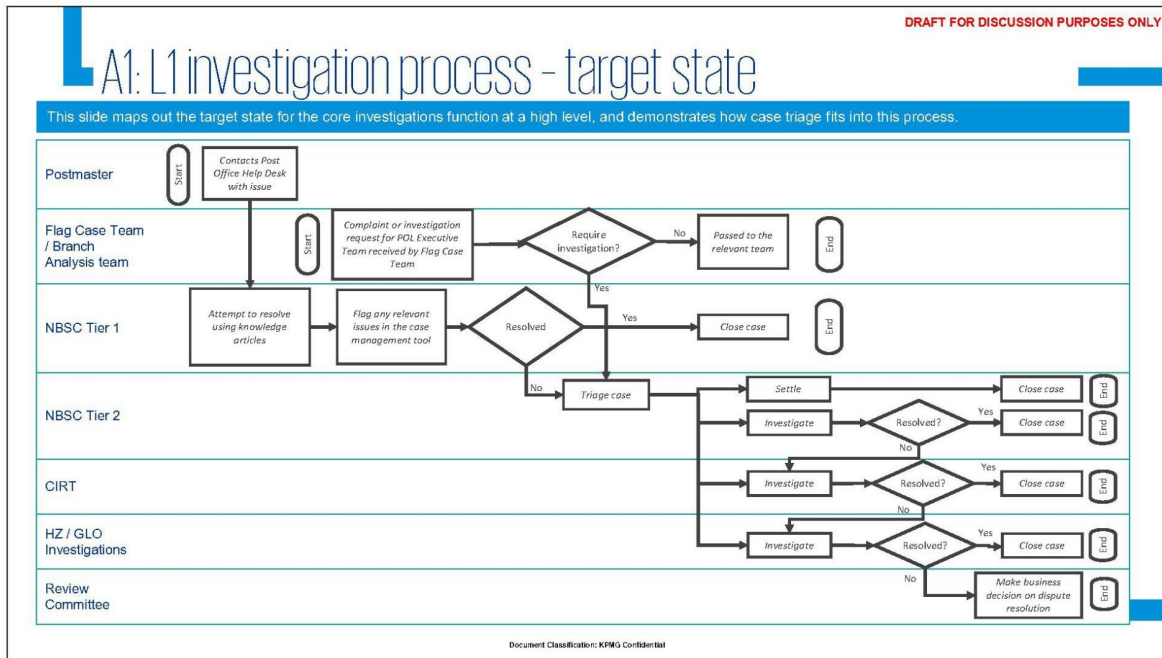


© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent member firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential



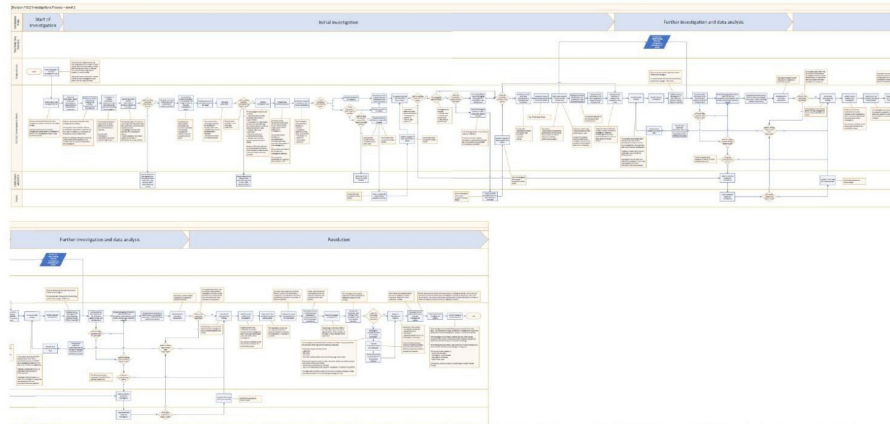




DRAFT FOR DISCUSSION PURPOSES ONLY

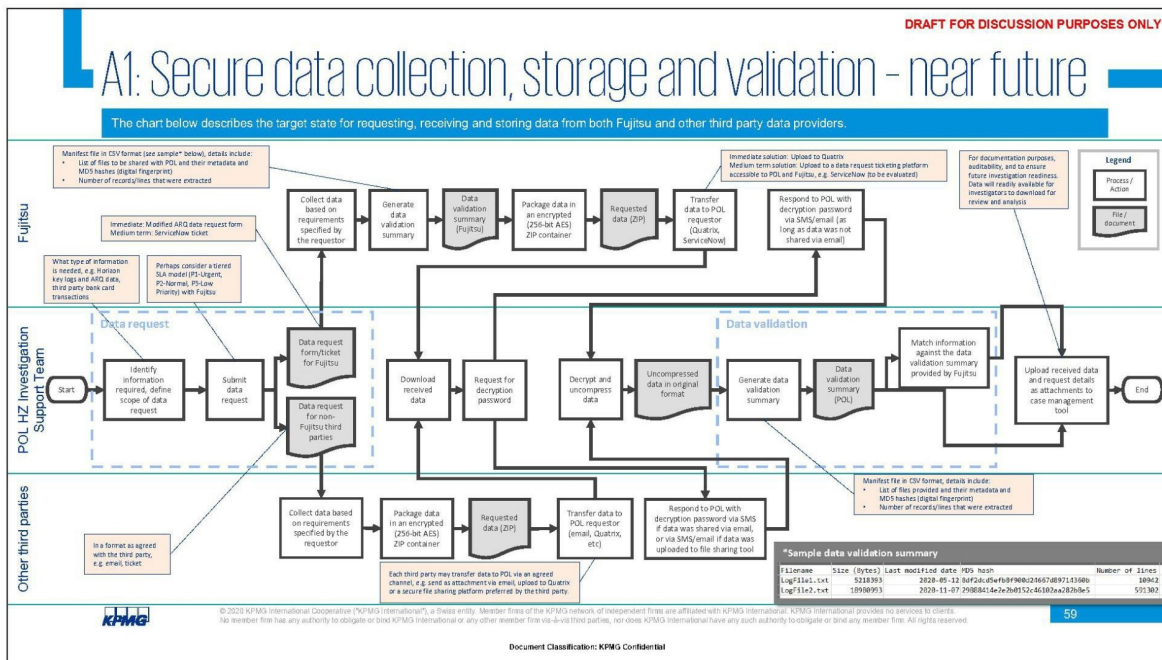
A1: L2 investigation process - target state

The target state L2 process for the Horizon Investigation Support Team has been mapped. The screenshot of the accompanying Visio document is below.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent member firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential



LA2

Detailed design – case triage



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

A2: Introduction

At present, POL do not have a documented process to identify the most high-risk or business critical investigations, and prioritise or escalate these cases.

