Item: 7.4

Monitoring and Audit Committee: 8 June 2023.

Internal Audit Report:
Disaster Recovery – Information Communications Technology.

Report by Chief Internal Auditor.

1. Purpose of Report

To present the internal audit report on processes and controls relating to Information Communications Technology Disaster Recovery.

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 whether there are adequate and effective disaster recovery arrangements in place which cover all key systems operating within the Council and that roles and responsibilities of officers in relation to disaster recovery are documented and understood, in order to obtain assurance that action has been taken or agreed where necessary.

3. Background

3.1.

The Council places significant reliance on the availability of technology in delivering many of its services. As a result, the ability to respond effectively and efficiently to a disaster which affects infrastructure and applications supported by the Council's Information Communications Technology (ICT) is of paramount importance.

3.2.

Disaster recovery planning is a key function of ICT and digital services. It is essential that robust arrangements are in place, maintained, and tested to ensure that ICT infrastructure and applications can be recovered in the event of a disaster.

3.3.

The objective of this audit was to review whether there are adequate and effective disaster recovery arrangements in place which cover all key systems operating within the Council.

4. Audit Findings

4.1.

The audit provides adequate assurance that procedures and controls relating to the Disaster Recovery are well controlled and managed.

4.2.

The internal audit report, attached as Appendix 1 to this report, includes three medium priority recommendations regarding the software inventory, the development of ICT business continuity and disaster recovery plans. There are no high 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: Disaster Recovery – Information Communications Technology.

Appendix 1

Orkney Islands Council

Internal Audit

Audit Report

Disaster Recovery (ICT)

Draft issue date: 29 March 2023

Final issue date: 17 May 2023

Distribution list:	**Corporate Director Neighbourhood Services and Infrastructure** **Head of Property, Asset Management and Facilities** **Head of Improvement and Performance** **Service Manager ICT**

Contents

Audit Opinion

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

Adequate	**Some improvements are required to enhance the effectiveness of the framework of governance, risk management and control.**

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

Executive Summary

As an organisation significantly reliant on technology in delivering many of its services, it is crucial that the Council has procedures in place to enable the recovery or continuation of key systems following a natural or human-induced disaster. Our audit indicates that there are disaster recovery arrangements in place but there is scope for these to be strengthened and formalised in business continuity and disaster recovery plans.

Our review identified a number of positive areas including:

- The setting up of an off-site disaster recovery data centre.
- The installation of an ‘immutable’ (unchangeable) back up system designed with measures to protect against ransomware cyber-attacks.
- A strong governance structure where resilience, business continuity and recovery are discussed and reported on.
- An awareness of potential risks and vulnerabilities, reflected in the Corporate IT Risk Register and constant activity monitoring.

The report includes 3 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
3	**0**	**3**	**0**

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

Introduction

The Council places significant reliance on the availability of technology in delivering many of its services. As a result, the ability to respond effectively and efficiently to a disaster which affects infrastructure and applications supported by the Council's Information Communications Technology (ICT) is of paramount importance. Failure to do so could result in significant disruption to business activities and reputational damage.

Disaster recovery planning is a key function of ICT and digital services and it is essential that robust and sufficiently detailed arrangements are in place, maintained and tested to ensure that ICT infrastructure and applications can be recovered in the event of a disaster.

Disaster recovery planning involves a set of policies, processes and procedures to enable the recovery or continuation of ICT infrastructure or systems following a failure or disaster. It focuses on the ICT systems that support business critical activities, as opposed to Business Continuity Plans (BCPs) which look at all aspects of keeping a business functioning. As such Disaster Recovery Plans can be considered as a subset of BCPs.

In October 2021, a tabletop exercise based on 'Exercise in a Box', developed by the National Cyber Security Centre was held with the overall aim to expose senior management to the issues that result from a ransomware attack. An action plan was drawn up as a result of the exercise.

On 9 June 2022 an audit report on Council-wide Business Continuity was presented at the Monitoring and Audit Committee. Nine recommendations were identified, including that matters identified from 'Exercise in a Box' should be included within the Council's business continuity plans and that existing Business Impact Analyses within the Council should be reviewed.

On 21 June 2022 the Policy and Resources Committee recommended approval of a Business Continuity Management Policy for the Council, updated to reflect best practice and the new management structure.

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

Audit Scope

The audit reviewed whether there were adequate and effective disaster recovery arrangements in place which covered all key systems operating within the Council and that roles and responsibilities of officers in relation to disaster recovery were documented and understood. It also ascertained if appropriate monitoring and reporting mechanisms were in place.

Audit work included, but was not limited to reviewing that:

- There is appropriate governance in place and policies and procedures exist to provide robust disaster recovery planning.
- All systems are adequately and accurately documented to aid the recovery process.
- There is a regularly reviewed inventory of data assets and business systems which are prioritised for recovery.
- All potential risks to the Council and its ICT facilities are identified and assessed in preparation of contingency arrangements.

