Item: 11.2

Orkney and Shetland Valuation Joint Board: 2 March 2023.

Internal Audit of IT Network and Security.

Report by Chief Internal Auditor.

1. Purpose of Report

To present the IT Network and Security Audit Report for Members' scrutiny.

2. Recommendations

It is recommended:

2.1.

That the Board scrutinises the findings of the internal audit relating to a review of the IT Network and Security arrangements, attached as Appendix 1 to this report, in order to obtain assurance that action has been taken or agreed where necessary.

3. Background

3.1.

The Orkney and Shetland Valuation Joint Board (the Board) holds information for various purposes, including valuing properties in Orkney and Shetland, to compile the non-domestic rating Valuation Roll, the Council Tax Valuation List and to maintain the Register of Electors.

3.2.

The Assessor and Electoral Registration Officer is the data controller for the Board. The respective islands Councils, who hold and process personal data, are defined as data processors who act on behalf of the data controller.

3.3.

The objective of this audit was to review the Board's IT network and cyber security arrangements, including data governance and compliance with data protection legislation.

4. Audit Findings

4.1.

The audit provides adequate assurance that the processes and procedures relating to the IT Network and Security are well controlled and managed.

4.2.

The internal audit report, attached as Appendix 1 to this report, includes one medium priority recommendation regarding IT service level agreements, and seven low priority recommendations regarding security policies, confirmation statements, the data protection officer, the records management plan and physical security arrangements. There are no high level recommendations made as a result of this audit.

5. Financial Implications

There are no financial implications associated directly with this report.

6. Governance Aspects

The content and implications of this report have been reviewed and, at this stage, it is deemed that the Board **DOES NOT** require external legal advice in consideration of the recommendations of this report.

7. Contact Officer

Andrew Paterson, Chief Internal Auditor, Telephone 01856 873535 extension 2107, Email andrew.paterson@orkney.gov.uk

8. Appendix

Appendix 1: IT Network and Security Audit Report.

Orkney & Shetland Valuation Joint Board

Internal Audit

Audit Report **IT Network and Security** **Draft issue date:** 16 January 2023 **Final issue date:** 10 February 2023	
Distribution list:	**Assessor & Electoral Registration Officer for Orkney & Shetland** **Data Protection Officer to the VJB** **Clerk to the VJB** **Treasurer to the VJB**

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

The objective of this audit was to review the Orkney and Shetland Valuation Joint Board's (VJB) IT network and cyber security arrangements including Data Governance and compliance with data protection legislation.

The VJB holds information for various purposes, including valuing properties in Orkney and Shetland, to compile the non-domestic rating Valuation Roll, the Council Tax Valuation List and to maintain the Register of Electors.

Electronic data is held on networks managed by either Orkney Islands Council or Shetland Islands Council and paper records are held at offices located in Kirkwall and Lerwick.

The Assessor for Orkney & Shetland and Electoral Registration Officer (the Assessor) is the data controller for the VJB. Data controllers exercise overall control over the purpose and means of processing personal data. The respective islands Councils who hold and process personal data are defined as data processors who act on behalf of the data controller.

The VJB has policies relating to data retention, data security and special category data. It also has record retention and disposal schedules for the data it holds. The VJB provides privacy notices as required to do so.

The report includes 8 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
8	**0**	**1**	**7**

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

Introduction

The Assessor and Electoral Registration Officer is responsible for preparing and maintaining three main documents, these are:

- The Valuation Roll which sets out the rateable value of all non-domestic properties. The valuations are used by the constituent local authorities as the base for collecting non-domestic rates.
- The Council Tax Valuation List which shows the council tax valuation band of every dwelling and is used by the constituent local authorities as a base for determining and collecting Council Tax.
- The Register of Electors which contains details of everyone who has registered to vote at parliamentary and local elections. Since 2003, two versions of the electoral register have been produced, the full version and the edited version (also known as the open register).

All three of these documents are available for public inspection at the Assessor's offices, and at public libraries.

The Data Protection Act 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998 and came into effect on 25 May 2018. It was amended on 1 January 2021 by regulations under the European Union (Withdrawal) Act 2018 to reflect the UK's status outside the EU.

The UK GDPR is the UK's General Data Protection Regulation. It is a UK law which came into effect on 1 January 2021. It sets out the key principles, rights and obligations for most processing of special category, (i.e., sensitive) personal data in the UK.

The VJB should be using a risk-based approach to justify how and why it uses personal data.

When the VJB shares data with either Orkney or Shetland Islands Council, or other bodies, this should be in conformance with Data Sharing Agreements in place.

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

Audit Scope

The Scope of this audit included a review of the VJB's processes and controls, in particular its compliance to the seven key principles of the UK GDPR, these are:

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage Limitation.
- Integrity and confidentiality (security).
- Accountability.

Audit Findings

1.0 Policy and Procedures

1.1. The VJB's Data Security policy documents state that both offices of the Board have Service Level Agreements (SLAs) with their respective constituent councils.

