Item: 5.3

Monitoring and Audit Committee: 16 November 2023.

Internal Audit Report: IT Operations.

Report by Chief Internal Auditor.

1. Purpose of Report

To present the internal audit report on procedures and controls relating to IT Operations.

2. Recommendations

The Committee is invited to scrutinise:

2.1.

The findings contained in the internal audit report, attached as Appendix 1 to this report, reviewing procedures and controls in place relating to IT Operations, in order to obtain assurance that action has been taken or agreed where necessary.

3. Background

3.1.

Orkney Islands Council relies heavily on ICT to deliver many critical services. It is therefore of great importance that IT operations can consistently run well and help support the organisation to meet its objectives.

3.2.

As well as an ever-changing technological landscape, the IT department in Orkney also supports Council systems across the length and breadth of the islands. This comes with geographical challenges and connectivity support needs for some users in remote locations.

3.3.

The objective of this audit was to assess the effectiveness, efficiency, and security of the IT operations within Orkney Islands Council. The audit focused on evaluating the governance, processes, controls, and infrastructure supporting the IT systems used.

4. Audit Findings

4.1.

The audit provides substantial assurance that procedures and controls relating to IT Operations are well controlled and managed.

4.2.

The internal audit report, attached as Appendix 1 to this report, includes seven low priority recommendations regarding policy reviews, job descriptions, training records, training course updates, retention periods, service level agreements and the IT asset register. There are no high or medium priority recommendations made as a result of this audit.

4.3.

The Committee is invited to scrutinise the audit findings to obtain assurance that action has been taken or agreed where necessary.

5. Corporate Governance

This report relates to the Council complying with governance and scrutiny and therefore does not directly support and contribute to improved outcomes for communities as outlined in the Council Plan and the Local Outcomes Improvement Plan.

6. Financial Implications

There are no financial implications associated directly with the recommendations in this report.

7. Legal Aspects

Complying with recommendations made by the internal auditors helps the Council meet its statutory obligations to secure best value.

8. Contact Officer

Andrew Paterson, Chief Internal Auditor, extension 2107, email andrew.paterson@orkney.gov.uk.

9. Appendix

Appendix 1: Internal Audit Report: IT Operations.

ORKNEY
ISLANDS COUNCIL

Internal Audit

Audit Report

IT Operations

Draft issue date: 20 October 2023

Final issue date: 2 November 2023

Distribution list:	**Corporate Director for Neighbourhood Services & Infrastructure** **Head of Service (Property, Asset Management & Facilities)** **ICT Service Manager** **ICT Programme Manager** **Team Manager (ICT Operations)** **Information Security & Assurance Officer** **Service Manager for Organisational Development**

Contents

Audit Opinion

Based on our findings in this review we have given the following audit opinion.

Substantial	**The framework of governance, risk management and control were found to be comprehensive and effective.**

A key to our audit opinions and level of recommendations is shown at the end of this report.

Executive Summary

Orkney Islands Council as an organisation relies heavily on IT Operations to ensure good communication, innovation, efficiency and security. Much of critical service delivery depends on systems and infrastructure that is supported by the IT team. Therefore, it is crucial that the IT department is well-resourced and able to run effectively. This audit has found that there is strong, dynamic governance in place which supports a dedicated team who are able to work together to provide a valuable service and demonstrate resilience despite staffing constraints. There have been key vacancies recently within a staff team that is already small.

The IT department is also providing support across the length and breadth of the isles and there are many examples of this contained within Information Services Programme Board (ISPB) Availability and Progress reports. Examples include restoring connectivity to schools on the outer isles, maintaining microwave links between different sites, building resilience into the network and keeping links functioning whilst facing challenges with delays in equipment being delivered. Nationally, OIC is a member of SWAN2- a programme set up to establish a single shared network and common ICT infrastructure across Scotland's public sector- delivering better connectivity, improved performance and faster speeds.

There are robust key controls in place to strengthen IT Operations for OIC and the recommendations made in this report are made to enhance those controls, improve efficiency and implement processes for continuous review.