We have set out a triage process over the following slides, where cases are reviewed and assigned to the different tiers of investigations teams within POL, based on their risk and priority to the business.

Case triage

- Explains at what stage case triage should take place, what it would involve, who would be involved, what criteria would be used to assess cases, and when cases would be escalated to the Horizon Investigation Support Team.

Case triage process

- Illustrates how the case triage steps fit into the wider Investigations process, showing the sources for cases, and the Investigations teams that cases could be assigned to.

Case triage criteria

- Sets out criteria which may lead to cases being immediately escalated beyond BSC Tier 2, for priority investigation by either the Contract Investigation and Resolution Team (CIRT), or by Horizon Investigation Support Team.

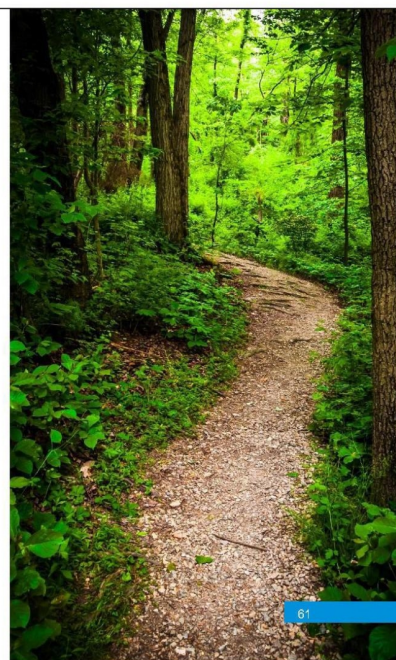
De minimis – current application and suggested changes

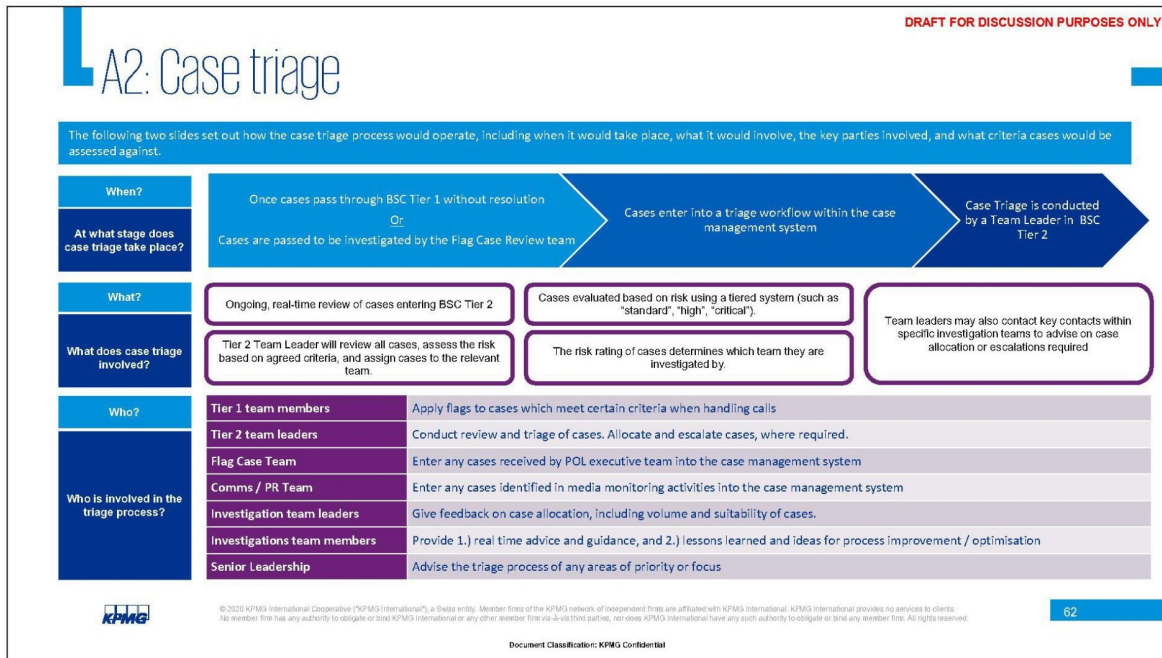
- Describes the current limited use of de minimis criteria within investigations in POL, and recommends changes which could be made to address this, as part of the case triage process.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm. KPMG International and its member firms are not liable for the actions or omissions of any member firm. All rights reserved.

Document Classification: KPMG Confidential






DRAFT FOR DISCUSSION PURPOSES ONLY

A2: Case triage (cont.)

How?	Assessment criteria may include:
What criteria are cases assessed against?	Media Coverage
	High monetary value
What?	Root causes suspected to be a Horizon system issue
	Recurring unresolved issues from the same Postmaster
When do the Horizon Investigation Support Team on investigations?	High profile themes (both long term or at a given point in time)
	Unresolved recurring issues
What?	The mandate of the team is to take on:
When do the Horizon Investigation Support Team on investigations?	The most high profile, high risk or complex cases
	With a particular focus on investigations requiring extensive or enhanced analysis of data.
When do the Horizon Investigation Support Team on investigations?	Cases which POL may consider escalating to the Horizon / GLO team include:
	Those with contentious media coverage, particularly in national or trade press
When do the Horizon Investigation Support Team on investigations?	Those which may place the integrity of any aspect of Horizon into doubt
	Those which include issues previously raised in the Horizon issues judgement

We have provided examples in the following slides of levels of risk within cases which would indicate that a case should be escalated to either the CIRT team, or to the HZ / GLO investigations Team.