1.2. Both Shetland and Orkney Islands Councils have a service level agreement document which applies to all users of Information Communication Technology (ICT) provided by the constituent Council. Neither document refers specifically to the VJB and is not signed by either party.

1.3. The purpose of an ICT Service Level Agreement includes ensuring that the following is provided:

1.3.1 Firewall and virus-checking on all computers and servers.
1.3.2 The operating system is set up to receive automatic updates.
1.3.3 Protection by updating all computers by downloading the latest patches or security updates.
1.3.4 Regular back-ups of the information on the file servers are taken.
1.3.5 Anti-spy ware to help protect computers from spy ware threats.

1.4. Both constituent Councils have their own IT security policies and although the absence of an agreed and signed ICT SLA is not a cause to believe the services listed within 1.3 are not being provided, it is recommended that ICT services provided by the constituent councils are formalised within an agreed and signed SLA.

Recommendation 1

1.5. A recent meeting between the Assessor and the Shetland Islands Council's ICT projects and analyst officer took place on 15 August 2022 which included discussion around the provision of ICT services to the Shetland Office. It would be good practice for SLA agreements with the constituent councils to provide for regular confirmation statements of compliance to be provided to the VJB.

Recommendation 2

1.6. The VJB's suite of policies for data retention, data security, and special category data do not include a timescale for review. The policies do not show any signs of having been reviewed since their introduction on 25 May 2018.

1.7. The VJB's report to the Keeper of the Records of Scotland, dated 31 July 2017 refers to several policy documents which are not included within the list of policies on the VJB's website, these being:

- Information Security Policy.
- Security Incident and Weakness Policy.
- Acceptable Use Policy.
- Physical and Environmental Security Policy.
- Access Control Policy.
- Backup and Restore Policy.
- Data Access and Building Security Policy.
- Security of IT Systems staff guidance document.

- Business Continuity Plans.
- Disposal of Media and Secure Disposal and Re-use of Equipment procedural documents.

1.8. The VJB's suite of data security and protection policies should be reviewed and updated to current legislation and include required timescales for their regular review.

Recommendation 3

2.0 Data Protection Officer

2.1 A specific requirement from legislation is that the VJB must publish the contact details of the Data Protection Officer and communicate these to the Information Commissioner's Office.

2.2 The name and contact details of the Data Protection Officer have been communicated to the Information Commissioner's Office but could not be found on the VJB website.

2.3 It is recommended that the contact details of the VJB Data Protection Officer should be shown on its website.

Recommendation 4

2.4 The VJB appointed the Head of Legal and Governance at Orkney Islands Council to be its Data Protection Officer at its meeting of 26 June 2018. The Board considered, inter alia, the tasks of the Data Protection Officer and assessed his role at Orkney Islands Council would present no conflict of interest in relation to his proposed appointment as Data Protection Officer to the Valuation Joint Board. The Data Protection Officer does not have a formal engagement agreement with the VJB. It is good practice, in situations where the Data Protection Officer is not under a contract of employment with the organisation to have a formal engagement agreement in place for the performance of this role. It is recommended that a simple agreement be drawn up between the VJB and its Data Protection Officer.

Recommendation 5

3.0 Records Management Plan

3.1 The most recent version of the VJB's Records Management Plan (the plan) which has received the approval of the Keeper of the Records of Scotland, was submitted to the National Records of Scotland during January 2017. The Keeper recommended that Orkney and Shetland Valuation Joint Board should publish its agreed Records Management Plan (RMP) as an example of good practice within the authority and the sector.

3.2 Applying a red, amber, green (RAG) system, the Keeper graded ten elements of the plan as green (noting his agreement), three elements as amber (noting his agreement to the element as an "improvement model"), and one element as not applicable due to the fact that the VJB does not generally share records with third parties unless there is legal requirement to do so.

3.3 The three elements, rated as amber, relate to the following:

3.3.1 Records Management.
3.3.2 Destruction Arrangements.
3.3.3 Audit Trail.

3.4 The Keeper agreed to the Records Management element of the plan under improvement model terms while awaiting (at the time) the appointment of an Assistant Assessor.

3.5 The VJB has identified the Assessor as the individual with overall responsibility for records management in the authority and the Assistant Assessor as the individual with day-to-day responsibility for implementing the plan.

3.6 The Keeper's guidance makes clear that it is possible (although unusual) under the Act for one individual to be identified in both roles and therefore may be a short-term solution. Due to the size of the VJB, covering a vacancy in either position will remain an ongoing risk.

3.7 The Keeper agreed the VJB's Destruction Arrangements element of the plan under improvement model terms. The Plan states under 'Element 6 Future Developments': "Consideration is currently being undertaken regarding the management and deletion of electronic records and their retention. These records should be deleted in accordance with this policy when it is finalised, and it will include reference to the same limits detailed in the Records Retention and Disposal Arrangements Schedule". The Keeper required a copy of this policy when it became available.