Areas of good practice were identified during this audit, including:

- When reviewing IT governance in place, it was evident that the ICT service strategy as well as delivery aligns with Orkney Islands Council objectives in supporting Orkney as a whole in the ever changing world of IT.
- The ISPB provides dynamic governance, assurance that service availability is meeting the needs of the end users that rely on this as well as monitoring the effectiveness of the security measures in place. There is clear assessment and active management of risk and issues arising detailed in the minutes of the quarterly meetings but this is also evident from how quickly critical issues are addressed on an ongoing basis.
- OIC policies and procedures related to procurement are being followed.
- Due to effective forward planning and budget monitoring the IT team have been able to stay within budget and keep systems and infrastructure running smoothly.

- There are robust security measures in place, with automated controls which are backed up by knowledgeable staff who ensure that manual controls required are in place to reduce the risk of security breaches or cyber-attacks. Although covered in a previous audit, there are also robust resilience measures put in place through the disaster recovery plans and support from third parties available, should a critical loss of data or service arise because of an adverse event.
- For new staff joining the service a bespoke induction process is in place to ensure that all new staff members have the information required when starting and ensuring consistency within the team.

The report includes 7 recommendations which have arisen from the audit. The number and priority of the recommendations are set out in the table below. The priority headings assist management in assessing the significance of the issues raised.

Responsible officers will be required to update progress on the agreed actions via Pentana Risk.

Total	High	Medium	Low
7	**0**	**0**	**7**

The assistance provided by officers contacted during this audit is gratefully acknowledged.

Introduction

Orkney Islands Council relies heavily on ICT to deliver many critical services. It is therefore of great importance that IT operations can consistently run well and help support the organisation to meet its objectives.

In recent years, the IT department has overseen a shift from the infrastructure being managed on OIC premises to core systems being hosted on the Cloud. The implementation of Microsoft Office 365 cloud services in 2016/17 was a key improvement and proved vital in supporting a 'new normal' way of working as part of navigating the impact of the COVID-19 pandemic. The IT department has played a crucial role in ensuring staff members are set up and supported to work remotely whilst maintaining security. Something that has continued long after employees made a return to the office.

As well as an ever-changing technological landscape, the IT department in Orkney also supports Council systems across the length and breadth of the islands. This comes with geographical challenges and connectivity support needs for some users in remote locations.

Underpinning the IT Strategy for 2021-24 are the principles 'common, simple and everywhere' and a recent report presented to the Asset Management Sub-Committee on 28 August 2023, detailed substantial progress towards meeting objectives in the strategy despite having had recent staff vacancies to contend with in an already small team. Key objectives have included supporting communication links between NHS staff and OHAC as well as introducing appropriate cloud technologies enabling OIC email to be entirely hosted via Microsoft 365. The IT Strategy is due to be refreshed in the next year.

The objective of this audit was to assess the effectiveness, efficiency, and security of the IT operations within Orkney Islands Council. The audit focused on evaluating the governance, processes, controls, and infrastructure supporting the IT systems used.

This review was conducted in conformance with the Public Sector Internal Audit Standards.

Audit Scope

The scope of this audit was to review the following:

- The governance structure and processes in place ensure IT are operating in accordance with organisational objectives.
- Staff roles and responsibilities are defined and staff are suitably trained.
- There are robust security procedures in respect of both hardware and software facilities, as well as network security.
- Risk management processes are in place.
- Suitable budget controls are in place to ensure the service is adhering to OIC financial policies and procedures.
- The procurement process adheres to OIC policies and procedures.
- Service desk operations are effective in supporting service users and communities across Orkney.

- IT infrastructure supports services within OIC to manage their systems well (such as Integra, Concerto etc.).
- There are effective asset management plans in place.
- There are policies and procedures for back-ups and resilience.
- Mobile technology controls and measures are in place.

Disaster Recovery was not covered within the scope as a previous audit reviewed this in 2022/23.

When reviewing asset management, assets pertaining to schools are outwith the scope of this audit and will be included in separate schools audits.

The audit work focuses on the period from April 2022 to October 2023.

Audit Findings

1.0 Governance

1.1 Having reviewed the current and previous OIC Plans and Delivery Plans, the IT Strategy is aligned with the priorities set out in these plans. The ICT Asset Management Plan highlights how it aligns with the Council's Mission, Values and Strategic Objectives and the latest Digital Strategy Delivery Plan links to the current Council Plan (2023-2028). The Information Security Policy is informed by standards set out by the International Organisation for Standardisation (ISO) and Staff Guidance sits alongside this. Both are accessible to staff on the Intranet and the staff guidance is embedded in the approach to induct new staff members to OIC, ensuring a consistency in the message being delivered about the importance of information security.

