POL00448324

Internal Audit Report

IT Control Framework

Context

The IT Control Framework (ITCF) is a set of 227 controls, maintained in the ServiceNow GRC (Governance, Risk & Compliance) module. It provides an ongoing assessment of the operation of controls across IT and any outstanding control remediations, based on control owner self-assessment. Internal Audit previously reported on the effectiveness of the ITCF in 2018/19 and 2020/21. We also reviewed the migration of the framework to ServiceNow in 2021/22.

Audit Objective

To assess whether the ITCF provides effective reporting of the operation of IT controls and supports risk monitoring and mitigation.

Conclusion

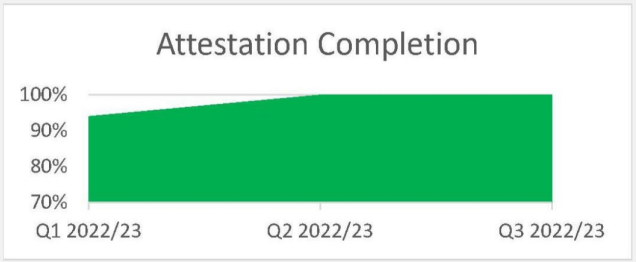
The ITCF, managed by the IT Governance & Reporting team, provides an effective mechanism to assess the operation of mostly high level IT controls. The quarterly attestation process works well and the framework has been successfully migrated to ServiceNow. The control framework has identified a significant number of control gaps and remediation plans have been defined to address these gaps.

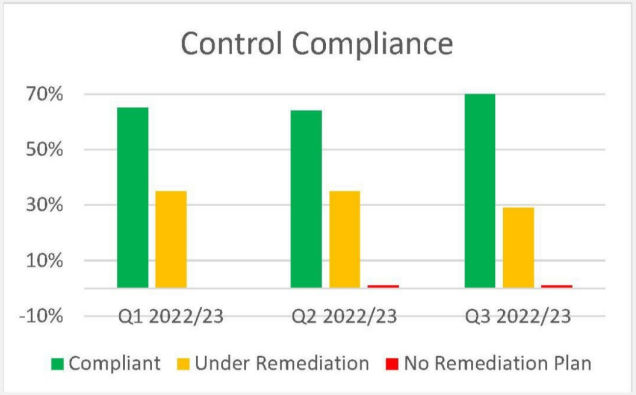
To further mature the framework, management have identified multiple initiatives that will significantly improve the coverage and focus of the framework, and support more effective assurance and decision making, including:

- Identification and mapping of controls against a wider global framework set, assignment of key controls from within this population, and full alignment with policies and standards.
- Alignment of controls against risks and realignment with Vendor Risk Management processes.

There is a need to formalise assurance around the ITCF in order to provide better oversight of control design and effectiveness, and to improve management reporting.

Progress has been made to mature the ITCF, however, additional work is required to enhance the framework and to address the significant number of control gaps identified. Therefore, we have rated this report as '***Needs Improvement***'.





Audit Findings

P1	1
P2	4
P3	0

Audit Rating

Needs Improvement

Report date: 14 March 2023

POL00448324

Executive Summary

Background

The IT Control Framework (ITCF) is a set of 227 controls, maintained in the ServiceNow GRC module. It provides an ongoing assessment of the operation of controls and any outstanding control remediations, based on control owner self-assessment.

Internal Audit previously reported on the effectiveness of the ITCF as part of the 2018/19 and 2020/21 Internal Audit plans. We also reviewed the migration to ServiceNow GRC in 2021/22.

Scope & Approach

This was a 'Limited Scope Review', focused on monitoring controls and other relevant key controls. The review covered the design and implementation of the ITCF, building on previous Internal Audit assessments. Specifically, it covered the following areas:

- ***ITCF design*** - assess the design of the ITCF to ensure risks, controls and associated control objectives are fit for purpose, incorporating industry best practices and Post Office control requirements.
- ***ITCF operation*** - assess the adequacy of the processes operated and tools used to deploy the ITCF, including sign-off by control owners and reviewers.
- ***Control effectiveness and ongoing management*** - review and assess the process for reporting on control effectiveness and identifying, tracking and escalating any remediations or control design improvements required.

We looked at key indicators, such as the completeness of control self-assessment and the number of remediations, to guide limited testing of control operation.