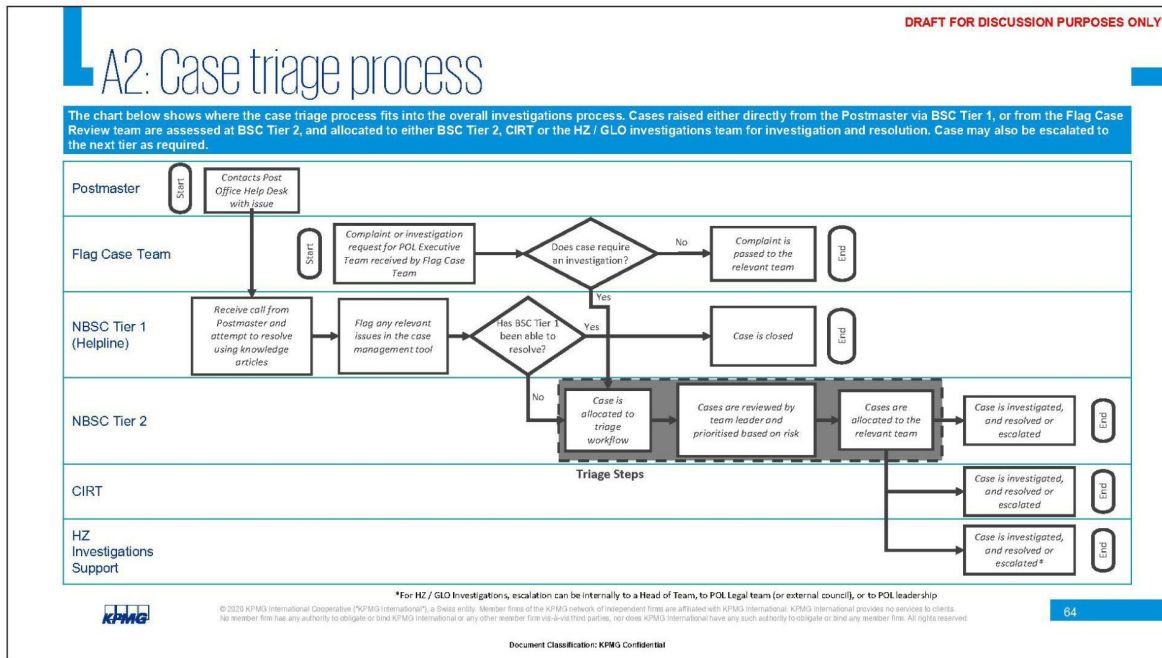
However, it is worth noting that criteria should not be viewed as binary indicators of escalation needs, and cases should be viewed across a range of factors, based on ongoing POL priorities. These priorities will be issues identified by POL as being high profile, high risk or of strategic importance to the business at a given point in time.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

63

Document Classification: KPMG Confidential



DRAFT FOR DISCUSSION PURPOSES ONLY

A2: Case triage criteria

Higher risk cases will be escalated to either CIRT (Contract Investigation and Resolution Team), or the Horizon Investigation Support Team. Criteria that determine which team these cases should be escalated to are shown below.

Criteria	CIRT		HZ / GLO Investigation Team	
Media coverage	Media coverage localised or low profile	Low risk of impact on POL reputation	National media attention (including trade press)	Likely to impact on POL reputation
Monetary value	Moderate financial risk to POL or Postmaster		High financial risk to POL or Postmaster	
Root cause suspected to be a Horizon system issue	Case would be escalated direct to HZ / GLO		Horizon systems issues are always escalated	May also require attention of other teams / leadership
Recurring unresolved issues from the same Postmaster	Issue has reoccurred with the same Postmaster	Root cause or potential fix not yet identified	Issue has reoccurred multiple times with the same Postmaster	Causing significant disruption or distress to Postmaster
			Root cause or potential fix not yet identified	Likely to impact on POL reputation
High profile themes*	Case would be escalated direct to HZ / GLO		High profile themes are always escalated	
Unresolved recurring issues	Issue has reoccurred on multiple occasions	Issue affects multiple Postmasters	Issue has reoccurred on multiple occasions	Risk of significant loss to POL or Postmasters
	Root cause or potential fix not yet identified		Root cause or potential fix not yet identified	Causing significant disruption or distress to Postmasters
			Issue affects a large number of Postmasters	Likely to impact on POL reputation

* E.g. IT / Horizon related, reference data or system comms failures

KPMG

KPMG is a global network of member firms, each of which is a separate legal entity. Member firms of the KPMG network are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm via a third party, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

65

DRAFT FOR DISCUSSION PURPOSES ONLY

A2: De minimis – current application and suggested changes

At present, POL do not apply de minimis levels to determine whether investigations will be pursued. This means that investigations are pursued, even where the financial value in question is less than the cost of the investigation. Applying a de minimis level, below which POL would not investigate, would help to reduce workload and cost and allow greater focus on priority cases. However, POL must also consider any additional risks associated with a case.

Current application

Currently POL does not have de minimis policies or guidelines to determine whether an investigation is pursued.

While the Branch Reconciliation Team has product-based "low value tolerances" in place to determine if a discrepancy may be automatically written off, these tolerances were not intended to be used in the context of investigations. In addition, these tolerances only consider monetary values, rather than the associated risk.

A list of the "low value tolerances" has been included as part of this pack.

Suggested changes

Overview


- To determine whether a discrepancy should be investigated or written off, besides the monetary value in dispute, POL should also consider the risks and implications involved when opting not to conduct a thorough investigation. This would form a simple version of a cost-benefit analysis.
- This assessment will be carried out at the Case Triage stage by the Tier 2 Team Leader. The assessment should be designed to be straightforward to ensure consistent outcomes.

Monetary value considerations

- Is the disputed amount above the de minimis threshold for the product? If the disputed amount is below the threshold, have there been recurring issues with the same branch or Postmaster, (e.g. multiple cases of the same nature over the past 3 months)?
- How does the disputed amount compare to the costs required to investigate (e.g. work-hours for Tier 2, BRT and CIR)?
- Is the cumulative write-off for the branch or linked branches unusually high compared to the national average (e.g. over the past 24 months)?

Risk considerations

- Is the discrepancy likely the result of systematic issue with Horizon?
- Is this a widespread/recurring issue, for which POL would benefit from identifying the root cause to prevent future occurrences?
- Is there a risk here that POL will sustain reputational damage by not investigating?
- Is there media coverage of this case?
- Will this set an unfavourable precedent that would leave POL vulnerable to exploitation in future?