1.2 Of seven IT policies sampled, three of the policies reviewed hadn't been updated in over 5 years, one was from 2008 and some required updating to reflect staff changes and the Council restructure. IT Policies and Procedures should be reviewed at least every 5 years, or sooner, where updates are required. A process for review should be implemented to ensure that policies are reviewed regularly and as appropriate added to the OIC Intranet to enable staff access as well as a central folder for IT staff on their Teams page where specific IT policies can be held and accessed.

Recommendation 1

1.3 The Information Services Programme Board (ISPB) provides governance over IT Operations. This board meets quarterly and at these meetings, ICT services availability progress reports as well as General Cyber Security Reports are presented which include recommendations and actions agreed to continually review and improve the service as well as address any issues arising or significant change management. There is also a change management system in place within the IT department. The Change Acceptance Board (CAB) meet weekly to plan and manage change as well as offer comment and advice. The helpdesk system supports the change management process, it requires the process to be completed in steps: Submission, Planning, Approval, Implementation and Review which ensures that change is managed and governed in a systematic way.

1.4 The IT team have a OneNote file that is used as a common knowledge base and covers procedures covering many topics. This is used mainly by IT Technicians and also covers some backup and database management procedures. Procedures within this file are updated on an ongoing basis where required. Systems change frequently so it's necessary to have a working document such as this available to all staff.

2.0 Staffing

2.1 The IT department has a clear organisational structure with a helpful section on its intranet page with staff names and their respective roles and contact details. There are defined roles and responsibilities and there is a sense that as a small team, they support each other in keeping the vast IT system running smoothly. Operations include manning a duty phone so there is a need for staff to participate in a standby duty rota. This is voluntary at the moment as there are plenty of staff willing to participate in this without it being a formal requirement.

2.2 There were two job descriptions that have not been updated to the new template and designation name- for the Information Security and Assurance Officer and for the ICT

Programme Manager. Both are key roles within the team and there is a recommendation that all roles in the IT department have an up-to-date job description retained on file and that the relevant jobs have an indication of the requirement to be on standby where required. The ICT Service Manager said that through the restructure, many job titles and roles changed and they are working through a process of updating job descriptions.

Recommendation 2

2.3 The ICT Operations Manager has developed an IT induction checklist for new staff which is comprehensive and covers IT specific areas that will be used alongside the HR induction checklist, ensuring consistency across the technician team.

2.4 The IT staff are always developing their knowledge and skills to stay up to date in an ever-changing IT landscape. Training is important to the team especially for new staff. There are currently no requirements to keep training records for the profession as there is in some other departments at the Council, however it would be good practice to do so and could help to monitor skills and knowledge acquired by the team as well as support performance evaluation and succession planning.

Recommendation 3

2.5 When corporate staff leave the OIC, there is a leavers form for managers to complete which includes details of IT equipment that the individual held as well as procedures to follow. This is located on the IT intranet page under 'New Staff- Forms & Information'. If this form isn't completed to alert IT to staff leaving, HR and Payroll inform them as a back-up so that they are aware to remove access appropriately.

3.0 Security

3.1 Security is a priority for IT operations. There are good security measures in place in terms of access to the building and procedures to ensure that visitors are recorded and only permitted on site with prior appointment.

3.2 There is information for staff in the Information Security Staff Guidance booklet around physical security and keeping hardware secure and all OIC staff must sign an IT user acceptance form on joining the organisation.

3.3 There are clear procedures on reporting and managing security breaches and incidents. All staff know what to do if there is a security breach as the iLearn course 'Information Security' contains information about how to report a breach and more importantly how to avoid one. The information on the iLearn 'Information Security' training should be updated with the correct contact details for the Information Governance Officer as the post holder has changed.

Recommendation 4

3.4 There are many different audit logs recorded and kept as another defence to support security. System logs are kept for a year and so could be accessed in the event that an investigation is required. Networking equipment logs are kept as long as the disk space allows and this isn't always able to be for one year. . Following Scottish Government Digital Office recommendations, the ICT Service Manager looked at options to put a Security Event Management (SEM) system in place. This should be progressed to ensure that logs are kept and available in the event of a security incident.

Recommendation 5

3.5 A big part of IT Operations is overseeing the corporate replacement programme, ensuring that devices used within OIC are up to date, secure and compatible with Windows 11. The IT operations team manage a significant level of deliveries of equipment and generally, items are delivered either directly to the client or to King Street where staff members will collect items or technicians will deliver them themselves.

