Item: 6.1

Monitoring and Audit Committee: 10 June 2021.

Internal Audit Report: IT Security – Remote Working.

Report by Chief Internal Auditor.

1. Purpose of Report

To present the internal audit report on procedures and controls relating to IT security for remote working.

2. Recommendations

The Committee is invited to note:

2.1.

That Internal Audit has undertaken an audit of the procedures and controls in place within the Council relating to IT security for remote working.

2.2.

The findings contained in the internal audit report, attached as Appendix 1 to this report, relating to the procedures and controls in place within the Council relating to IT security for remote working.

It is recommended:

2.3.

That the Committee review the audit findings to obtain assurance that action has been taken or agreed where necessary.

3. Background

3.1.

In response to the COVID-19 pandemic, the IT Service was required to roll out remote working so that the Council could continue to provide essential and non-essential services to the public. Due to the large number of employees now working remotely there is an increased cybersecurity risk.

3.2.

The objectives of this audit were to confirm that there are adequate processes and controls in place to ensure that the Council's systems and information are protected from unauthorised access, phishing emails and scams, and that any suspected breaches are reported and investigated.

4. Audit Findings

4.1.

The audit provides substantial assurance that the processes and procedures relating to IT security for remote working are well controlled and managed.

4.2.

The internal audit report, attached as Appendix 1 to this report, includes one low priority recommendation within the action plan. There are no high or medium level recommendations made as a result of this audit.

4.3.

The Committee is invited to review 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 Officers

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

Karen Rorie, Internal Auditor, email karen.rorie@orkney.go.uk

9. Appendix

Appendix 1: Internal Audit Report: IT Security - Remote Working.

Appendix 1

ORKNEY ISLANDS COUNCIL

Internal Audit

Audit report **IT Security – Remote Working** **Draft issue date: 18 May 2021** **Final issue date: 28 May 2021**	
Distribution list:	**Executive Director of Development & Infrastructure** **Head of IT and Facilities** **Information Security and Assurance Officer** **Information Governance Officer**

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

This audit reviewed the IT security controls in place for remote working to ensure they are sufficient to keep the Council's data and systems safe from unauthorised access.

Our review provides substantial assurance that controls are in place and operating well.

Several areas of good practice were identified during the audit including:

- There are a number of comprehensive policies and procedures in place for remote working including a Remote Working Support Guide, Working from Home Guidance and Information Security Guidance. These are communicated to all staff.
- Mandatory IT Security online training is required to be completed annually by all computer users.
- Staff are informed about keeping data safe while working remotely.
- All devices provided for remote working have security built in and firewalls, anti-virus and automatic updates all configured.
- There are remote access security monitoring procedures in place to detect any potential unauthorised systems activity.
- There are cloud-based back-ups provided by Microsoft to ensure all data is backed up while working remotely.
- Employees are advised of current security threats of phishing emails and scams and the signs to look out for as well as how to report a data breach.

The report includes one recommendation which has arisen from the audit. The priority of the recommendation is 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 action via Pentana Risk.

Total	High	Medium	Low
1	**0**	**0**	**1**

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

Introduction

With remote working, there are real cybersecurity issues that put any organisation's sensitive data at risk. Protecting data when staff are working outside of their normal office environment is therefore critical and requires an IT security policy and procedures that apply specifically to remote workers.

There is an increased risk to cybersecurity while large numbers of employees work from home due to the restrictions in place from the COVID-19 pandemic. In response to the pandemic, the IT service was required to very quickly roll out remote working to all staff whose job facilitated it so that the Council could continue to provide essential and non-essential services to the public.

This review was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing.

Audit Scope

The scope of this audit was:

- To confirm that there are procedures in place for IT security in remote working which are communicated to all staff.
- To confirm that guidance is provided to staff on keeping data secure from unauthorised access while working remotely.
- To confirm that there is an adequate level of remote access security in place which incorporates a secure physical location for primary servers and prevents or detects unauthorised remote connections.
- To confirm that staff are provided with software to ensure their critical documents are backed up while working remotely.
- To confirm that there is a defined remote access request and authorisation process in place which is designed to ensure only authorised users are granted remote access to systems.
- To confirm that there are procedures in place for any actual or suspected data breaches.
- To confirm that there is a process in place to remind employees of the threats of phishing emails and scams to ensure they are alert to the risks.

Audit Findings

1.0 Defined Remote Access Request and Authorisation Process

1.1 There is a defined process in place for the provision of remote access requests. However, this process has not been set out formally in writing.

1.2 A written procedure should be produced which sets out the defined process to be followed for remote access requests and the authorisation thereof.

Recommendation 1

Action Plan

Recommendation	Priority	Management Comments	Responsible Officer	Agreed Completion Date
1 A written procedure should be produced which sets out the defined process to be followed for remote access requests and the authorisation thereof.		Comment Accepted in full	Head of IT and Facilities	30 June 2021

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.