HIGHLAND AND WESTERN ISLES VALUATION JOINT BOARD

20 June 2024

Agenda Item	**8a**
Report No	**VAL/8/24**

Internal Audit Report – Information Management Arrangements

Report by Strategic Lead (Corporate Audit & Performance), Highland Council

Summary

Details are provided of the audit review of Information Management Arrangements and a copy of the report is attached.

Internal Audit Reports

Every Internal Audit report issued contains an audit opinion based upon the work performed in respect of the subject under review. There are five audit opinions which can be provided:

(i) Full Assurance: There is a sound system of control designed to achieve the system objectives and the controls are being consistently applied.

(ii) Substantial Assurance: While there is a generally a sound system, there are minor areas of weakness which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

(iii) Reasonable Assurance: Whilst the system is broadly reliable, areas of weakness have been identified which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

(iv) Limited Assurance: Weaknesses in the system of controls are such as to put the system objectives at risk, and/ or the level of non-compliance puts the system objectives at risk.

(v) No Assurance: Control is generally weak, leaving the system open to significant error or abuse, and/ or significant non-compliance with basic controls leaves the system open to error or abuse.

Since the last update to the Board there has been one audit report issued relating to a review of Information Management Arrangements. This report has the audit opinion of “Reasonable Assurance” as a number of areas for improvement were identified. As a result, the report contains 6 recommendations comprising of 5 medium and 1 low grade priorities.

Recommendation

The Board is asked to consider the Internal Audit findings and audit opinion provided, and to raise any relevant points with the Strategic Lead (Corporate Audit & Performance).

Designation: Strategic Lead (Corporate Audit & Performance)

Date: 6th June 2024

Author: Donna Sutherland, Strategic Lead (Corporate Audit & Performance), Highland Council

The Highland Council
Comhairle na Gàidhealtachd

Internal Audit Final Report

Office of the Assessor and Electoral Registration Officer

Information Management Arrangements

Description	Priority	No.
Major issues that managers need to address as a matter of urgency.	High	0
Important issues that managers should address and will benefit the Organisation if implemented.	Medium	5
Minor issues that are not critical, but managers should address.	Low	1

Audit Opinion

The opinion is based upon, and limited to, the work performed in respect of the subject under review. Internal Audit cannot provide total assurance that control weaknesses or irregularities do not exist. It is the opinion that **Reasonable Assurance** can be given in that whilst the system is broadly reliable, areas of weakness have been identified which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

Distribution:
Assessor and Electoral Registration Officer
Depute Electoral Registration Officer / Business Manager

Report Ref:	ASS03/001
Draft Date:	21/12/23
Final Date:	12/02/24

1. Introduction

1.1 The core functions of the Office of the Assessor and Electoral Registration Officer (ERO) are the compilation and maintenance of the Valuation Roll and the Council Tax Valuation List and the preparation and publication of the Register of Electors. Staff are based at sites in Inverness, Wick and Stornoway. Information technology assets, systems and services are provided and maintained in partnership with Highland Council (HC) ICT Services.

1.2 The audit examined the policies and procedures in place to manage both physical and electronic information to ensure that they are complete, up to date and have been communicated to all staff. Training provided to staff in this area was also reviewed to determine whether it had been undertaken by all relevant staff.

The audit also looked at whether the risks surrounding information management (IM) had been identified, documented, and assessed and whether there are appropriate mitigating actions in place to manage these.

The systems and controls in place to support IM were assessed to ensure that they are effective, applied consistently and comply with applicable statutory obligations.

2. Main Findings

2.1 *Policies and procedures*

This objective was substantially achieved. All of the expected policy documents were in place with the exception of information security which is covered by the HC Information Security & Assurance Policy. All policies were reviewed and updated as part of the annual review of the Records Management Plan which is a requirement of The Public Records (Scotland) Act 2011. A Progress Update Review was submitted to the Keeper of Records Scotland (the Keeper) as part of the annual review.

There was no information asset register in place, but this will form part of the revised Records Retention Schedule (see 2.4).

2.2 *Staff awareness*

This objective was partially achieved which means there is a risk that not all staff are aware of relevant policies and practices and the role they play in effective IM.

Staff awareness of IM was promoted in the following ways:

- Staff induction.
- Mandatory e-learning course.
- Policies stored centrally on SharePoint.
- Staff informed by email when changes are made.