3.6 There are regular firewall updates and these are checked. A programme called 'Nessus' scans the system and reports if there are any issues. External consultants are also used to check that security measures are up to date and effective. To support the application for PSN (Public Service Network) accreditation, IT commissions an external health check which concludes with a report detailing any issues that require remedial action. IT put plans in place immediately to deal with critical issues and take high issues into account to ensure that the systems in place ensure the highest level of security possible.

3.7 As part of ensuring that data is secure, equipment that is deemed to be at the end of its operational life and is out of warranty is securely disposed of using a degausser that wipes all data. There is a reallocation form used to record when items have been degaussed, when they have been removed from the asset register and when they have been safely disposed of at the waste transfer site. Our testing indicated that there were some items due for disposal that had not been removed from the asset register. We recommend that all items due for disposal are removed from the register and the reallocation form is kept up to date. Internal audit will include checks that items due for disposal from schools are removed from school IT inventories during school audits.

See Recommendation 7

3.8 Access to systems for staff is granted on a least privilege basis. There are procedures in place to restrict access appropriately when new members of staff join the organisation or move between roles.

4.0 Risk Management

4.1 There is an IT risk register in place which is regularly reviewed. This register aligns with the objectives set out in the IT Strategy and is monitored to ensure mitigations are undertaken and effective.

4.2 Risk assessments are put in place to support the health and safety of staff in the IT building and whilst working at different sites such as the Wideford Mast. Some of the risk assessments we sampled are clearly reviewed regularly and updated as and when required. There are some risk assessments due to be reviewed such as the fire risk assessment however there are weekly fire checks carried out that sit alongside this. We recommend that as part of the continuous review processes for policies and procedures, risk assessments are included in this to ensure that they are all reviewed at least annually and more often if there are significant changes to consider.

See Recommendation 1

5.0 Budgeting

5.1 Suitable budget controls are in place to ensure that the service is adhering to OIC financial policies and procedures. An annual budget is set and approved by the Policy and Resources Committee. There is an IT indicative programme submitted to the Asset Management Sub-Committee detailing how the annual budget will be allocated, prioritising urgent and critical work or replacements needed to support systems and infrastructure due to budget constraints. The budget is monitored, and regular expenditure monitoring reports are presented as well as underspends reported recently due to staff vacancies across the IT service and also reduced costs for IS Networking Supplies and Services. Recharge costs are apportioned correctly, and all purchases tested as part of the audit adhered to policy and procedure.

6.0 Procurement

6.1 The IT service is adhering to Council policies and procedures, complying with OIC Financial Regulations and Contract Standing Orders in respect of supplies and services, with justification given to use single supplier frameworks or non-competitive actions.

6.2 'Green IT' is certainly on the agenda and is something the service is aware of, for example having virtualised servers- going from 198 in 'The Bothy' (server storage site) to just one. Owing to most purchases going through frameworks, only the framework sustainable policy can be adhered to and the OIC's sustainable policy cannot be enforced upon them and at times, the nature of the service being contracted means it is difficult to include a metric that could realistically measure sustainability however there is the intention to carry out procurement in a sustainable way as much as possible.

7.0 Service Desk Operations

7.1 Procedures are well documented and accessible to OIC staff regarding how and where requests and incidents should be reported. IT service contact details are available on the OIC Intranet and there has also recently been an email circulated with preferred methods of contact. There is also information in for staff issued when commencing employment with OIC through the 'Information Security Staff Guidance'.

7.2 There are clear procedures for handling requests that come into the service desk and systems for monitoring these to spot trends and recurring issues as well as ensure that time-restricted requests are handled accordingly. These are reported to senior management and discussed at weekly meetings. Knowledge around recurring faults is used to help with forward planning in terms of what work takes priority or the urgency of replacing equipment under the replacement programme. There is a system for ensuring that all requests are assigned to the appropriate individual who will be responsible for resolving this or passing it on to a more senior member of staff if required. In the most recent copy of the ISPB Availability and Progress report, progress continues to be made to maintain high levels of availability for IT services.

7.3 There is an ICT Support Services Charter which provides a description of the services offered by IT, support standards, roles and responsibilities of customers and the ICT Team, details of prioritisation and targets for availability. The Service Manager stated that a Service Level Agreement is due to replace the ICT Support Services Charter and this is being worked on.

