CLACKMANNANSHIRE COUNCIL

Report to: Audit & Scrutiny Committee

Date of Meeting: 24 October 2024

Subject: Internal Audit Progress Report

Report by: Internal Audit Manager

1.0   Purpose

1.1   This report provides an update on progress with completion of the 2024/25 Internal Audit Plan.

2.0   Recommendations

2.1   It is recommended that the Committee notes the progress being made with completion of the 2024/25 Internal Audit Plan.

3.0   Progress with Completion of the 2024/25 Internal Audit Plan

3.1   The 2024/25 Internal Audit Plan was agreed by Audit and Scrutiny Committee on 13 June 2024. It set out 15 assignment areas to be completed by the team during the year. This includes 9 audit reports to be issued to Clackmannanshire Council (those 9 audit reports do not include those assignments or reports undertaken and issued to the Clackmannanshire and Stirling Integration Joint Board or the Central Scotland Valuation Joint Board). Of these 9 audit reports:

- 2 audit reports have been completed to final report stage (as part of our committed assignment programmes of work);

- 2 audit reviews are currently in progress and will be reported to a future Committee; and

- 5 have not been started.

3.2   A summary of progress is set out at Appendix 1. Details on the scope of, and findings arising, from the two reviews finalised are at Appendix 2. The assurance is provided in line with the definitions at Appendix 3.

4.0   Conclusions

4.1   2024/25 Internal Audit work will contribute to a balanced and evidenced based year end opinion on arrangements for risk management, governance, and control.

5.0 Sustainability Implications

5.1 None Noted.

6.0 Resource Implications

Financial Details

6.1 The full financial implications of the recommendations are set out in the report. This includes a reference to full life cycle costs where appropriate. Yes ☐

6.2 Finance have been consulted and have agreed the financial implications as set out in the report. Yes ☐

Staffing

6.3 No implications other than those set out in the report.

7.0 Exempt Reports

7.1 Is this report exempt? Yes ☐ (please detail the reasons for exemption below) No ☐

8.0 Declarations

8.1 The recommendations contained within this report support or implement our Corporate Priorities and Council Policies.

(1) **Our Priorities** (Please double click on the check box ☑)
Clackmannanshire will be attractive to businesses & people and
ensure fair opportunities for all ☐
Our families; children and young people will have the best possible
start in life ☐
Women and girls will be confident and aspirational, and achieve
their full potential ☐
Our communities will be resilient and empowered so
that they can thrive and flourish ☐

(2) **Council Policies**
Complies with relevant Council Policies ☒

9.0 Equalities Impact

9.1 Have you undertaken the required equalities impact assessment to ensure that no groups are adversely affected by the recommendations?

Yes ☐   No ☐

10.0 Legality

10.1 It has been confirmed that in adopting the recommendations contained in this report, the Council is acting within its legal powers.　　Yes ☐

11.0 Appendices

11.1 Please list any appendices attached to this report. If there are no appendices, please state "none".

- Appendix 1: Internal Audit Plan 2024/25 Progress at 01 October 2024

- Appendix 2: Internal Audit Plan 2024/25 Assignment Outcomes Summary of Key Findings from Assignments Complete to Final Report Not Previously Reported to Committee

- Appendix 3: Definition of Internal Audit Assurance Categories

12.0 Background Papers

12.1 Have you used other documents to compile your report? (All documents must be kept available by the author for public inspection for four years from the date of meeting at which the report is considered)

Yes ☐ (please list the documents below)　No ☐

Author(s)

NAME	DESIGNATION	TEL NO / EXTENSION
Isabel Wright	Internal Audit Manager	01324 506342

Approved by

NAME	DESIGNATION	SIGNATURE
Chris Alliston	Strategic Director Partnership and Performance	███████████

INTERNAL AUDIT PLAN 2024/25

Progress at 01 October 2024

	Client / Directorate	Assignment	Status
Annually Recurring Assignments			
1.	All Directorates	National Fraud Initiative	**Ongoing**
2.	All Directorates	Continuous Auditing	**Ongoing**
3.	Place	Climate Change Act Public Body Duties Audit	**In Progress**
4.	All Directorates	Consultancy Work	**Ongoing**
5.	All Directorates	Work on Recommendations Outstanding	**Ongoing**
6.	Internal Audit	Public Sector Internal Audit Standards: Self Assessment	**Ongoing**
7.	All Directorates	Validation Work Requests	**Ongoing**
Committed Assignments			
8.	Partnership and Performance / All Directorates	IT and Information Security Governance	**Final Report Issued**
9.	People	School Admissions Policy	**Final Report Issued**
10.	Partnership and Performance / All Directorates	Community Benefits	Not Started
11.	Partnership and Performance / People	Follow Up of the Review of Leisure Banking	Not Started
12.	People / All Directorates	Follow Up of the Review of Purchase Order Arrangements at Clackmannanshire for Adult Social Care	Not Started
13.	All Directorates	Follow Up of Grade 1 Recommendations	Not Started