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

66

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

A2: Tolerance levels applied at transaction correction stage

The following are the tolerance levels currently used by the Branch Reconciliation Team at the transaction correction stage

Product Type	Low Value Tolerance	Product	Low Value Tolerance
Camelot Online Sales		PABA Cheque Control	
Camelot Scratchcard Activation		Cheques to EDS	
Camelot Prize Payments		Cash in Transit	
Travellers Cheque Returns		Bureau in Transit	
Moneygram Sent/Received	IRRELEVANT	Vouchers on Hand and in Transit	IRRELEVANT
ATMs		AP Products (excluding AON)	
ATM retracts		DVLA Northern Ireland	
Personal Banking Withdrawals and Deposits		DVLA	
Santander Manual Errors			



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, or independent firms affiliated with KPMG International, KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

67

Document Classification: KPMG Confidential

LA3

Detailed design – roles and responsibilities



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

68

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

A3: Detailed descriptions of roles and responsibilities

This slide describes in detail required roles to deliver the scope of investigation services to be delivered by Horizon & GLO IT function

Role & band	Responsibilities
Head of Horizon Security & Risk (4)	<p>Reporting and Oversight</p> <ul style="list-style-type: none">• Provide oversight of the team's work, included identifying key KPIs and metrics to track investigation outcomes and efficiency.• Provide direct reporting to Simon Oldhall and POL leadership.• Work closely with investigations leadership (e.g. Tim Perkins) to raise any instances or concerns of where investigations processes have not been followed.• Acts as a point of escalation within the team. <p>Sharing of best practice and lessons learned</p> <ul style="list-style-type: none">• Shares learnings from the team at a senior level and identifies collaboration opportunities with other teams and departments. <p>Management and support of the team</p> <ul style="list-style-type: none">• Manages team priorities and budgets (such as for development or tooling) for investigations support.• Provides guidance and critical challenge for the work of other team members.• Acts as a representative for the team when dealing with serious or high-profile investigations, including liaising with law enforcement or providing evidence in court.• Raise awareness of the importance of data driven investigations within the wider POL business.
Branch Accounting Investigator (3B)	<p>Investigations Support</p> <ul style="list-style-type: none">• Act as an accounting SME for investigation teams, both on ongoing investigations and on an ad hoc basis.• Support investigation teams (such as BRT and Disputes) with technical queries relating to branch discrepancies. <p>Sharing of accounting best practice and lessons learned</p> <ul style="list-style-type: none">• Review financial aspects of completed or ongoing investigations, and identify and share lessons learned from these.• Share best practice to resolve any ongoing issues (e.g. any issues with suspense accounts). <p>Improving and enhancing the use of data in investigations</p> <ul style="list-style-type: none">• Identify improvements to accounting and finance systems, as well as any accounting treatments or processes, which could increase the opportunities for data driven evidence in investigations.• Work with data experts to ensure the necessary tools and analysis are in place to support financial aspects of investigations.• Work with the Data Platform team to identify what data can be stored and how this can be applied to investigations.• Develop investigations use cases for the Data Platform, and ensure this supports and enhances investigations work from a financial perspective. <p>Data insights</p> <ul style="list-style-type: none">• Identify root causes for discrepancies, to reduce occurrences of these, and reduce failure demand.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

69

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

A3: Detailed descriptions of roles and responsibilities (cont.)

Role & band	Responsibilities
Data Investigator (3B)	<p>Investigations Support</p> <ul style="list-style-type: none">• Provide investigative support for data analysis and investigations in the most complex cases. <p>Sharing of data best practice and lessons learned</p> <ul style="list-style-type: none">• Sharing of data driven investigations best practice, skills and techniques to investigations teams (i.e. through workshops, knowledge sharing initiatives, etc.).• Share data driven investigations knowledge across the wider business.• Review previous or ongoing investigations to identify best practice and learnings from a data driven evidence perspective.• Promote effective use of evidential processes, including chain of custody recording and data integrity.• Conduct data mining to identify common issues and themes from investigations.• Share learnings from proactive data driven analysis within the business.• Develop investigations use cases for the Data Platform.• Review any instances of investigations found by the Investigations Team to not be following agreed processes or meeting agreed standards, and escalate to the Head of Team where appropriate. <p>Improving and enhancing the use of data in investigations</p> <ul style="list-style-type: none">• Work with investigators to identify additional data sources, processes and automation to enhance investigations.• Work with investigators to identify opportunities for further use of data driven technologies.• Liaise with external data providers to develop and secure additional data sources or tools. <p>Data insights</p> <ul style="list-style-type: none">• Work with members of Investigations team to identify what further data insights they require.• Assess and scope the possibilities for further data insights.• Work with data analysts in the business to develop additional data analysis tools and business intelligence logic.• Identify, consolidate and share the existing key BI tools within the business (such as FREDDO).



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

70

DRAFT FOR DISCUSSION PURPOSES ONLY

A3: Detailed descriptions of roles and responsibilities (cont.)

Role & band	Responsibilities
Data Investigations Analyst (2B)	<p>Investigations Support</p> <ul style="list-style-type: none">• Support the Forensic Data Investigator to provide investigative support for data analysis and investigation in the most complex cases. <p>Sharing of data best practice and lessons learned</p> <ul style="list-style-type: none">• Organising knowledge sharing sessions to share data driven investigations knowledge within the business• Work with investigation teams to ensure effective use of evidential processes, including chain of custody recording and data integrity• Conduct reviews of investigations undertaken to ensure agreed processes have been followed.• Escalate (to Data Investigator) any instances of investigations not following agreed processes or meeting agreed standards. <p>Improving and enhancing the use of data in investigations</p> <ul style="list-style-type: none">• Act as the primary point of contact for POL Investigations teams seeking to increase, alter or enhance their use of data and data tools.• Identify, consolidate and share the existing key BI tools within the business (such as FREDD-O). <p>Other</p> <ul style="list-style-type: none">• Support the Forensic Data Investigator in carrying out their responsibilities (as listed above)
Technical Data Insights Lead (3B)	<p>The initial focus of this role is on providing technical data knowledge and support to the investigations team. This would involve developing tools and reports as raised and recommended by the team, as well as giving guidance and advice on possible solutions. A candidate for this role should be able to set up logical workflows in relation to software development and communicate business requirements effectively to development teams.</p> <p>Investigations Support</p> <ul style="list-style-type: none">• Provide bespoke data analysis support for specific high profile or complex investigations• Work to integrate any bespoke analysis applied to individual investigations (as mentioned in the point above) into being applied and deployed more widely on a BAU basis <p>Improving and enhancing the use of data in investigations</p> <ul style="list-style-type: none">• Acts as technical data expert, both within the team, as well as supporting the wider business• Develop and design tools and models to meet the data need of investigation teams.• Provide advice and guidance to other team members of potential data capabilities, or alterations that could be made to existing reports or tools• Drive the identification and development of automation in manual processes that currently take place within investigation teams, including in the obtaining, validation and processing of data• Take active part in integrating the Data Platform process into streamlining the investigation workflow.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