Conclusion

Migration of the ITCF to ServiceNow has provided enhanced functionality and usability and all relevant control information is populated. The quarterly attestation process works well, and provides reasonable coverage against COBIT and NIST frameworks. There are a large number of initiatives in place to further enhance the ITCF and management should ensure that these are appropriately funded and resourced. These include:

- Review of a wider UCF control set against IT policies and standards and alignment of those policies and standards with the ITCF.
- Mapping of ITCF to FCF (Financial Control Framework) controls to bring IT related controls solely under the ITCF.
- Identify and agree key controls, and update ServiceNow accordingly.
- Complete risk mapping of controls against intermediate risks.
- Alignment with the Vendor Risk Management supplier questionnaire.
- Identify KPIs for enhanced reporting.
- Integrated assurance with other parts of the business.

Completion of these activities will significantly enhance the effectiveness of the ITCF, providing better assurance and support for management decision making.

POL00448324

Executive Summary

Whilst there is some functional support across IT to provide a level of objective control assurance, responsibilities for this are not clearly defined and there may be gaps in coverage. Additionally, the Compliance function is not resourced to provide second line assurance. This was identified as a weakness in a previous audit and additional resourcing was agreed. However, due to organisational changes, this still remains as a gap. Additional work is also required to provide focused reporting to the management team.

We noted a high number of controls which were not operating effectively (69 out of 227), although this number has reduced over the past 3 quarters. We consider that the framework is effectively helping the business identify these control weaknesses and remediation plans are in place for 66 of the 69 controls. The IT Governance and Reporting team have undertaken a further analysis of non-compliant controls, identifying only 8 as being 'key' controls.

We consider the risk of control failures not being identified to be low, and that management are taking steps to mitigate risks associated with existing control gaps.

Given the workload required to enhance the framework, and the challenges faced in addressing control gaps, we have rated this report as **'Needs Improvement'**.

Management Comment

"I thank all involved in this piece of detailed and important work. I am pleased that we are making progress with our various ITCF initiatives and that we are now robustly executing all the basic processes consistently. Whilst we have completed significant work over the last few years, we have more to do to ensure that we have done everything reasonable for an organisation of our size and stature. Moving to the next level of effectiveness and maturity will require investment which will need to be balanced off against other demands where funding is required. In the meantime, we will continue to execute continuous improvement opportunities and activities where these are viable."

Dean Bessell, CISO

POL00448324

Summary of Findings

Finding	Rating*	Action Owner	Date
Scope Area: 1. ITCF Design			
1. There are multiple initiatives in place to further mature the ITCF which need to be resourced and tracked.	**P2**	Dean Bessell, CISO	30 Jun 2023
2. There is no comprehensive CMDB in place to enable controls to be linked to systems or infrastructure components.	**P2**	Aatish Shah, IT Governance and Reporting Manager	31 Oct 2023
Scope Area: 2. ITCF Operation			
None			
Scope Area: 3. Control effectiveness and ongoing management			
3. There are a significant number of non-compliant controls.	**P1**	Dean Bessell, CISO	31 Aug 2023
4. Reporting and MI could more effectively support management decision making.	**P2**	Dean Bessell, CISO Aatish Shah, IT Governance and Reporting Manager	31 Oct 2023
5. Organisational support for objective assurance over the ITCF is not fully defined and resourced.	**P2**	Dean Bessell, CISO Anshu Mathur, Interim Group Compliance Director	31 Dec 2023

*P1 = High Priority, P2= Medium Priority, P3 = Low Priority

POL00448324

Detailed Findings and Agreed Actions

Scope Area 1: ITCF Design

This scope area covers the design of the ITCF, it's coverage, alignment with Post Office policies and standards, and international control frameworks. In addition, it covers guidance on control completion and alignment with risk processes.

ITCF coverage

On implementation, the ITCF was aligned with a subset of the COBIT5 (Control Objectives for Information and Related Technologies). Additional COBIT5 processes have been added, as well as controls from the NIST (National Institute of Standards & Technology) cybersecurity framework.