	Client / Directorate	Assignment	Status
14.	Partnership and Performance / All Directorates	Capital Arrangements	Not Started
15.	Place / All Directorates	Asbestos Management	**In Progress**
Other Client Work			
16.	Clackmannanshire and Stirling Integration Joint Board	The Internal Audit Plan for 2024/25 was presented to the IJB Audit and Risk Committee on 26 June 2024.	**In Progress**
17.	Central Scotland Valuation Joint Board	The Internal Audit Plan for 2024/25 was presented to the Central Scotland Valuation Joint Board on 28 June 2024.	Not Started

INTERNAL AUDIT PLAN 2024/25 ASSIGNMENT OUTCOMES
Summary of Key Findings from Reviews Complete to Final Report
Not Previously Reported to Committee

Review	Directorate	Assurance
School Admissions	People	**Limited Assurance**
Scope	**Final Report Executive Summary**	

<table>
<tr>
<td>

Extensive legislation governs the provision of education in Scotland, including the Education (Scotland) Act 1980 (as amended) and the Standards in Scotland's Schools Act etc 2000. It places a duty on Local Authorities to provide an adequate and efficient education to all children and young people of school age living within their respective boundary area. It sets out the parameters for which a child / young person is considered to be of school age.

This review is to evaluate and report on the adequacy and availability of the Policy for mainstream primary and secondary schools, and any written operating procedures to assist with the implementation of this Policy. This includes a high-level comparison of the Clackmannanshire Council Education and Learning webpages to both the:
- Enrolment related requirements set out in the Education (Scotland) Act 1980 (as amended) and the Standards in Scotland's Schools Act etc 2000.
- School Admission Policies for a sample of four other Local Authorities across Scotland (included Falkirk Council, Fife Council, Renfrewshire Council, and Stirling Council). These were selected as they are comparators; the Improvement Service has assigned them to the same 'Family Group' for child related benchmarking exercises and / or they share a border with Clackmannanshire Council.

We also surveyed all primary Headteachers to ascertain what operational guidance exists around standard enrolments, due to these being administered at a local level. We received responses from twelve out of eighteen primary schools surveyed.

</td>
<td>

We were content that:

- Parents / guardians are able to access much of the information they need for enrolment on the Council website.
- Guidance is available for assessing Early Entry applications, supporting well evidenced and consistent decision making in this area.

We did identify areas, however, where there is scope for further improvement. Clackmannanshire Council do not have an Enrolment / Admissions Policy, with the information available to parents / guardians located across several parts of the Council website. This makes it difficult to ensure compliance with all legislative requirements. There are also no written operating procedures for many of the key processes relating to enrolment / admission, increasing the risk of errors or inconsistency in approach.

We have made the following recommendations to address the issues noted above:

- To produce prioritisation criteria guidance in relation to placing requests to ensure compliance with the Education (Scotland) Act.
- To produce a consolidated information document that covers all legislative requirements so that parents / guardians can find all the information they need in one place.
- To write operational procedures for all enrolment processes that will facilitate Officers in completing all stages and types of enrolment consistently and efficiently.
- To ensure that St Mungo's Primary School complies with the Education (School and Placing Information) (Scotland) Regulations 2012 by making the School Handbook available online.
- To review the list of improvements identified via benchmarking at Annex 3 and consider incorporation of these into the digitalisation process where appropriate.
- To ensure that parents / guardians have assurance that the Catchment Area Map is an accurate and reliable source of school catchment information.
- To make information on mid-session enrolment available to parents / guardians.
- To ensure that a deadline for initial Early Entry form submission to Early Learning and Childcare settings is set for parents prior to the deadline for full completion of all paperwork.

We are content that the Education Services team have responded positively to the findings raised in the report, working swiftly to resolve two of our recommendations that concerned compliance with the Education (Scotland) Act 1980, and the Education (School and Placing Information) (Scotland) Regulations 2012.

The remaining six actions are lower priority and have been assigned longer timescales accordingly.

</td>
</tr>
</table>

Review	Directorate	Assurance
IT and Information Security Governance	Partnership and Performance / All Directorates	**Limited Assurance**