71

Document Classification: KPMG Confidential

LA5

Detailed design – data platform technology requirements



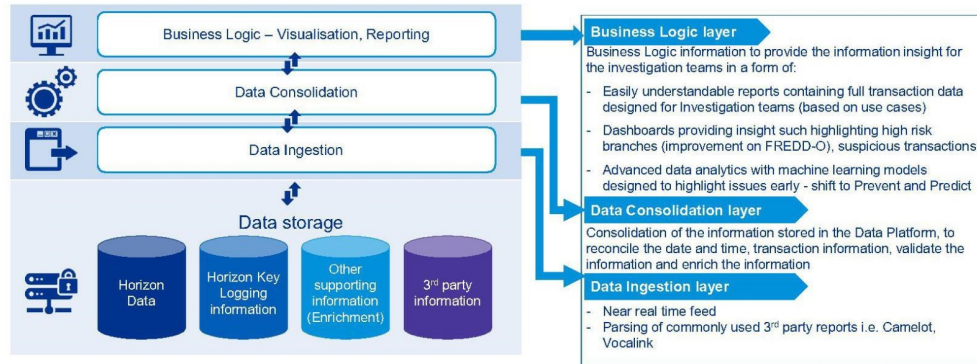
© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

A5: Data platform: benefits and potential solution design

A more robust access to the transaction information is needed in order to reduce the reliance on Fujitsu and other data providers and enable investigation teams to have access to all information near real time, enriched with additional data sources to inform the investigation teams. POL wide Data Platform project could be leveraged to serve investigation teams to reduce the costs and time related to data platform introduction.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

73

DRAFT FOR DISCUSSION PURPOSES ONLY

A5: Recommendations for data platform

Recommended requirements and considerations for the Data Platform

Data import

- Serve as the single source of truth for all transactions for case investigations.
- The Data Platform may take data feeds from sources other than Horizon, e.g. Dynamics, ServiceNow, Vocalink, Camelot, ATM data.
- Key Logging data should be stored in the Data Platform.
- There should be robust import and validation processes for pulling data from Horizon and third party sources to ensure the data integrity on the Data Platform.
- Data should be retained for the statutory period (e.g. 6 years + 1).
- As part of the setup for data import, data sources should be categorised to identify what type of information should be immutable or editable, e.g. transaction data should be immutable, whereas pricing reference data could be editable.
- Audit logging should be in place for editable data to track the creation and modification details of each transaction record, e.g. usernames and timestamps.
- The Data Platform may carry two layers of data. The first layer (e.g. Business Logic Layer) provides near real-time data to teams such as Tier 1 that require instant visibility. The second layer (e.g. Data Consolidation Layer) carries delayed (e.g. available next day) but complete and enriched data geared towards teams such as Tier 2 and investigation teams, as cases/issues would generally reach these teams hours or days after the transaction in question took place.

Data import

Security

Visualisation

Processing and reporting

Data Platform Requirements

01

02

03

04

KPMG

© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent member firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

74

DRAFT FOR DISCUSSION PURPOSES ONLY

A5: Recommendations for data platform (cont.)

Security

- Data Platform needs to be designed with security in mind, including user access and administration, data storage and redundancy.
- A secure data store (with elevated access requirements) and special handling procedures should be in place to account for sensitive data that may be received from third parties, to ensure that the Data Platform is compliant with GDPR.
- Access to Data Platform should be restricted, monitored and reviewed.

Visualisation

- Data Platform should have feeds from Dynamics and ServiceNow to pull in key case and ticket information.
- By analysing the key information from the cases and tickets (e.g. FAD code, Postmaster, issue type, monetary value), Data Platform performs automated pattern identification, generates logic-based alerts and presents the information in dashboards. This can provide investigators with visualisation for additional context and background information beyond the immediate case details.
- Quick dashboarding for Tier 1 to look up branch information when receiving the call, e.g. recent transactions, current balances, top transactions/ products, till activity.

01 Data import

02 Security

03 Visualisation

04 Processing and reporting

Data Platform Requirements

KPMG

© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

75

DRAFT FOR DISCUSSION PURPOSES ONLY

A5: Recommendations for data platform (cont.)

Processing and reporting

- Investigations teams should be able to query and run reports on data as a self-service. The age of the data should not be a limitation as long as it is within the statutory period.
- Produce reports that are tailored for investigations teams, with information and fields that are more relevant and usable than reports generated by Credence and HORice.
- Investigations teams should be able to customise reports with the help of POL in-house teams such as Technical Data Insights Lead.
- Searches run on Data Platform should be recorded (query used, username, timestamp) for auditing if required.
- As a long-term solution, apply business logic for matching transactions to alleviate investigations teams of labour intensive and repetitive processes, as well as reduce human error in manual processes.

01 Data import

02 Security

03 Visualisation

04 Processing and reporting

Data Platform Requirements

KPMG

© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

76

A5: Data platform use cases

Use case 1

Tier 1 handles initial contact with Postmaster

- Postmasters calls Tier 1 for support with transactional issues.
- Tier 1 agent obtains FAD code from the caller and queries it on Data Platform.
- Data Platform generates an overview dashboard that consolidates and translates near real-time data from Horizon, Dynamics and ServiceNow to a visual presentation of key information and statistics on the branch and caller.
- Information on the overview dashboard is structured to be well organised but high-level, so that it is digestible by the Tier 1 agent quickly on the call. This equips the agent with key information on the branch such as recent transactions, current balances, top transactions/products, till activity, as well as common types of issues raised by the branch previously, and whether the current issue has been reported by a significant number of branches in the past 24 hours.
- The aim of the overview dashboard is to assist the Tier 1 agent with early identification of issue (e.g. user error, widespread system issue), resulting in improved Postmaster experience via quicker resolution, higher resolution rate at Tier 1, and more accurate triage if escalation is required.