As part of the migration to ServiceNow, the Universal Control Framework (UCF) plugin was purchased to provide access to a wide range of standardised control libraries. The team is currently assessing additional sources for controls, including CREST (Council of Registered Security Testers), European Banking Authority, ISACA (Information Systems Audit and Controls Association), Payment Card Industry (PCI), International Standards Organisation (ISO),and US Federal Government. They have identified approximately 1600 controls across these sources which may be relevant to the ITCF and work is ongoing to identify which are key controls.

It is intended that these will provide a more refined level of control detail, assist in identifying key controls and provide the ability to demonstrate alignment with common control frameworks. Framework alignment work is included as an activity in the Controls Roadmap document, which sets out a plan for delivering multiple initiatives to improve the ITCF.

Risk alignment

Work has been started to align controls against intermediate risk. So far 37 controls have been mapped to 13 intermediate risks and completion of this activity is included in the Controls Roadmap. Additionally, risk workshops are being held to identify and confirm intermediate risks for IT Change Management.

Risk alignment is included as an activity on the Control Roadmap.

Key control definition

On inception, all controls were marked as key controls. There is now an ongoing activity to define which controls are key. This is dependent on the ITCF coverage work outlined above, with key controls being selected against the full list of UCF controls. This work is included in the Control Roadmap.

The POL-wide Control Framework being developed by Compliance will provide an overall approach to control definition and monitoring across the business and is being piloted with IT Change Management Controls. Compliance have provided the team with a definition for key controls, although overall alignment work is ongoing.

POL00448324

Alignment with other Post Office policies, standards and frameworks

Work is ongoing to align Minimum Control Standards contained in Policy and Standard documents with ITCF controls. This is included in the 'UCF Controls Parent Child' spreadsheet. In addition, work is being undertaken to map Financial Control Framework (FCF) controls to the ITCF and retire the controls from FCF. Hazel will provide a roadmap for completion of these activities.

Work is also progressing to fully align the selected control set to Post Office IT Policies and Standards and this is include on the Control Roadmap.

Completeness of control information

We confirmed that all control fields are fully populated within ServiceNow, and that all controls had attestation guidance and evidence requirements defined.

Control attestation and evidence guidance

Annual exercises are undertaken in September/October to discuss controls with control owners and control reviewers to ensure they are properly aligned. Controls are also refined following conversations with control owners either ad-hoc or prior to quarterly attestations. Finally, the IT Governance and Reporting Manager will check a sample of controls on a regular basis to confirm they are well defined.

ServiceNow

Post Office have migrated from TrAction to ServiceNow and this platform provides significant enhancements over the previous platform, including increased automation, integration with UCF, much better dashboards and visibility of controls, greater ability to align with Risk (especially through GRC integration in SNOW) and a full audit trail of changes. Discussions with stakeholders confirmed ServiceNow provides adequate support for control self-attestation but that alignment with the CMDB module would provide greater integration. This module is not yet fully implemented.

Conclusion

Migration of the ITCF to ServiceNow has provided enhanced functionality and usability and all relevant control information is populated. The quarterly attestation process works well, and provides reasonable coverage against COBIT and NIST frameworks. There are a large number of initiatives in place to further enhance the ITCF and management should ensure that these are appropriately funded and resourced.

POL00448324

1. There are multiple initiatives in place to further mature the ITCF which need to be resourced and tracked. (P2)

There are a significant number of initiatives in progress to enhance the ITCF and it is not clear whether the resources and funding are available to achieve these in a timely manner.

Work is ongoing to enhance the design and operation the ITCF to provide greater alignment with business objectives and international frameworks, including:

- Review of a wider UCF control set against IT policies and standards and alignment of those policies and standards with the ITCF.
- Mapping of ITCF to FCF (Financial Control Framework) controls to bring IT related controls solely under the ITCF.
- Identify and agree key controls, and update ServiceNow accordingly.
- Complete risk mapping of controls against intermediate risks.
- Formalise a mechanism to ensure control issues are fed into risk management processes, where required.
- Realignment with the Vendor Risk Management supplier questionnaire.
- Identify KPIs for enhanced reporting.
- Integrated assurance with other parts of the business other than financial control and SPO.

This work will lead to a more focused ITCF, providing a greater ability to manage risks and ensure that key controls are operating effectively across IT. A roadmap for delivery has been defined, however, it represents a substantial amount of work and it is not clear whether the resources and funding is available to complete these activities.