7.4 There is currently one Service Level Agreement in place with the Valuation Joint Board which has recently been established therefore we did not test this however we reviewed the

agreement against necessary elements and noted that future SLAs should include how performance will be monitored against the objectives and include a process for obtaining user feedback on the service provided.

Recommendation 6

7.5 In addition to helping to resolve IT issues for the OIC staff team, the department is also providing support across the length and breadth of the isles and there are many examples of this contained within ISPB Availability and Progress reports. Examples include restoring connectivity to schools on the outer isles, maintaining microwave links between different points, building resilience into the network and keeping links functioning whilst facing challenges with delays in equipment being delivered. Nationwide, OIC has participated in the Pathfinder North partnership which consists of five local authorities and is responsible for the delivery of the Scottish Wide Area Network (SWAN). The Pathfinder North partnership is going to be dissolved and a procurement process has recently been completed for SWAN2. OIC will become an active member and a Deed of Adherence has recently been completed. This programme was set up to establish a single shared network and common ICT infrastructure across Scotland's public sector- delivering better connectivity, improved performance and faster speeds.

8.0 Systems Support

8.1 The ICT Service Charter details that the ICT Service provides infrastructure support of servers and networking to support the delivery of Council Service's specific IT systems, including PARIS/Integra/Northgate HR and Concerto. The ICT Asset Management Plan 2021-2026 states that at the heart of technology lies the business systems that support the wide range of services (e.g., Housing system, financial ledger system). These and other "back office" systems are delivered by servers, databases and storage infrastructure. For example, Northgate, used by the Revenue and Benefits team as well as the Housing team, is mainly supported through the setting up of servers to support the software and to enable the software to interact efficiently with other software.

8.2 IT support for the PARIS (Case Records Management used by OHAC & NHS colleagues) system and the recent upgrade has been significant. The IT team provide infrastructure and network support but also bolster resilience through involvement in meetings to stay up to date and support, help to co-ordinate and can step in during the absence of the system developer. User requests, password resets and system requests/issues come through the helpdesk so these can be monitored. The PARIS system developer has access to the helpdesk and there is an IT technician and Data/GIS Officer who can step in as well to support when required.

9.0 Asset Management

9.1 There is a clear ICT Asset Management in place at the governance level. There is also an Information Security Guidance booklet for staff which includes information about physical security of assets- it is a requirement to adhere to this and all users need to sign a user agreement.

9.2 There is insurance in place for property damage which includes an element of portable equipment used out with OIC premises. Measures in place within IT Operations also act like insurance such as immutable backups and devices in stock that IT themselves can build in the event of a catastrophic event.

9.3 There are thousands of pieces of IT equipment in use at OIC. There is an asset register used to record equipment and details of who it is allocated to. A reallocation form is used when allocating goods to staff and which also includes disposing of goods. There is also an asset worksheet which is a record of new stock pertaining to the corporate replacement programme.

9.4 Through our tests on the asset register we found that equipment isn't consistently recorded within the asset register and some information is missing such as staff names against equipment. Some older items of equipment are not recorded as they would have been on an old asset register and not transferred over. The ICT Service Manager indicated that the asset register relies on staff to keep it up to date manually and due to staffing constraints, this can be challenging to do. We are aware of plans within the IT department to create one master list for all equipment from computers to network switches both in corporate OIC and Schools. SharePoint and Power Apps will be used to create this to make it easier to manage.

9.5 The use of removable media has decreased significantly now that there is access to OneDrive and SharePoint. When removable devices have been issued to members of staff in the past, they are password protected and encrypted to reduce the risk of a data breach. In discussion with members of the IT team, there is no up to date record of removable media devices and the last audit on this was conducted in 2018. The software used to conduct such audits is no longer in use as it runs on an old operating system. Removable media should be registered on the asset register so there is information about who uses these devices and for what purpose. If these devices exist but are obsolete, employees should be encouraged to return these to IT for secure disposal. The IT team are in the process of contacting known previous users of safesticks to quantify the amount within the OIC staff team and to check whether they are still in use.