Use case 2

Investigations team gathers information

- A case has been escalated to the Tier 2 investigation team in relation to card payment transaction discrepancies.
- The investigations team would like to interrogate a variety of data from Horizon and third parties, such as transaction details, terminal/PIN pad Key Logging records, and Vocalink records.
- As Data Platform pulls and retains data from various sources, the investigations team is able to query Data Platform and obtain information and reports relevant to the transaction of interest.
- Data Platform also records and retains history of queries and reports exported to form part of the audit trail. This ensures that the investigation is conducted in a manner that is repeatable and defensible.
- Automated analysis and visualisation of trends/patterns by Data Platform provides investigators with details such as common types of issues by the branch or caller previously, which helps the investigators in exploring possible root causes of the issue.
- Using Data Platform as a centralised system for data query and export, information gathering will be conducted more consistently and efficiently, thus contributing to the improvement in quality of investigations.

Data Platform



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm via a third party, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

A5: Obtaining data - near future 'to-be' process

This slide outlines near future target state for requesting, receiving and storing data from Fujitsu.

Step owner	High Level Process Steps	Comments and Considerations
POL	1. Requester identifies information required – defines scope of the request	<ul style="list-style-type: none">When scoping the request, the requestor will need to identify:<ul style="list-style-type: none">What type of Horizon information is needed, such as:<ul style="list-style-type: none">Keylogs: postofficecounter.log containing: PIN Pad, CBA screen messages, printer log [TBC by Fujitsu]HORice informationARQ Data<ul style="list-style-type: none">Predefined Fields for the type of the investigation required, Credence / HORice + othersRequired Info: Branch (PAD), Date Range or Session IDCase Management tool tracking number: MS Dynamics (for investigation teams) or ServiceNow (for IT teams)Any member of investigation teams can request data (currently only BSC T2 and T3 [CIRT])
	2. Data Request submission to Fujitsu	<ul style="list-style-type: none">Requests to be submitted:<ul style="list-style-type: none">Currently a form (in Word format) is sent to a Fujitsu Mailbox for ARQ requestsService Now form to be created to help streamline the processPerhaps consider a tiered SLA model (P1-Urgent, P2-Normal, P3-Low Priority)
Fujitsu	3. Fujitsu to acknowledge the request and provide a request number	<ul style="list-style-type: none">Allows POL to reference the specific requests and to escalate any outstanding requests
	4. Fujitsu steps to retrieve the data	<ul style="list-style-type: none">For retrieval of Keylogging information, we understand the process to be:<ul style="list-style-type: none">Remote extraction of the local POC log file from the EPOS system (potentially filtering the data in the process)Provision of data to POL
	5a. Fujitsu to provide data to requester	<ul style="list-style-type: none">Data transfer to POL – format and method:<ul style="list-style-type: none">As industry practice, Service Now should be used to exchange encrypted files which would help with trackingFor smaller files, encrypted ZIP file with built in CRC checks, sent by emailFor larger files, encrypted ZIP file, uploaded to central storage or sent using Quattrin (limited to 30 days retention)Data to include raw data and the data manifest file including MDS and records count
	5b. Fujitsu to validate data	<ul style="list-style-type: none">Fujitsu data validation steps to include:<ul style="list-style-type: none">Generation of Digital Fingerprint (MDS #) for data in uncompressed state to ensure data integrityGeneration of data manifest, including a summary of the provided files:<ul style="list-style-type: none">List of files provided, and their metadata, including the generated MDSNumber of records that were extracted from Fujitsu system and included in each raw data file i.e. lines
POL	6. Requester receives data and performs validation check	<ul style="list-style-type: none">POL data validation steps to include:<ul style="list-style-type: none">Verification of Digital Fingerprint (MDS #) for data in uncompressed state to ensure data integrityVerification of data manifest files:<ul style="list-style-type: none">List of files received, and their metadata including the generated MDSNumber of records that were ingested into POL analysis tool and included in each raw data file i.e. lines
	7. Data is uploaded and attached to the case management tool	<ul style="list-style-type: none">For documentation purposes, auditability, and to ensure future investigation readiness
	8. Investigator starts to conduct analysis	

KPMG

No member firm has any authority to obligate or bind KPMG International or any other member firm via a third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

A5: Obtaining data - existing ARQ process & recommendations

At present POL follows the ARQ process to obtain Horizon data from Fujitsu. The proposed Immediate and medium term changes below aim to streamline and enhance the data request and transfer processes with Fujitsu.

Step owner	High Level Process Steps	Existing ARQ process	Proposed changes															
POL	1. Requester identifies information required – defines scope of the request		Immediate <ul style="list-style-type: none">Include key logging requirements in the existing form.In addition to ARQ data requirements, the form will specify key logging parameters (e.g. session ID and other transaction details).															
	2. Data request submission to the POL Security Team		Medium term <ul style="list-style-type: none">Requests to be submitted to Fujitsu via ServiceNow															
Fujitsu	3. Data request submission to Fujitsu	<ul style="list-style-type: none">POL Security Team submits ARQ data request forms to a Fujitsu mailbox.																
	4. Fujitsu steps to retrieve the data	<ul style="list-style-type: none">Fujitsu collects data based on the requirements specified by the requestor.ARQ data is provided in raw format in Excel spreadsheets. This includes two data files, one for transactional data, one with events information.	Immediate <ul style="list-style-type: none">Fujitsu to provide key logging data if requested in the existing form. Medium term <ul style="list-style-type: none">Raw data for key logging <i>postofficecounter.log</i> to be provided to POL per parameters requested.															
	5. Fujitsu provides data to POL Security Team	<p>Data transfer to POL - format and method:</p> <ul style="list-style-type: none">Data is posted to POL Security on an encrypted CD or, since the COVID lockdown, using Quatrix (an online secure file transfer tool).	Immediate <ul style="list-style-type: none">Stop transferring data using CDs (where appropriate), and use an online secure file transfer tool (e.g. Quatrix) appropriate for the data volume and usage as the default means of data sharing instead.Include data validation steps: each transfer should be accompanied by a manifest file in CSV format, to detail the following:<ul style="list-style-type: none">List of files provided and their metadata, including MD5 hashes of data in uncompressed state.Number of records/lines that were extracted by Fujitsu and included in the raw data filePrior to transfer, the data should be packaged in an encrypted ZIP container (256-bit AES).The encryption password should be different for each transfer and shared via a different channel, i.e. via email if files are shared over Quatrix. <table><tr><th>Filename</th><th>Size (Bytes)</th><th>Last modified date</th><th>MD5 hash</th><th>Number of lines</th></tr><tr><td>Logfile1.txt</td><td>5218393</td><td>2020-05-12 8:42:05</td><td>84f908624667289711350b</td><td>10942</td></tr><tr><td>Logfile2.txt</td><td>18909993</td><td>2020-11-07 2:08:54</td><td>4e2e2b0f52c4c102aa782d3e5</td><td>591382</td></tr></table>	Filename	Size (Bytes)	Last modified date	MD5 hash	Number of lines	Logfile1.txt	5218393	2020-05-12 8:42:05	84f908624667289711350b	10942	Logfile2.txt	18909993	2020-11-07 2:08:54	4e2e2b0f52c4c102aa782d3e5	591382
Filename	Size (Bytes)	Last modified date	MD5 hash	Number of lines														
Logfile1.txt	5218393	2020-05-12 8:42:05	84f908624667289711350b	10942														
Logfile2.txt	18909993	2020-11-07 2:08:54	4e2e2b0f52c4c102aa782d3e5	591382														
POL	6. Data received by POL Security Team																	
	7. Requester receives data and performs validation steps																	
	8. Investigator starts to conduct analysis		Medium term <ul style="list-style-type: none">Data potentially to be shared over ServiceNow (feasibility to be confirmed)															