Risk

Without clear resourcing and funding available, there is risk that necessary enhancements to the ITCF will not be delivered, reducing the effectiveness of control assurance and management decision making.

Agreed Management Action

The CISO will confirm that resources and funding are available to support ITCF enhancements, and ensure that timescales are achievable.

Action Owner: Dean Bessell, CISO

Date: 30 June 2023

POL00448324

2. There is no comprehensive CMDB in place to enable controls to be linked to systems or infrastructure components. (P2)

At present, the Configuration Management Database(CMDB) is not sufficiently implemented to enable the alignment of the ITCF with Post Office systems and infrastructure.

ServiceNow's CMDB module provides an inventory of system and configuration information which can be linked to other modules, including GRC to provide component specific control assessments. Post Office have partially implemented the CMDB, however it does not yet provide a functional inventory of Post Office systems and infrastructure. As a result, controls within the ITCF cannot easily be linked to infrastructure components. An approach for fully implementing the CMDB is being defined by the NBIT Programme and it is intended that this will be rolled out across the business.

Risk

In the absence of a fully functional CMDB, control failures cannot be linked to specific components, making it difficult to identify and address control issues related to specific systems.

Agreed Management Action

The IT Governance and Reporting Manager will work with the NBIT programme to identify requirements and methodology for integrating the ITCF with the CMDB.

Action Owner: Aatish Shah, IT Governance and Reporting Manager

Date: 31 October 2023

POL00448324

Scope Area 2: ITCF Operation

This scope area covers the effective operation of the ITCF, including attestation completeness, data quality, and user training and guidance.

Attestation guidance

The 'ServiceNow IT Controls User Guide' provides clear guidance on control self-assessment and is provided to all control owners each quarter. ServiceNow includes fields for 'Attestation Guidance' and 'Expected Evidence' fields which provide bespoke guidance for control attestation. We confirmed these fields were complete for all controls. Furthermore, training is provided by the IT Governance and Reporting Manager to individuals and groups of users on how to use ServiceNow.

Control and attestation completion

Control details are defined in ServiceNOW via a download from UCF and all fields must be completed. Evidence provision for attestations is mandatory and enforced through ServiceNOW. The IT Governance and Reporting Manager sends reminders to all control owners to complete self-assessments. Required assessments are also captured in the Compliance Dashboard on ServiceNow.

Assignment of Control Owners and Control Reviewers

Annual exercises are undertaken in Q3 to discuss controls with control owners to ensure they are properly aligned. Controls are also refined following conversations with reviewers following the annual review process, or with control owners either ad-hoc or prior to quarterly attestations. The IT Governance and Reporting Manager will check a sample of controls on a regular basis to confirm they are well defined.

Control Frequency

Annual exercises are undertaken by the IT Governance and Reporting Manager to discuss controls with control owners to ensure they are properly aligned. Controls are refined through conversations with reviewers following the annual review process, or with control owners either ad-hoc or prior to quarterly attestations. Finally, Aatish will check a sample of controls on a regular basis to confirm they are well defined. "

Conclusion

We found that there is clear guidance on the completion of quarterly attestations and that appropriate training is in place to support control owners and reviewers in the operation of the ITCF. Mechanisms are in place to refine and update attestation guidance, and controls ownership.

POL00448324

Scope Area 3: Control effectiveness and ongoing management

This scope area covers control remediation, escalation, reporting and risk management.

Identification and remediation of non-compliant controls

Controls are defined as compliant or non-compliant based on self-assessment. Controls which are non-compliant automatically create an Issue in ServiceNow within the GRC module or elsewhere. Recommendations and Action Plans are captured in ServiceNow along with date raised, ownership and number of updates.

Month	Attestation completion	Compliant	Non-compliant with remediation plan	Non-compliant, no remediation plan
July 2022	94%	65%	35%	0%
October 2022	100%	64%	35%	1%
January 2023	100%	70%	29%	1%

Attestation completion has been at 100% for the last two quarters and the number of non-compliant controls, whilst high, is reducing. Non-compliant controls are those which are not considered to operating effectively. Control compliance has increased over the year from 65% to 70% and, as at February 2023, 69 of the 227 controls have been assessed as non-compliant. Issues have been raised for all non-compliant controls and remediation plans are in place for 66 of the 69 controls. The ITCF attestation and issue identification processes is working effectively, allowing management to identify control gaps, however there are clear challenges faced by the business in resolving control these gaps, including financial and resourcing limitations.