- There are, for all critical systems, recovery arrangements in place that are comprehensive, regularly reviewed and appropriately communicated.
- Recovery arrangements are aligned with the Business Continuity Plan and other Council policies and procedures.
- Recovery arrangements are signed off by senior management.
- Recovery arrangements are periodically tested and documentation updated to reflect lessons learned.
- Roles and responsibilities are documented and understood and officers have been suitably trained.
- There are policies and procedures for back-ups, offsite storage and alternative capacity provision.
- Regular Business Impact Analyses are carried out.
- IT customer disaster recovery requirements have been formally captured to understand customer expectations.
- The organisation has insurance coverage for disaster recovery related issues.
- There is a communication plan in place for disaster events.
- Actions arising from ‘Exercise in a Box’ have been addressed.

Audit Findings

1.0 Offsite Disaster Recovery infrastructure

1.1 Disaster recovery usually focuses heavily on IT and technology systems supporting critical business functions. Infrastructure is a key element of this. An important component of disaster recovery arrangements is the provision of a secondary site situated in a different location to the main data centre. The Council has recognised this and set up a secure, remote disaster recovery site with an uninterruptable power supply (UPS). By synchronising IT systems between the two sites data will be protected in the event of a total loss of the Council's main data centre and ensure continuity of operations.

1.2 It is important to understand how systems installed react under various failure conditions. During implementation of the recovery infrastructure various failure scenarios were tested. Future tests and exercises are planned.

2.0 Data Recovery Capability.

2.1 The Council has purchased an immutable back up system. Immutable (or unchangeable) backups are copies of files and data that cannot be altered or tampered with for a pre-set period of time. This is a tiered solution designed to protect against ransomware attacks and adds an additional layer of protection to systems and data.

2.2 Our audit found that there is a schedule of backups covering all servers. This shows the servers that are backed up, the frequency of backups, and the number of restore points (e.g. days retained). Backup data is stored at both datacentre locations ensuring that if one set of backups are damaged another copy is available elsewhere. There are robust security procedures around access to the system and maintenance and support that includes health status monitoring.

3.0 Risk identification and activity monitoring

3.1 In the preparation of contingency and recovery arrangements it is essential that all potential risks to the Council's ICT infrastructure and data are identified and assessed. The Corporate Risk Register identifies the risk of inadequate information security and management and inadequate cyber security. Mitigating Actions include Public Services Network (PSN) accreditation, 'Exercise in a Box' (see section 6.4 below) and the provision of off-site infrastructure. The ICT Service has its own risk register, recognising nine risks of which seven are relevant to disaster recovery, these include physical security, staffing, key system failure, electrical supply failure, weather, cyber security attack and contractual support. Mitigating actions are identified for all risks.

3.2 The monitoring of activities, unusual or otherwise is an important process in reducing the risk of disaster events occurring. The Council commissions an independent IT Health Check on an annual basis. This involves the testing of the Council's perimeter defences, evaluation of firewall, server, network and Wi-Fi configurations and examination of passwords and password policies. A detailed report is issued, and a remediation plan is developed to address any issues arising. Internal Audit has viewed the remediation plan for the 2022 health check and all actions have been marked as complete. Weekly vulnerability testing is carried out to identify any unusual activities. The Council also receives notices and intelligence from a number of agencies.

4.0 ICT Governance

4.1 Due to the level of reliance placed on the availability of ICT, it is important that there are good governance arrangements over this, both to mitigate the likelihood of serious events and to plan for recovery and continuity. A key body is the Information Services Programme Board (ISPB). The ISPB is made up of members of the Corporate Leadership Team, Heads of Service and senior ICT staff and is chaired by the Chief Executive. It meets four times a year to review ICT performance, consider significant change requests, review the ICT Capital Programme and ensure strategic fit working with the Council's Asset Management Strategy. A review of board minutes indicated that items of relevance to disaster recovery were discussed such as the new remote site and the new backup system. Standing items on the agenda include a report on the availability of IT services and cyber resilience. A Change Management Board meets weekly to discuss ICT changes. A Digital Strategy Consultative Group meets as required and includes as part of its remit the need for effective ICT infrastructure and systems to support delivery of the outcomes in the Digital Strategy. The Council is also a member of a number of national initiatives for sharing intelligence.

4.2 Disaster recovery related issues are included in many of the Council's IT strategies and plans. These include the ICT Asset Management Plan which covers the period 2021-26, the IT Strategy 2021-24, the IT Strategy Delivery Plan 2021-24, and the IT Capital Replacement Programme. These are presented and discussed at the Asset Management Sub-committee. Disaster recovery also features in the Digital Strategy which is presented at the Policy and Resources Committee.