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm via a third party, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

79

Document Classification: KPMG Confidential

A5: ARQ and key logging request form

Below is an example of how ARQ request form could be adopted to capture the Key Logging Information (MVP)

Request Form

At present, POL data requesters use the ARQ Form to request ARQ data from Fujitsu. This is sent to Fujitsu via the Post Office Security team who keeps track of the requests for billing purposes.


This form could be quickly and easily modified to include the option to request Keylogging data in addition to ARQ data, as shown in blue (in the image to the right).

The long term solution is to use a ServiceNow form to streamline the process.

Current ARQ request form

ARQ request V7.docx



		
Audit Recovery Query (ARQ)		
Requestor Name and contact details:		
Branch Name:		
ARQ ref no:	ARQP ref No (Automated Postal Order Payment)	
Witness Statement required	<input type="checkbox"/> Yes/No	
Transaction Format Requirements	A report of all transactions and events including magnetic input and output for all information for the query including remittances received. Transfers between stock units and Transaction Commodity. Information to be provided in Excel 97 format with each category in a separate column. OUTSIDE OF SCOPE TO BE MARKED "CONFIDENTIAL". Also to include all BEE calls (Call lists) Column headers as follows – CD, User ID, Stock unit, date, time, Session & transaction ID, Trade type (e.g. shares, bonds, Futures, Rem in etc, Product number, quantity, Amount etc, entry method).	
	Trading Information – Customer Session ID Transaction ID Data Source	<input type="checkbox"/> Yes/No <input type="checkbox"/> Yes/No <input type="checkbox"/> Yes/No <input type="checkbox"/> Yes/No
ARQP voucher information is required for voucher number(s)		
		<input type="checkbox"/> Yes/No
Analysis of historical helpdesk call logs (date period if different from above date range)		
		<input type="checkbox"/> Yes/No
Confirmation that there was no reported system malfunctions during the date range period.		
PAN or equivalent identifier (i.e. credit / debit card number)		
		<input type="checkbox"/> Yes/No
Barcode information required for:		
Provide given full explanation of information required:		
Others:		
Signed:		
Date:		

Key logging parameters subject to change

LA6

Detailed design – data sources catalogue



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

A6: Data sources catalogue

This slide outlines the Data Sources Catalogue that captures data sources and reports used by Investigations team within POL.

Teams included in the catalogue	Data sources included in the catalogue	
AP Enquiry Team	APOP	Global Merchant Payment
BSC Tier 2	Bardays Portal	HORice
Branch Analysis / Network Monitoring	BART	MDM
Case Review Team	BIT Tool	NaSa
Contract Investigation and Resolution Team (CIRT)	CFS	Parseq
Disputes	CFS BI	PCI PAL
Open Item Reconciliation Team	Credence	Post Office Data Exchange Server
Postmaster Account Support Team	Dynamics	Puzzel
	Dynamics Small App CACH	Stock Landing Report
	Financial SharePoint	TESQA
	FREDD-O	Traction
	Gemalto	UKPA
	Global Iris	Vocalink

The Data Sources Catalogue lists the data sources and reports used by investigations team within POL. The catalogue captures the use case for each source and can be used as a reference guide for investigators to identify reports which may be valuable to their investigations. The data in the catalogue was provided by each of the investigation teams in a catalogue template.

The catalogue can be found in an accompanying Excel file with a screenshot shown below. A list of the teams and systems captured is also shown in the table below.

The screenshot shows an Excel spreadsheet titled 'Data Sources Catalogue'. It contains a 'Master List' of data sources and reports. The table has columns for 'Data Source', 'Data Source Description', 'Data Source Type', 'Data Source Location', 'Data Source Access', 'Data Source Status', and 'Data Source Owner'. The data is organized into rows, with some rows highlighted in blue. The table lists various data sources and reports used by the investigations team within POL, including APOP, Bardays Portal, BART, BIT Tool, CFS, CFS BI, PCI PAL, Credence, Dynamics, Dynamics Small App CACH, Financial SharePoint, FREDD-O, Gemalto, Global Iris, NaSa, Parseq, Post Office Data Exchange Server, Puzzel, TESQA, Traction, UKPA, and Vocalink.