There had been 4 new starts since 01/04/23 and all had received an induction. All staff were required to complete the IM module on the HC Traineasy online learning system. Completion of mandatory training was recorded on a spreadsheet, and this was periodically cross-referenced with information provided by HC People Development to ensure it was accurate and up to date. Out of 78 employees listed on payroll records, 58 (74%) had completed the IM training. The following points were noted:

- Good information management practice requires all staff who handle personal or sensitive information to be appropriately trained in order to manage the associated risk.
- The training record maintained by the Assessor was last checked against HC People Development records on 08/02/23.
- Temporary staff members (only one at time of audit) were not required to complete mandatory training.
- 17 out of 20 Electoral Canvassers have not completed the training as they don't generally have access to the HC network and therefore Traineasy.
- Mandatory training was only carried out once and is not refreshed periodically.

See action plan M1.

2.3 *Risk management*

This objective was partially achieved which increases the likelihood of incidents occurring such as data breaches, identity theft, loss of intellectual property, and reputational damage. Risks relating to data accessibility, data security and data management were recorded on the Risk Register. The Risk

Register was reviewed at monthly management team meetings and a Risk Profile Review report was periodically put before meetings of the Highland and Western Isles Valuation Joint Board.

The risks associated with IM on the Risk Register (references 2, 4, 5 and 7) were examined and a number of mitigating actions were not up to date (date of completion/review date now in the past) or required further consultation with HC ICT Services before an update can be provided (see action plan M2).

2.4 *Systems and controls*

This objective was partially achieved which could increase the risk of information not being protected from unauthorised access, use, disclosure, disruption, modification, or destruction. Information was held on electronic systems which allow data to be easily interrogated:

- Electoral Section – Elector8
- Assessors Section – Corona A2K
- Central Admin – Corona Personnel Database.

Information was also stored on shared drives which have a structured folder system, but work is underway to move this data to SharePoint. Where paper documentation was received, this was scanned and uploaded to the relevant electronic record. For electoral information, it was kept in a locked cabinet for 13 months and then securely shredded. For the Assessors Section, all paper documentation was held in the corresponding physical property file. There is currently an ongoing exercise to digitise these files, following which they are securely shredded, and physical files were no longer created for new properties.

The Records Retention Schedule was currently being worked on and a draft version had been provided to the Keeper as part of this year’s review (see 2.1). In the meantime, some document disposal was carried out but not always in line with the current Records Retention Schedule (see action plan M3).

IM practices are compliant with the HC Information Security & Assurance Policy in all key areas apart from:

- Clear Desk and Clear Screen Policy – there was no formal policy, but staff were aware that screens should be locked when they are away from their desks and desks tend to be clearer now with the move to hybrid working and hot desking (see action plan L1).
- Vulnerability Assessment and Penetration Testing – One of the systems used, Elector8, is a cloud hosted platform managed by a third-party vendor and was therefore not within the scope of the HC annual PSN Health Check and quarterly vulnerability scans (see action plan M4). In line with ICO guidance, ERO should seek from the software provider and review independent assurances to assist in verifying the security of the software provision.
- Mobile and Flexible Working – there was no formal policy, and this could lead to inconsistent practices by staff therefore increasing the risk of information theft, fraud or a security breach caused by sensitive information being left unattended and in plain view. (see action plan L1).

The ERO Data Protection Policy was in line with the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR), and appropriate action was taken to ensure that data protection legislation was adhered to.

Business continuity planning ensures the ongoing availability of key information in the event of an unplanned event and therefore should be taken into account to support business needs. There was a 'Business Continuity Plan in the Event of Information Systems Failure' document (BCP), the purpose of which was to identify the key risks which threaten critical computer systems and detail the measures in place to mitigate the effects of failure in any part of the system which may have an adverse effect on business continuity. A test exercise had not been carried out to ensure that it was fit for purpose, although a meeting had been requested with HC ICT Services to discuss how this might be undertaken (see action plan M5). There was therefore a risk that critical functions could be adversely affected in the event of an unplanned event.

3. Conclusion

3.1 There were established systems and controls in place to support effective IM and further improvements had been made by the

Depute Electoral Registration Officer/Business Manager who took over the role of Records Manager in early 2023. Annual updates provided to the Keeper allow for greater scrutiny of the IM arrangements in place and mean that policies were regularly reviewed and updated. There was a good awareness amongst staff of the basic principles of IM, including information security.

There was a reliance on HC ICT Services for aspects of information security and this was reflected in the Risk Register and BCP. However, both of these require to be reviewed and updated to include more detail on how these plans would work in practice.

