POL00448330

DRAFT – Internal Audit Report

HNG – A: Reference Data Management

Context

The Horizon IT system (latest iteration "HNG-A") is used by Post Office Limited ("POL") to account for transactions in Post Offices across the UK. System configuration updates to the Branch counter terminals are centrally managed by POL (and by Fujitsu on behalf of POL) through 'Reference Data'. This process enables POL to make configuration updates to the Branch counter terminals used in the Post Office branches. The Reference Data is accessed by branch counter terminals to configure how the software behaves.

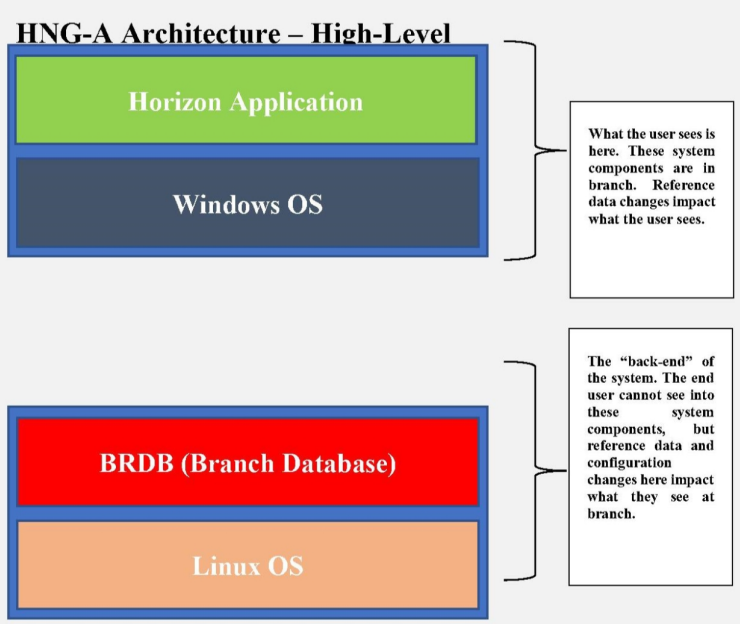
Audit Objective

Internal Audit were asked by management to complete an independent review over the Reference Data Management process for the HNG-A system. This review was an in-year addition to the agreed FY23 internal audit plan and was delivered by an Internal Audit co-source partner who worked directly with management.

Conclusion

We have sample tested POL led HNG-A control activities and concluded based on this limited testing that there are some controls operating to support the identification of some erroneous changes prior to their deployment to the production environment. However control weaknesses have been identified within the Reference Data change management process at POL over the HNG-A system that could cause some inappropriate changes to the HNG-A system's reference data to remain undetected. Further, controls operated by Fujitsu Limited ("Fujitsu") have not been assessed (refer to Pages 2 and 3 for a detailed breakdown). Due to the lack of cooperation provided by Fujitsu stakeholders during fieldwork, several intended in scope work items (specifically Scope Areas 5, 6, 7 and 9, per the table on Page 7) could not be suitably performed, **and therefore the overall audit rating is "N/A – No Rating"**.

Control weaknesses have been grouped into two key findings, with **two P2 findings** (lack of counter-level verification and supporting documents for sampled changes; improvement opportunities in Reference Data process documentation).



Audit Findings

P1	0
P2	2
P3	0

Audit Rating

N/A

No Rating

POL00448330

DRAFT - Internal Audit Report

HNG-A: Reference Data Management

PLEASE NOTE: Due to lack of cooperation provided to the fieldwork team by Fujitsu Limited ("Fujitsu") stakeholders during fieldwork, several intended scope elements could not be assured.