Scope	Final Report Executive Summary
Scope	**Final Report Executive Summary**

Scope	Final Report Executive Summary
The Council is responsible for a high volume of personal and sensitive data, which can make it a target for fraudsters, scammers, and cyber criminals. Potential consequences of a cyber attack include data loss, financial loss, disruption to service, and reputational damage. 'Cyber Essentials' certification requires an organisation to have a level of technical controls in place to ensure protection against a wide variety of the most common cyber attacks. The National Cyber Security Centre (NCSC) defines it as "an effective, Government backed scheme that will help protect organisations of all sizes, against a whole range of the most common cyber attacks." The Scottish Environment Protection Agency (SEPA) endured a complex ransomware attack in December 2020, which resulted in data being stolen and prevented access to their IT systems. SEPA reported the attack was likely to have been carried out by a serious and organised cyber-crime group intent on disrupting public services and extorting public funds. Audit Scotland reported on the SEPA incident in February 2022. SEPA were unable to access a significant amount of its systems (including financial systems[1]) and data and, at the time of the Audit Scotland report (more than one year later), systems were still being reinstated[2]. The report states that the majority of the data had been encrypted, stolen[3], or lost. The cyber attack resulted in a weaker control environment and SEPA's management had limited financial information to monitor performance and make decisions. As at March 2022, the financial	At the time of this review the Council did not hold a current Public Services Network (PSN) compliance certificate and last achieved compliance in 2018. By not being PSN compliant the Council risks disconnection from the network and not being able to share and receive information over the network which could impact on Council functions. Work is ongoing, however, on implementing measures and gathering supporting evidence for PSN compliance with a target date for certificate submission by the end of September 2024. The Council adopts the Cyber Essentials standards which include controls on Firewalls, secure configuration, user access controls, malware protection, and patch management in line with the Government backed 'Cyber Essentials' implementation profile. Reviews are undertaken against the standards on an annual basis. The Council is not Cyber Essentials certified, and we have recommended in order to demonstrate and strengthen the framework of controls to mitigate Cyber Security Risks, that the feasibility of Cyber Essentials certification is formally considered, and a plan for achieving certification is developed. We are generally content that there are sufficient IT and Information Security Governance roles and responsibilities in place. These include Senior Management, a Data Protection Officer, and dedicated groups responsible for implementing the Council's Digital and Data Transformation Programme. The clarity of the governance roles and inter relationships, however, could be improved by formally defining them in an overarching IT and Information Security Policy. Over the last couple of years, the Council has undertaken considerable work in progressing its Digital Transformation Programme. This has improved IT and Information Security Governance and strengthened the cyber security control framework. Digital transformation measures have also addressed some of the IT security weaknesses highlighted in the SEPA report as follows: • working with consultants on digital transformation over 2023/24, specifically on network and information security and PSN compliance; • establishing Project Management Risk Office and Technical Design Authority Groups responsible for ensuring delivery of Digital and Data Transformation Programme and related projects; • completing an independent IT security health check on the Council's full network; and • designing Microsoft 365 architecture in support of implementation. We did, however, identify potential risks at the time of this review, including not effectively responding and recovering from Cyber Security incidents. There is scope for further improving the existing framework of control with Digital Transformation Programme measures still to be fully implemented. We have made the following recommendations: • the Council's governance arrangements for cyber security should be formally agreed and documented. A Cyber Security Incident Response Team should be formed, with roles and responsibilities documented. The

---

[1] The Audit Scotland report states that SEPA was unable to record any income received, payments made, or match them to pre-existing information held on its systems, such as sales and purchase orders.

[2] The Audit Scotland report states that "key systems have been rebuilt, such as SEPA's financial accounting system, with others being built from new and data recovered or recreated securely, and this will take time."

[3] The Audit Scotland report states that cyber security specialists identified the theft of circa 1.2 GB of data.

impact of this incident reported by the Scottish Parliament was c£4m.

This high level review focussed on the IT and Information Governance arrangements and implementation of the actions arising from the key weaknesses identified from the December 2020 SEPA incident.

Providing an opinion on the Council's vulnerability to a cyber attack is not within the scope of this review, however, we will consider Cyber Security Resilience and IT Incident Management within the context of future Internal Audit Plans.

remit for this team should be defined and responsibilities included in a finalised Cyber Security Incident Response Plan;

- Corporate and Service Business Continuity Plan (BCP) reviews should be completed and should include loss of IT in the finalised BCPs. In addition, a formal comprehensive, risk based, testing programme should be implemented;

- all IT and Information Security policies and standards should be reviewed, updated, and be made available to employees via the Council's intranet. Related operational procedures should be developed to ensure implementation and compliance and also be available to all relevant staff; and

- consideration should be given to how the IT and Information Security related training completion rates can be improved.

DEFINITION OF INTERNAL AUDIT ASSURANCE CATEGORIES

Level of Assurance	Definition
Substantial assurance	Largely satisfactory risk, control, and governance systems are in place. There is, however, some scope for improvement as current arrangements could undermine the achievement of objectives or leave them vulnerable to error or abuse.
Limited assurance	Risk, control, and governance systems have some satisfactory aspects. There are, however, some significant weaknesses likely to undermine the achievement of objectives and leave them vulnerable to an unacceptable risk of error or abuse.
No assurance	The systems for risk, control, and governance are ineffectively designed and operated. Objectives are not being achieved and the risk of serious error or abuse is unacceptable. Significant improvements are required.