Recommendation 7

10.0 Backups and Resilience

10.1 The ICT Asset Management Plan 2021-26 stipulates that one of the values of the Council is resilience. IT supports resilience using data backup systems and infrastructure. These are used to ensure that all the organisation's data and configuration is copied onto secure storage so that if there was a catastrophic event, it can be restored to a recovery point that minimises organisational loss. There is a back-up policy which supports the Council's Information Security Policy. In addition, details of data storage and backup is provided in the Information Security Staff Guidance booklet to ensure staff follow policy to support this. There are IT specific backup procedures accessible to the IT team through the common knowledge base OneNote file.

10.2 There are schedules for backups, patches and updates. Backups operate daily using a blend of methods to suit the range of systems in place. The backup schedule details a list of all servers requiring backup, retention cycles and the dates they are scheduled. There is an automated programme that manages the backups across the servers and this programme communicates with the ICT Infrastructure Officer, alerting to any issues arising. For the network, backups are only scheduled manually on an ad hoc basis and when significant changes have been made. Going forward, Cisco DNA Centre will change this in that as it is a new centralised maintenance system, it will be set up to ensure more regular backups are scheduled, involving less manual input from the Systems Support Engineer, reducing workload in this area.

11.0 Mobile Technology

11.1 There are clear procedures around remote working on the IT Intranet page that detail how things are set up to protect the Council's data and systems as well as to ensure there is no unauthorised access. There is a two-step authentication process in place which is explained in the remote working guide.

11.2 There are two kinds of remote working. Standard remote working is the ability to use a Council laptop outside the offices to access emails, Teams and OneNote.

11.3 VPN remote working is the ability to use a Council laptop to remotely control another council computer, that's sitting inside the office. This allows staff to use the G Drive, Paris, Integra etc. Most staff have standard remote working, some also have the VPN feature, and a small minority of staff only have the VPN feature.

Action Plan

Recommendation	Priority	Management Comments	Responsible Officer	Agreed Completion Date
1 A system should be put in place to support a continuous process of review for all policies, procedures and risk assessments. This would include adding relevant policies to the OIC intranet and/or storing them in a central folder accessible to the IT team.	Low	Recommendation is accepted and agreed	ICT Service Manager	01/11/24
2 All roles in the IT department should have a job description retained on file and that the relevant jobs have an indication of the requirement to be on standby where required.	Low	Agreed, job descriptions exist, but need to be updated to new template and designation	ICT Service Manager	01/11/24
3 Training records should be kept as this is evidence of training received and may help monitor skills and knowledge acquired by the team as well as support performance evaluation and succession planning.	Low	Agreed, training is ongoing for staff and as a small team, managers are aware of training completed. However, fully agree with recommendation and this will be put in place.	ICT Operations Manager	01/11/24
4 The information on the iLearn 'Information Security' training should be updated with the correct contact details for the Information Governance Officer as post holder has changed.	Low	The Service Manager for Organisational Development has updated the Information Security iLearn course.	Service Manager for Organisational Development	Action Confirmed as Completed 31/10/23
5 The plan to implement a Security Event Management system (SEM) should be	Low	This is an ongoing desire of IT, and agreed this should be put in place.	ICT Service Manager	01/06/25

progressed to ensure that logs are kept and available in the event of a security incident.		Investigations with digital office and /or independent solutions are ongoing. Agree fully with recommendation		
6 Future SLAs should include how performance will be monitored against the objectives and include a process for obtaining user feedback on the service provided.	Low	Agreed	ICT Service Manager	01/12/24
7 Asset registers and reallocation forms should be kept up to date to record what items are held against which department/staff member (including removable media) and show when items have been securely disposed of. Where removable media devices exist but are obsolete, employees should be encouraged to return these to IT for secure disposal.	Low	Asset registers are kept at present, but due to the large volume of asset turnover, small errors are inevitable due to human error. Therefore, an electronic system will be explored. In the meantime, processes will be reviewed.	ICT Operations Manager	01/06/25

Key to Opinion and Priorities

Audit Opinion

Opinion	Definition
Substantial	The framework of governance, risk management and control were found to be comprehensive and effective.
Adequate	Some improvements are required to enhance the effectiveness of the framework of governance, risk management and control.
Limited	There are significant weaknesses in the framework of governance, risk management and control such that it could be or 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.

Recommendations

Priority	Definition	Action Required
High	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.
Medium	Weakness in governance, risk management and control that if unresolved exposes the organisation to a significant level of residual risk.	Remedial action should be taken at the earliest opportunity and within an agreed timescale.
Low	Scope for improvement in governance, risk management and control.	Remedial action should be prioritised and undertaken within an agreed timescale.