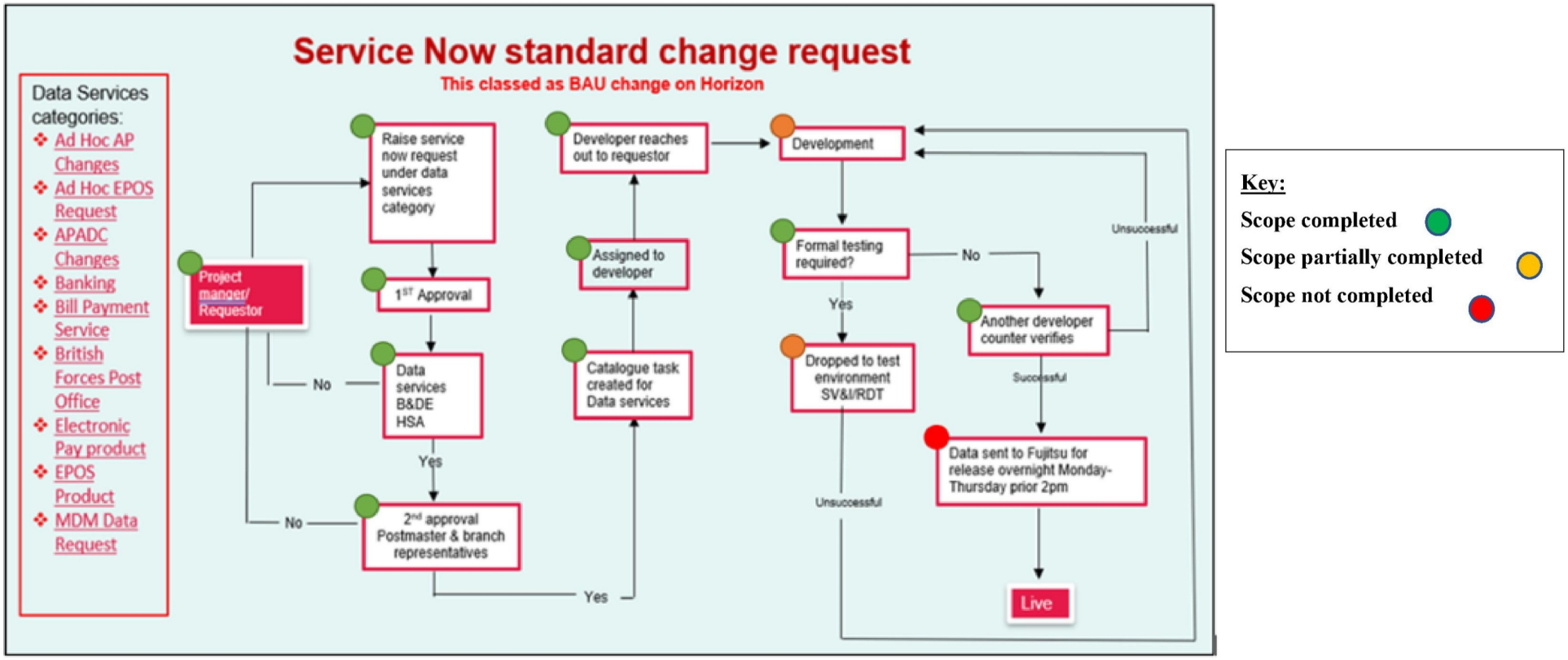


Figure 1: To aid in understanding of the scope coverage described in the table on Page 7, this diagram takes the process design for a Horizon change request at POL (per POL's internal process documentation) and maps the scope covered against each process area, given the challenges experienced with Fujitsu cooperation highlighted above.

POL00448330

DRAFT - Internal Audit Report

HNG-A: Reference Data Management

Background

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

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

Certain updates to the Reference Data tables called by local HNG-A terminals in branch are centrally managed by POL (and by Fujitsu on behalf of POL) through a 'Reference Data Management Process'. This process enables POL to make configuration updates to the branch counter terminals used in the Post Office branches. The Reference Data is accessed by branch counter terminals and is used to both configure what the user sees as well as how the software behaves.

For example, Reference Data is used to:

- Update text that is shown in messages and dialogue boxes
- Enable and disable certain features and functions, such as enable or disable the ability to sell mobile top-ups (as not all branches provide the same services)
- Update the behaviour and processing performed by the system by changing computer scripts.

Objectives & Scope

The scope of this internal audit covers the change management processes and controls in-place for Reference Data. This Reference Data change process is used to maintain the branch counter terminals software as used by the Post Office branches. The table below sets out the objectives of the overall internal audit and the coverage provided by this report.

Objective	Coverage by this report
Objective 1 – To assess and test the change management controls in place as part of the Reference Data Management Process. These controls should mitigate the risk of un-authorised or untested changes being introduced into the branch counter terminals via the Reference Data Management Process	Scope partially completed (see table overview on Page 7) – This report includes observations related to the Reference Data management process operated by POL. (Controls operated by, or reliant on, Fujitsu have not been tested at this time. See table on page 7 for an overview).