Whilst the IT Governance and Reporting team will discuss non-compliant controls with control owners, they are focused on the operation of the ITCF itself rather than issue resolution. The identification of more focused key controls, as discussed above, will impact the number and impact of non-compliant controls and enhanced reporting may help the first line monitor and resolve issues more effectively. However, the absence of organisational support to provide oversight of the effective operation of controls impacts the ability of IT to confirm and address control weaknesses effectively.

Issue tracking

Issues raised from remediations are tracked (see 'IT Issue & Aging' spreadsheet). A process for monitoring and closing these is undertaken on an ad-hoc basis and there is ongoing work to reduce the number of non-compliant controls. A more formal process should be led by Compliance as part of the POL-Wide Control Framework.

Reporting of ITCF operation and outputs

The IT Governance and Reporting team provide input to the security slide for the monthly ITB (IT Board) meeting. In addition, they have undertaken an analysis of themes for non-compliant controls to provide more focused MI to management and this has been shared with the CISO. Discussions with the CDIO indicated that he would prefer a more detailed and focused level of reporting to support decision making.

POL00448324

Conclusion

Overall, we found that the ITCF was operating effectively, with high levels of attestation completion and identification of non-compliant controls. Issues are raised for all non-compliant controls and action plans for remediation are present in almost all cases. High level results from the attestation process are reported upwards, although it is not clear whether this process feeds into risk identification. Additional work is also required to understand how objective assurance is provided over the design and operation of the ITCF.

POL00448324

3. There are a significant number of non-compliant controls. (P1)

There are a significant number of controls which have been assessed as not operating effectively.

As at February 2023, 69 of the 227 controls have been assessed as non-compliant. Issues have been raised for all non-compliant controls and remediation plans are in place for 66 of the 69 controls. Responsibility for ensuring the correct operation of controls sits with control owners, however, the IT Governance & Reporting function can assist the business by providing clear reporting to management on control defects and supporting in issue resolution.

The IT Governance and Reporting team have put together a list of key themes for control gaps and shared this with the CISO. The impact of the control gaps will be clearer once work to define key controls has been completed. In the interim, the team have performed an analysis of the non-compliant controls, identifying 8 as key controls. Clear remediation plans are in place for all 8 controls, although these are largely reliant on resourcing or tooling being available. The remaining controls are non-compliant for the following main reasons:

- The control may not be operating across its full scope (e.g., controls may operate for a subset of key systems only).
- Evidence has not yet been received from third parties (e.g., for Fujitsu physical access controls).

They are linked to the 8 key controls identified above, although they are not key controls in their own right. The risk is being reduced in that only 8 of the non-compliant controls are key controls.

Risk

IT risks faced by the business and highlighted by the ITCF may not be mitigated.

Agreed Management Action

The CISO will identify a process to enhance reporting to, and interaction with, the business to address control gaps, focusing on key controls. This may require clarification and resourcing of objective control assurance, as well as enhanced reporting of control defects to management (see observations 4 and 5 below).

Action Owner: Dean Bessell, CISO

Date: 31 August 2023

POL00448324

4. Reporting and MI could more effectively support management decision making. (P2)

There is limited reporting to management of ITCF outputs.

Discussions with key stakeholders identified a lack of actionable information arising from the ITCF process. Whilst ServiceNow provides more integrated MI than the previous ITCF platform, through the creation of control dashboards, control owners have limited visibility of all controls operating across their teams.

A short summary of ITCF outcomes in provided to the monthly ITB but this is highly summarised and does not highlight key control gaps.

Integration with the UCF provides an opportunity to demonstrate compliance with global standards and frameworks, however this is not currently done. Ongoing work to align with a wider range of standards and to identify key controls may make this more achievable and relevant.

Risk

Management may not have actionable information on which to understand and act upon the risk and control positions highlighted by the ITCF.

Agreed Management Action

a. The CISO will provide focused feedback on the operation of the ITCF and key control gaps on a monthly basis. This could include key themes, actions and quarterly trend reporting.