3.8 The plan also states that "Further consideration is being given to the possibility of an automated deletion of records being incorporated into the Board's IT system, which would ensure the timely destruction of those records deemed to have passed their retention date". The Keeper commented that the controlled and systematic deletion of records held on shared drives is a particular area of difficulty for many public authorities and the Keeper welcomed the acknowledgement of this. The Keeper agreed that the suggested improvements the Board were considering, were a reasonable response to these difficulties. The aspiration of the VJB to be operating an automated system to ensure record retention and disposal has recently been discussed at team meetings.

3.9 The Keeper agreed to the Audit Trail element of the Records Management element of the plan under improvement model terms. Within the plan the VJB stated that "for paper files a simple logging out sheet requires to be implemented for paper property records which will be added to the senior management's remit". The Keeper agreed to this action. Our audit found that hard-copy files are rarely removed from the offices, however the logging out sheets have not been in use since the commencement of Covid i.e., March 2020.

3.10 The Keeper also acknowledged that IT systems operated by the VJB will have documented tracking functionality built in, however they noted that public records held on shared drives will require manual input following imposed naming conventions. The Keeper suggested that, for these records, version control and naming convention guidance should be created and disseminated to all staff. The Assessor acknowledged this recommendation. Our review has found that the VJB has not implemented naming procedures or version control procedures.

3.11 It is recommended that the VJB reviews whether each of the commitments made within, and as a result of the plan have been embedded into processes and implement any remaining required improvements.

Recommendation 6

3.12 It is recommended that following revision of Policies and Procedures within the VJB, staff should be updated on any significant revisions made and reminded of Office Security Rules within the VJB's Data Security Policy.

Recommendation 7

4.0 Office Security

4.1 A site visit of the Office at Kirkwall was carried out. Access by the front door is locked overnight but allows open access during the day. No data is held on the ground level however there is a kitchen, toilet, and rooms where there is no visibility to whether persons may be entering or remaining in this area. The main offices are on the first floor, some data, such as personnel records is held in a locked cabinet. For two of the Offices and one storage area there are no keys for the locks. Several of the cabinet files similarly do not have keys to the locks. Office doors do not provide visibility into the room and although offices are relatively small, the risk of accidently locking a person in a room should be mitigated. Our review did not include a physical review of the Lerwick Office.

4.2 It is recommended that office doors and cabinet files at the Kirkwall Office should have keys or alternative security arrangements such as code lock entry devices.

Recommendation 8

Action Plan

Recommendation	Priority	Management Comments	Responsible Officer	Agreed Completion Date
1) ICT services provided by both constituent councils should be formalised within signed SLA agreements.	Medium	Agreed – The existing SLA with OIC and SIC will be reviewed and amended to include signatures.	The Assessor and Electoral Registration Officer	31/03/2023
2) Service level agreements with the constituent councils should provide for regular confirmation statements of compliance to be provided to the VJB.	Low	Agreed – Arrangements for this will be incorporated into the new SLAs.	The Assessor and Electoral Registration Officer	31/03/2023
3) The VJB's suite of data security and protection policies should be reviewed and updated to current legislation and provide required timescales for their regular review.	Low	Agreed – Current policies appear substantively complete, but will require some updates, although these are likely to be relatively minor in scope. Data security and protection policy review periods should be fixed at a maximum of three years.	The Assessor and Electoral Registration Officer in conjunction with the VJB's DPO.	30/06/2023
4) The contact details of the VJB Data Protection Officer should be shown on its website.	Low	Agreed – website now updated.	The Assessor and Electoral Registration Officer	Action Completed
5) A simple service agreement should be drawn up between the VJB and its Data Protection Officer.	Low	Agreed – A service agreement between the VJB and its Data Protection Officer has now been put into place.	The Assessor and Electoral Registration Officer in conjunction with the VJB's DPO.	Action Completed

Recommendation	Priority	Management Comments	Responsible Officer	Agreed Completion Date
6) The VJB should review whether each of the commitments made within, and as a result of the records management plan have been embedded and develop an action plan to implement the remaining required improvements.	Low	Agreed – It is envisaged that the VJB will be invited to submit a Progress Update Review (PUR) in 2023 to National Records of Scotland. This will consist of a root and branch review of the previously submitted Records Management Plan ensuring that existing and planned records management arrangements are up to date and relevant.	The Assessor and Electoral Registration Officer in conjunction with the VJB's DPO.	31/03/2024
7) Following revision of Policies and Procedures within the VJB, staff should be updated on any significant revisions made and reminded of required practices to data security and protection.	Low	Agreed – Communications bulletin will be produced to highlight requirements for both digital and physical data security practices and provide a link to the updated policies for staff to access. In addition, bespoke online training will be delivered to VJB staff. Staff currently undertake mandatory Data Protection training and receive Council updates on cyber security.	The Assessor and Electoral Registration Officer in conjunction with the VJB's DPO.	31/08/2023
8) Office doors and cabinet files should have keys or alternative security arrangements such as code lock entry.	Low	Agreed – Arrangements are being made to install code lock entry systems to individual office doors in the Kirkwall Office. Replacement keys are being sourced to ensure all existing cabinets and cupboards used for document storage can be locked.	The Assessor and Electoral Registration Officer	01/05/2023

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.