4. Action Plan

					Implementation	
Ref	**Priority**	**Finding**	**Recommendation**	**Management Response**	**Responsible Officer**	**Target Date**
M1	Medium	Staff training is a critical part of ensuring IM arrangements operate effectively. However, review of training showed that: • Out of 78 employees listed on ResourceLink, 58 had completed the IM training. • The training record maintained by the Assessor was last checked against HC People Development records on 08/02/23. • Temporary staff members are not required to complete mandatory training. • 17 out of 20 Electoral Canvassers have not completed the training as they don't generally have access to the Councils Network and therefore Traineasy. • Mandatory training is only carried out once and is not refreshed periodically.	A review of the way in which mandatory training is delivered and monitored should be carried out (in consultation with HC People and Development) and the following points should be considered: • More regular monitoring of mandatory training completion (options for doing this in Traineasy should be explored) • The requirement for all staff who handle information to complete the mandatory training (including temporary staff and Electoral Canvassers). • The requirement to refresh mandatory training periodically.	The use of Traineasy to monitor training and other functions such as review of policies will be explored in the coming months once a full management team is in place in March 2024. Ways of delivering training to Electoral Canvassers was explored in June 2023 with the Depute ERO being presented with some different options from HC which has to be explored further. Through the use of Traineasy, it is hoped that a process to refresh mandatory training can be set up with automatic e-mails generated to VJB employees.	Depute ERO & Business Manager / Management Team	31/10/24
M2	Medium	A number of mitigating actions in the Risk Register were not up to date or require further consultation with HC ICT Services before an update can be provided.	The mitigating actions for Risk Register reference numbers 2, 4, 5 and 7 should be refreshed to reflect an updated date of completion/review and further detail from HC ICT Services.	A meeting has been arranged with the Head of ICT and Digital Transformation has been set up for the beginning of February 2024. These points will be raised at that meeting. Any updates to the risk register will be presented at the next available Board meeting.	Assessor & ERO / IT Systems Manager	30/06/24

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	Target Date
M3	Medium	Some document disposal was carried out but not always in line with the current Records Retention Schedule.	The revised Record Retention Schedule should be finalised and from the date of approval, arrangements made to ensure that all records are managed in line with the Records Retention and Disposal Policy and the Record Retention Schedule.	The Records Retention and Disposal Schedule will be prioritised in the coming months. The Assessor has advised the Keeper that a voluntary updated Records Management Plan will be submitted in summer/autumn 2024.	Depute ERO & Business Manager / Management Team	31/10/24
M4	Medium	The Elector8 system is not within the scope of the HC annual PSN Health Check and quarterly vulnerability scans. In line with ICO guidance, ERO should seek from the software provider and review independent assurances to assist in verifying the security of the software provision.	In line with ICO Guidance on the use of cloud computing, sufficient guarantees about the technical and organisational security measures governing the processing carried out and the steps to ensure compliance with those measures should be sought from the system provider. Any such measures should be included within the contract arrangement with the third-party provider.	The ERO will be migrating to a new Cloud Hosted Provider in February 2024. As part of the new contract, this point will be raised and covered.	Depute ERO & Business Manager	31/05/24
M5	Medium	Business continuity planning ensures the ongoing availability of key information in the event of an unplanned event and therefore should be taken into account to support business needs. There was a BCP, but it only covers information systems failure and does not look at all potential impacts of an unplanned event. A test exercise had not been carried out to ensure that the BCP was fit for purpose, although a meeting had been requested with HC ICT Services to discuss how this might be undertaken.	The BCP should be updated to set out how critical business functions and their key information requirements would be restored in the event of all implications of an unplanned event e.g., staff shortages, loss of key staff, ICT failures, loss of utilities or damage to infrastructure/ buildings. A test exercise should then be carried out to ensure that the updated BCP is fit for purpose.	An update to the BCP will be carried out with presentation to a future Board meeting. With the appointment of new members of the management team, it is hope that this can be progressed quite quickly. A test exercise will be carried out and any action points noted/resolved.	Depute ERO & Business Manager / Management Team	30/09/24

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	Target Date
L1	Low	There was no Clear Desk and Clear Screen or Mobile and Flexible Working Policy within the Assessor & ERO's office. This could lead to inconsistent practices by staff therefore increasing the risk of information theft, fraud or a security breach caused by sensitive information being left unattended and in plain view.	A Clear Desk and Clear Screen Policy and a Mobile and Flexible Working Policy should be put in place (in line with guidance set out in the HC Information Security & Assurance Policy).	These points will be raised with the management team in March 2024. Policies will be presented at a future Board meeting.	Depute ERO & Business Manager	31/10/24