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent member firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Document Classification: KPMG Confidential

82

L A7

Document and stakeholder engagement lists



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

83

Document Classification: KPMG Confidential

A7: Document list

DRAFT FOR DISCUSSION PURPOSES ONLY

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

Title	Description	Date received
BLANK- CRT Investigation checklist v3.docx	Sample CRT investigation checklist	15 October 2020
Fujitsu Branch Checks Required 19_10_20.xlsx	List of issues that required Fujitsu branch checks	19 October 2020
Horizon analysis V0.3a (002).docx	Overview of the IT architecture of Horizon	20 October 2020
GLO Horizon IT Team v0.3	GLO organisational chart	25 October 2020
account martix.xlsx	List of products handled by BRT, sample BRT transaction correction	2 November 2020
Transaction History Lark Hill 150920 draft v0.1.docx	Lark Hill investigation report	3 November 2020
UEM-012b - POL IT Landscape v1.5 (002).docx	Overview of the IT architecture of Horizon	17 November 2020
ARQ request V7.docx	Sample ARQ data request form	19 November 2020
Messages Extract Database for POL (002) as of 24112020.xls	Reference listing for message codes used in Horizon endpoint terminals	25 November 2020
Avondale Road Timeline.docx	Avondale Road investigation report	30 November 2020
lark hill data.docx	Sample key logging documentation	2 December 2020
[Iris] De-minimis level queries	List of BRT thresholds for discrepancy write-off	7 December 2020
POL data sources catalogue v.1.xlsx	Lists of reports used by investigations teams	11 December 2020



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

84

Document Classification: KPMG Confidential

A7: Stakeholder list

DRAFT FOR DISCUSSION PURPOSES ONLY

In the course of this work we spoke to a number of stakeholders. They are listed below.

Name	Title	Nature of discussion	Date
Simon Oldnall	GLO/Horizon IT Director	Investigations TOM	Regular updates
Paul Smith	Major Incident and Problem Manager	Investigations TOM	Regular updates
Charlotte Muriel	Branch Accounting	Investigations TOM	Regular updates
Dean Bessell	Security Architect	Investigations TOM	Regular updates
Paul Kingham	Access Controls	Investigations TOM	Regular updates
Tim Perkins	Head of Service and Support	Investigations TOM	Regular updates
Graham Hemingway	Contractor	Remediation schemes overview	28 October 2020
Kevin Hutchinson	Contractor	Remediation schemes overview	28 October 2020
Alison Bolsover	Branch Reconciliation Area Lead	Branch reconciliation	29 October 2020
Colette Mcateer	Branch Reconciliation Operations Manager	Branch reconciliation	29 October 2020
Alison Clark	Branch Analysis and Control Manager	Branch analysis and loss prevention	3 November 2020
Martin Godbold	Head of IT Service for Retail	IT operations and engineering	3 November 2020
Andrew Kenny	Service Centre Manager	BSC Tier 2	5 November 2020
Louise Liptrott	Tier 2 Team Leader	BSC Tier 2	5 November 2020
Sharron Logan	Case Review Manager	Case review teams	5 November 2020
David Southhall	Contract Investigation and Resolution Manager	Case review teams	5 November 2020
Wayne Brant	Contract Management, Chief Operating Officer	Case review teams	5 November 2020
Huw Williams	Contract Investigation and Resolution Team	Case review teams, key logging, ARQ process	5 November 2020



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

85

Document Classification: KPMG Confidential

DRAFT FOR DISCUSSION PURPOSES ONLY

A7: Stakeholder list (cont.)

In the course of this work we spoke to a number of stakeholders. They are listed below.

Name	Title	Nature of discussion	Date
Steve Page	Solution Architect	Horizon IT architecture	6 November 2020
Dave King	Head Security Architect	IT security architecture	9 November 2020
Michelle Stevens	Loss Prevention Manager	Branch analysis and loss prevention	10 November 2020
Drew Mason	Network Monitoring and Support Analyst	Branch analysis and loss prevention, FREDD-O	10 November 2020
Sree Balachandran	Operational Analysis	Branch IT and monitoring with HORice	10 November 2020
Paula Jenner	Head of IT Service for Corporate	IT systems	11 November 2020
Matt Quincey	Service Manager for Accenture and Verizon	IT systems	11 November 2020
Ketul Patel	Network Delivery Director	Key logging and network analysis	12 November 2020
Ruk Shah	Group MI and Analytics Director	Data Platform	16 November 2020
Maria Opaniran	SPO, Chief Operating Officer	Data Platform	16 November 2020
Dean Whitehead	Service Center Support Manager	Dynamics and Puzzel	16 November 2020
Laura Tarling	External Communications, Corporate Affairs and Communications	Flag Case Team	17 November 2020
Tony Hogg	Head of Cyber Operations	Security operations	17 November 2020
Steven Browell	Fujitsu	Investigation requirements for Fujitsu	18 November 2020
Matthew Lenton	Fujitsu	Investigation requirements for Fujitsu	18 November 2020
Christopher Knight	Intel Team Manager	ARQ data request process	19 November 2020
Sally Rush	Business Analysis	Horizon IT architecture	23 November 2020
Min Dulai	ServiceNow System Manager	ServiceNow	26 November 2020



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

86

Document Classification: KPMG Confidential

LA8

Case for change in detail



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

87

Document Classification: KPMG Confidential

A8: Case for change – in detail

The need for change is clear. Post Office must re-establish trust with Postmasters in regards to investigations

The judgement of December 2019 found failings in POL's process for investigating stock and cash discrepancies

The engagement was established in Oct 2020 to help POL report into the public inquiry and specifically on the points concerning 'lessons learnt' and whether progress has been made to prevent failings happening again. This report summarises our findings on the processes of investigating transactional issues within Horizon and captures recommendations for improvement.

The KPMG review suggests that failings in the Horizon investigation processes still persist

- The processes for investigating stock and cash discrepancies and transaction corrections is at relatively low levels of maturity with mostly manual processes for collecting and collating data making those processes prone to manual errors and delay
- The governance around processes is weak with limited of Management Information to track performance of investigation team
- Tools used by investigation teams are not fit for purpose and data is not readily available

In the future, POL aspires to have lower volume of Horizon transaction issues requiring investigations, more robust and evidenced outcomes of investigation activities, and prompt, fair and communicative process for resolving disputes

The Horizon & GLO IT function has been set up to improve and ensure the use of data and evidence driven investigation processes in investigating transactional issues within Horizon to drive to more robust investigation outcomes for both Postmasters and POL supported by appropriate technology

To deliver the vision Horizon & GLO IT team will:

- "Fix fundamentals": Design a repeatable and auditable process for investigating transactional issues which is driven by data and ensures evidential integrity of data received from Horizon to Postmasters
- "Strengthen investigative processes": Build governance and tools to enable stronger investigative processes
- Shift to "Predict & Prevent": Introduce changes to Horizon and branch infrastructure to reduce volume of transaction corrections and implement proactive / predictive platforms to address issues sooner



© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network, of independent firms affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

88

Document Classification: KPMG Confidential



home.kpmg/socialmedia



© 2020 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

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.

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