Approach

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

1. Interviews were held with POL personnel to understand POL-managed elements of the Reference Data Management Process.
2. Process documents provided by POL personnel were reviewed to assess alignment with the described process and validate the design of the POL-managed elements of the Reference Data Management Process.

POL00448330

DRAFT - Internal Audit Report
HNG-A: Reference Data Management

3. A population of 2,665 Reference Data changes was provided by POL personnel, for the seven months between 01/01/2023 and 31/07/2023.
4. A total sample of 25 Reference Data changes was randomly sampled from the population of 2,665 Reference Data changes provided by the POL reference data team for the twelve months preceding this review.
5. Evidence was provided by POL personnel, and reviewed by the IA team, to confirm compliance with the POL-managed elements of the documented Reference Data Management process.
6. Fujitsu personnel were engaged over email and teleconference to support the internal audit of the Fujitsu-managed elements of the Reference Data Management Process, but due to a lack of cooperation from Fujitsu personnel, these elements of the scope could not be assessed (refer to Pages 2 and 3 for a detailed breakdown of scope areas assured and not assured on this basis).
7. Findings were identified through the interviews and evidence reviewed, which were subsequently discussed and agreed with the Reference Data team at POL prior to inclusion in this assurance report.

Stakeholders interviewed included:

- Matthew Warren, Head Of POL Data Services
- Katimay John, Service delivery manager-Reference data

Unsuccessful attempts were made to interview Steven Browell and Daniel Walton from the Fujitsu POL Account Team

The following documents were received and reviewed as part of the assurance activity:

Horizon Ref Data Governance and Approval Process R-RDM-0004.pptx	R-RDM-0014 - AIS140 RDPAIS014 MDM To Horizon AIS.docx
R-RDM-0004 - Horizon Ref Data Governance and Approval Process.pptx	R-RDM-0017 - Service now approvers.docx
R-RDM-0006 - Deloitte audit- Dashboards.msg	ServiceNow Ref Data change approvals – Various Sampled
R-RDM-0006 - MDM Batch Report - Previous Day_59_3007020243224347.-.pdf	R-RDM-0012 - Update Data Services CAB 3010.msg

POL00448330

Executive Summary

Conclusion

It was identified through sample testing that there are controls implemented within POL to support the identification of erroneous changes prior to their deployment to the production environment. However, several weaknesses in control operation have been identified within the Reference Data change management process at POL over the HNG-X (legacy Horizon) system that could cause some erroneous or malicious changes to remain undetected.

These control weaknesses have been grouped into two key findings below, with **two Priority 2 findings**, as follows:

Lack of counter-level verification and supporting documents for sampled changes (P2): No documentation was retained by POL to show counter-level verification of the change's success for 3/25 Reference Data changes sampled requiring this level of validation, meaning that errors introduced by the change may go undetected. Additionally, no ServiceNow ticket was retained or raised to support the change request and document the process through to closure for 1/25 Reference Data changes sampled.

Improvement opportunities in Reference Data process documentation (P2): There is a lack of clear documentation defining the terms 'Standard' and 'BAU' changes, including the expected change handling, testing and recordkeeping, with a further lack of roles and responsibilities defined for those involved in the change process. This could lead changes to undergo less stringent testing than suitable or remain untested before deployment.

PLEASE NOTE: Due to a lack of Fujitsu personnel co-operation in supporting audit queries, the reported findings relate to the POL process for Reference Data change management only. Our assurance work has not in any way considered the controls operated by Fujitsu to support this process.

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

Management Comment

"TBC."