Action Owner: Dean Bessell, CISO

Date: 30 September 2023

b. The IT Governance and Reporting Manager will investigate how and whether reporting can be enhanced to provide visibility of the operation of controls across each IT area, at GE-1 level.
c. The IT Governance and Reporting Manager will assess the feasibility and value of providing reporting of compliance against the Post Office selected frameworks.

Action Owner: Aatish Shah, IT Governance and Reporting Manager

Date: 31 October 2023

POL00448324

5. Organisational support for objective assurance over the ITCF is not fully defined and resourced. (P2)

Responsibilities for control assurance within Technology are not clearly defined or resourced.

Whilst there is some functional support across IT to provide a level of objective control assurance, responsibilities for this are not clearly defined and there may be gaps in coverage. Additionally, the Group Compliance function is not currently structured to provide systemic second line assurance.

Risk

In the absence of objective oversight and second line assurance, there is a reliance on control owners to provide accurate and pertinent updates and evidence. As a result, the business may have an incomplete or inaccurate understanding or objective assurance of the efficacy of the control environment.

Agreed Management Action

a. The CISO will work with IT to identify control assurance coverage and create a plan to address these gaps.

Action Owner: Dean Bessell, CISO

Date: 31 August 2023

b. The Group Compliance function are in the process of re-assessing their structure and coverage for POL. This exercise, once completed, will define the basis for 2 LOD assurance activities, including for IT controls. There is, however, a significant first line contingency for the completion of this task.

Action Owner: Anshu Mathur, Interim Group Compliance Director

Date: 31 December 2023

POL00448324

Distribution List

	Name	Job Title
Executive Sponsor:	Zdravko Mladenov	Group CDIO
Distribution:	Dean Bessell	CISO
	Aatish Shah	IT Governance and Reporting Manager
	Hazel Freeman	Security Consultant
	Anshu Mathur	Interim Group Compliance Director
	Rebecca Barker	Deputy Head of Risk
Audit Team:	Jonathan Acres	Senior Audit Manager
Key Dates:	ToR	27 October 2022
	Fieldwork	9 November – 10 February 2023
	Draft Report	7 March 2023
	Final Report	14 March 2023
	RCC	14 March 2023
	ARC	28 March 2023

POL00448324

Appendix 1 – Terms of Reference

Background:

The IT Control Framework (ITCF) is a set of 227 controls, maintained in the ServiceNow GRC module. It provides an ongoing assessment of the operation of controls and any outstanding control remediations, based on control owner self-assessment.

Internal Audit previously reported on the effectiveness of the ITCF as part of the 2018/19 and 2020/21 Internal Audit plans. We also reviewed the migration to ServiceNow GRC in 2021/22.

Audit Objective:

To assess whether the ITCF provides effective assurance of the operation of IT controls and supports risk monitoring and mitigation.

Impact on Postmasters:

The ITCF provides assurance that IT controls are operating effectively, reducing the risk of disruption to branch operations.

Key Risks:

High level risks that should be addressed by the control framework include:

- Confidentiality – unauthorised access being gained to Post Office systems and data.
- Integrity – threats to the consistency, accuracy and reliability of data.
- Availability – inability to access systems and data as required.

Scope of Audit:

This will be a 'Limited Scope Review', focused on monitoring controls and other relevant key controls.

The review will cover the design and implementation of the ITCF, building on previous Internal Audit assessments.

Specifically, it will cover the following areas:

- ITCF design: assess the design of the ITCF to ensure risks, controls and associated control objectives are fit for purpose, incorporating industry best practices and Post Office control requirements.
- ITCF operation: assess the adequacy of the processes operated and tools used to deploy the ITCF, including sign-off by control owners.
- Control effectiveness and ongoing management: review and assess the process for reporting on control effectiveness and identifying, tracking and escalating any remediations or control design improvements required.

We will look at key indicators, such as the completeness of control self-assessment and the number of remediations, to guide limited testing of control operation.

Where appropriate, data analytics will be used to support the review.

Timeline:

Pre-Work:	November 2022
Field Work:	12 December 2022 – 20 January 2023
Draft report:	3 February 2023
Final report	17 February 2023

Audit Team:

Jonathan Acres, Senior Audit Manager

Reporting:

We will produce a report to management at the end of the audit and the results will be summarised for the March 2023 RCC and ARC meetings.

POL00448324

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