5.0 Inventory of ICT infrastructure

5.1 In the event of an emergency situation, it is important to know which systems should be prioritised for recovery. In order for this to be effective it is important to have comprehensive, up to date inventories of hardware and software assets. The Council does have these inventories of which the most relevant to disaster recovery is the inventory of systems. This includes useful information such as whether the system is held on premises, the cloud or both, its importance to the Council, the Council's commitment to the system and whether it is defined as a corporate core system. A review of the inventory indicated that the list was fairly comprehensive, but it was noted that one system likely to be considered of high importance to the Council was not included and at least one was included that is no longer in use. There is also no firm procedure in place to ensure that any new systems are added to the inventory. We have been made aware that work has been ongoing on the inventory but would recommend that procedures are developed to ensure that the completeness of the software inventory is periodically reviewed, new systems are added and systems no longer in use are removed.

Recommendation 1

5.2 The vast majority of the 'back-office' business systems used to support the wide range of Council services are supplied by third party vendors. As part of the audit, six of the systems marked as being a core corporate system of high importance in the inventory were selected to check disaster recovery arrangements. Contracts and Service Level and Maintenance Agreements were reviewed and where necessary arrangements were discussed with administrators and users. Our review found that in an emergency situation robust support arrangements were in place.

5.3 When purchasing new cloud based or remotely hosted systems each system is assessed for security and every hosting supplier is assessed for their security posture, control mechanisms and governance. This is done by means of a detailed Security Questionnaire. This can often be an iterative process and only when the answers are considered satisfactory will a final decision be made.

6.0 Recovery Plans

6.1 Business Continuity Plans look at all aspects of keeping a business functioning after major disruptions or disasters. The Council has a Business Continuity Management Policy which was recommended for approval by the Policy and Resources Committee on 21 June 2022. This requires Corporate Directors and Heads of Service to ensure that all functions within the service areas they lead are within the scope of a recovery plan and business continuity arrangements which are reviewed and exercised regularly. The policy states that Corporate Directors will ensure that Business Continuity Plans exist across their Service areas. The ICT Service currently does not have a Business Continuity Plan.

6.2 An important component of a Business Continuity Plan is a Business Impact Analysis which defines the service's recovery time objective. The ICT Service has carried out a Business Impact Analysis and has ranked each risk to determine the degree of importance and consequence of that system being unavailable for any extended period. The lowest maximum tolerable period of disruption, and the recovery time objective for each activity have been identified. This reflects business criticality and ensures that recovery takes place in the correct sequence after a disaster. However, the analysis is not current and should be reviewed and updated prior to completing the Business Continuity Plan.

Recommendation 2

6.3 It is considered good practice to develop a Disaster Recovery Plan which is usually a subset of the Business Continuity Plan. This formalises and documents the processes and procedures that will ensure that the Council can respond to a disaster or other emergency that affects information systems and minimise the effect on its operations. The ICT Service does not have a Disaster Recovery Plan currently in place although most of the key elements of a plan are outlined in sections one to five above. An ICT disaster recovery plan should be developed.

Recommendation 3

6.4 In October 2021, a tabletop exercise based on 'Exercise in a Box', developed by the National Cyber Security Centre, was carried out. Its specific objectives were to provide awareness of the consequences of a ransomware attack, to determine the best means to prepare for such an attack, to develop a recovery strategy for such an attack and to develop a subsequent action plan. A review of the plan indicated that most actions had been completed with the exception of those relating to the completion of Business Continuity Plans and delivery of 'Exercise in a Box' to all Service Managers. In the Business Continuity Audit carried out in 2022 a recommendation was made that Management should ensure that the 'Exercise in a Box' Action Plan is completed. As work on this is ongoing no further recommendation is required.

6.5 The Council has a Major Emergency Plan which was updated in December 2022. This has some relevance to ICT disaster recovery and sets out how Orkney Islands Council will activate and manage its corporate response to a major emergency that has the potential to impact on the Council's functions. Amongst other things the plan describes roles and responsibilities, communication and media liaison, insurance and recovery. These will be important considerations in the development of a Disaster Recovery Plan.

Action Plan

Recommendation	Priority	Management Comments	Responsible Officer	Agreed Completion Date
1. Procedures should be developed to ensure that the completeness of the software inventory is periodically reviewed, new systems are added and systems no longer in use are removed.	Medium	Ownership of the maintenance of the systems inventory list will sit with Improvement and Performance working closing with IT. The audit action will be to bring the list up to date and put a process in place for its ongoing maintenance.	Service Manager Improvement and Performance	31 March 2024
2. An ICT Business Continuity Plan should be created once the ICT Business Impact Analysis has been reviewed and updated.	Medium	Agreed	Service Manager ICT	31 December 2023
3. An ICT Disaster Recovery Plan should be developed.	Medium	Agreed	Service Manager ICT	31 December 2023

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 high 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.