Name, Job Title

POL00448330

Detailed Findings and Agreed Actions

Finding	POL coverage	Fujitsu coverage	Finding Refs. & Priorities
Scope Objective 1 - To assess and test the change management controls in place as part of the Reference Data Management Process.			
Scope Item 1. Clearly documented understanding of accountabilities and responsibilities across the change management process and associated controls.	Tested. Findings identified.	Not tested.	2 – P2
Scope Item 2. Change requests are assessed and authorised prior to Reference Data development commencing.	Tested. Findings identified.	N/A – POL control	2 – P2
Scope Item 3. Changes are appropriately tested in a non-production environment prior to implementation.	Tested. Findings identified.	N/A – POL control	1 – P2
Scope Item 4. Changes are approved prior to being implemented in the production environment.	Tested. Findings identified.	N/A – POL control	1 – P2
Scope Item 5. Access to implement changes into the production environment is appropriately restricted.	N/A – Fujitsu control	Not tested	N/A
Scope Item 6. Development access is not granted in the production environment.	N/A – Fujitsu control	Not tested	N/A
Scope Item 7. A secure, separate development environment is in place, with access appropriately restricted.	N/A – Fujitsu control	Not tested	N/A
Scope Item 8. The deployment of approved changes into Post Office branches is monitored to validate the successful rollout of the change. Incomplete rollouts or issues caused by the rollout are identified and resolved.	Tested. Findings identified.	N/A – POL control	1 – P2
Scope Area 9. There is a clear and documented segregation of incompatible duties across the change management process, and this is effectively enforced.	N/A – Fujitsu control	Not tested	N/A

Scope Objective 1: Change Management Controls Implemented as part of Reference Data Management Process

It was identified through sample testing there are controls implemented within POL to support the identification of erroneous changes prior to their deployment to the production environment. However, several weaknesses in control operation have been identified within the Reference Data change management process at POL over the HNG-X (legacy Horizon) system that could cause erroneous or malicious changes to remain undetected.

These control weaknesses have been grouped into two key findings below, with **two Priority 2 findings**:

POL00448330

Detailed Findings and Agreed Actions

1. Lack of counter-level verification and supporting documents for sampled changes (Priority 2):

No documentation was retained by POL to demonstrate counter-level success verification for 3/25 Reference Data changes sampled. Additionally, no ServiceNow ticket was retained or raised to support the change request and document the process through to closure for 1/25 Reference Data changes sampled.

2. Improvement opportunities in Reference Data process documentation (Priority 2):

There is a lack of clear documentation defining the terms 'Standard' and 'BAU' changes, including the expected change handling, testing and recordkeeping, with a further lack of roles and responsibilities defined for those involved in the change process. This leads to potential inconsistencies in the process, whereby some changes will undergo less stringent testing than suitable for the change or are not tested, which could introduce unidentified errors and malfunction into the application.

POL have a dedicated Reference Data team that is knowledgeable about the system of internal control currently in place.

Due to a lack of Fujitsu personnel co-operation in supporting audit queries, the reported findings relate to the POL process for Reference Data change management only. Our assurance work has not in any way considered the processes operated by Fujitsu to support this process.

Below we describe the findings summarised in further detail and outline the agreed management actions that will address the findings identified.

POL00448330

1. Lack of counter-level verification and supporting documents for sampled changes (P2)

From a sample of 25 Reference Data changes, an absence of documentation in ServiceNow was noted in four instances. This included:

- For three Reference Data changes where counter verification was required, there was no documentation retained to show the developers counter-level verification of change success.
- For one Reference Data change, no ServiceNow ticket was retained or raised to support the change request and document the process through to closure.

Risk

Changes may have unintended consequences impacting transactional process that remain undetected in the absence of sufficient counter-level verification.

Agreed Management Actions (TBC)

For the four Reference Data changes without associated documentation, management should confirm the changes were appropriately reviewed and tested and there are no issues in production.

For all changes, counter-level verification should be performed and documented, to confirm the success of the change versus the intended and approved consequences.

For clean-up activities, or other activities that include a Reference Data change, a ServiceNow ticket should be raised to ensure traceability and retain evidence of the change.

Action Owner: Person, role

Date: [XX]

POL00448330

2. Improvement opportunities in Reference Data process documentation (P2)

POL currently has a high-level PowerPoint presentation that outlines the workflow of Reference Data changes, without clearly defined roles and responsibilities for POL and Fujitsu-led teams.

Further, there is a lack of clear documentation defining the terms 'Standard' and 'BAU' changes, including a lack of description of the expected change initiation, handling, testing and recordkeeping for these two categories.

This lack of clear definition leads to potential inconsistencies in the process, whereby some changes will undergo formal testing, whilst others are only counter-level verified, with some not tested in any capacity. This can cause confusion and errors in the system of change control.

Risk

Changes may not be subject to sufficiently robust testing and approval before being introduced into the production environment, resulting in system functionality bugs and errors, including those that may impact transactional processing.

Agreed Management Actions (TBC)

Create clear and comprehensive process documentation that outlines the process for handling BAU changes versus standard changes, including definitions of what constitutes and BAU vs. a standard change, to ensure that all changes are handled consistently, thoroughly and with the prerequisite level of control for their significance.

This policy should detail which teams are responsible for approvals and which teams are responsible for handling the changes and which type of changes are handled, including specific roles and responsibilities definitions (in the form of a Responsible/Accountable/Consulted/Informed, or "RACI" matrix).

All new process documentation should be reviewed and updated on a regular (at least annual) basis.

Action Owner: Person, role

Date: [XX]

POL00448330

Distribution List

	Name	Job Title
Executive Sponsor:	Simon Oldnall	IT Director
Distribution:	Simon Oldnall	IT Director
	Matthew Warren	Head of POL Data Services
	Dean Bessell	Interim CISO
Audit Team:	Carol Murray	Engagement Partner
	Helen Cutting	IT Specialist Partner
	Lewis Keating	IT Audit Director
	Matt Brennan	IT Audit Senior Manager
	Sope Folayan	IT Audit Manager
	Deloitte Co-source	
Key Dates:	ToR	October 2023
	Fieldwork	November – December 2023
	Draft Report	February 2024
	Final Report	February 2024
	RCC	
	ARC	

POL00448330

Appendix 1 – Terms of Reference

Background:

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

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

Certain updates to the branch counter terminals are centrally managed by POL (and by Fujitsu on behalf of POL) through a 'Reference Data Management Process'. This process enables POL to make configuration updates to the branch counter terminals used in the Post Office branches. The Reference Data is uploaded and stored on the branch counter terminals and is used to both configure what the user sees as well as how the software behaves. For example, Reference Data is used to:

- Update text that is shown in messages and dialogue boxes.
- Enable and disable certain features and functions, such as enable or disable the ability to sell mobile top-ups (as not all branches provide the same services).
- Update the behaviour and processing performed via updating the AP ADC scripts.
- Internal Audit were asked to complete an independent internal audit over the reference data change management process for the HNG-A system. This review was an addition to the agreed internal audit plan for FY23.

Audit Objective:

The objective of this internal audit was to test the change management controls in place as part of the Reference Data Management Process. These controls should mitigate the risk of unauthorised or untested changes being introduced into the branch counter terminals via the Reference Data Management Process.

Key Risks:

The internal audit covered the design and operation of controls in place to mitigate the risk of inappropriate Reference Data changes impacting system functionality in local Post Offices. The following risks were included in scope:

- Deployment of erroneous changes into the production HNG-A system that impact transactional processing and other functionality.
- Deployment of malicious changes with intent by development personnel.

Scope of Audit:

As part of this internal audit the end-to-end change management controls design, implementation and operation were assessed, including controls to determine the extent to which:

- Clear documented understanding of accountabilities and responsibilities across the change management process and associated controls.
- Change requests are assessed and authorised prior to Reference Data development commencing.
- Changes are appropriately tested in a non-production environment prior to implementation.
- Changes are approved prior to being implemented in the production environment.
- Access to implement changes into the production environment is appropriately restricted.
- Development access is not granted in the production environment.
- A secure, separate development environment is in place, with access appropriately restricted.
- Controls are in place to prevent introduction of security vulnerabilities in new or changed code.
- The deployment of approved changes into Post Office branches is monitored for successful deployment and introduced system function to validate the successful rollout of the change. Incomplete rollouts or issues caused by the rollout are identified and resolved.
- There is a clear and documented segregation of incompatible duties across the change management process, and this is effectively enforced.

A total sample of 25 Reference Data changes were tested for the purposes of this internal audit. This random sample of 25 was spread across the different Reference Data change types. Although not the focus of this internal audit, observations and improvement opportunities related to the Reference Data Management Process were also raised, where identified.

Timeline:

Pre-Work:	October 2023
Field Work:	November – December 2023
Draft report:	February 2024
Final report	February 2024

Audit Team:

Lewis Keating, Audit Director

Matt Brennan, Senior Audit Manager

Sope Folayan, Audit Manager

POL00448330

Appendix 1 – Terms of Reference

Deloitte Co-source support team

Reporting:

We will produce a report to management at the end of the audit and the results will be summarised for the June 2024 RCC and ARC meetings.

POL00448330

Appendix 2 – Report and findings rating guide

Report Ratings:

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

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

We will categorise our report opinion according to the below rating criteria:

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

Finding Ratings:

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

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