Internal Audit Report

Application Technology Controls (SEEMiS)

28 November 2022

CW2202

Overall Assessment	Effective

Contents

This Internal Audit review is conducted for the City of Edinburgh Council under the auspices of the 2022/23 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2022. The review is designed to help the City of Edinburgh Council assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

The internal audit work and reporting has been performed in line with the requirements of the Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Although there are specific recommendations included in this report to strengthen internal control, it is management's responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud. This is an essential part of the efficient management of the City of Edinburgh Council. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings will be raised with senior management and elected members as appropriate.

Executive Summary

Overall opinion and summary of findings

The design and operating effectiveness of the controls in place to manage system security, data quality, and data loss prevention for the SEEMiS system are generally satisfactory.

We have noted the following improvement actions:

- some records are not being disposed of in line with published retention schedules, and retention schedules are not comprehensive
- user access checks in schools are not performed at sufficient frequencies
- there should be greater use of standardised user access profiles in order to reduce the risk of inappropriate access to data.

Areas of good practice

Our review identified:

- adequate data quality controls have been established within the system
- there is consistent completion of the annual pupil data checks
- comprehensive guidance documents and procedures supporting use of the system (SEEMiS help sheets) are published on the Orb
- there is an effective system in place to escalate and resolve issues with system performance
- leavers are removed from SEEMiS in a timely manner.

Audit Assessment

Audit Area	Control Design	Control Operation	Findings	Priority Rating
1. System strategies	🟢	🟢	No issues noted.	N/A
2. System data quality controls	🟢	🟢	No issues noted.	N/A
3. Information governance and system security	🟠	🟠	Finding 1 – SEEMiS Records Retention and Disposal	Medium
4. System access	🟢	🟠	Finding 2 – SEEMiS User Access Checks	Low
			Finding 3 – Review of SEEMiS User Profiles	Low
5. Ongoing supplier management	🟢	🟢	No issues noted.	N/A

See Appendix 1 for Control Assessment and Assurance Definitions

Internal Audit Report: CW2202– Application Technology Controls (SEEMiS)

Background and scope

SEEMiS is an education management system used by all Edinburgh schools and Early Years settings, and throughout Scotland. The system is provided by the SEEMiS Group, which is a limited liability partnership owned and managed by Scotland's 32 local authorities.

SEEMiS is used to manage student data for schools and early years and includes a range of modules supporting pupil and staff record management, nursery application management (NAMS), attendance, pastoral notes, progress and achievement, and reporting.

The system also provides interfaces with external agencies such as ScotXed and the Scottish Qualifications Authority (SQA).

SEEMiS is accessed through the Council's network, with CGI (the Council's technology partner) deploying the application to user machines when requested and supporting ongoing secure system access.

Systems access is managed by the Digital Education Team who ensure that appropriate access is allocated based on user roles and responsibilities (for example, head office and school business support teams have wider access than teachers) and provide ongoing training and general support.

Personal Sensitive Data

SEEMiS and Council networks include data that meets the definition of personal sensitive data outlined in relevant data protection legislation (The Data Protection Act and UK GDPR) as it will include information on racial and ethnic origins, religious or other beliefs, physical and mental health. Reports generated from both systems are also produced to support management decision making and are provided to the Scottish Government.

Consequently, it is important to ensure that there are either appropriate user access, data quality, and data loss prevention controls, included in the system; or that manual data quality reviews are performed, with appropriate

network access and records management processes established and consistently applied by services.

Scope

The objective of this review was to assess the adequacy of the design and operating effectiveness of the key SEEMiS technology controls established to manage system security, data quality, and data loss prevention; and the processes and controls applied by services to ensure that personal sensitive records maintained on the Council's network are appropriately protected.

Risks

- **Technology and Information** - potential failure of cyber defenses. network security. application security. and physical security and operational arrangements

- **Supplier, Contractor, and Partnership Management** - inability to effectively manage the Council's most significant supplier and partnership relationships.

Limitations of Scope

The scope of our review was limited to understanding the assurance that the Council receives from third parties (CGI and SEEMiS Group) in relation to relevant system and supplier management controls, with no direct engagement with these third parties.

Reporting Date

Testing was undertaken between 23 May 2022 and 7 October 2022.

Our audit work concluded on 7 October 2022 and our findings and opinion are based on the conclusion of our work as at that date.

Findings and Management Action Plan

Finding 1 – SEEMiS Records Retention and Disposal

Finding Rating	Medium Priority

Our review established that archived SEEMiS pupil records have held since academic year 2005/06, when the system was first introduced. However, the Council's Records Retention Schedule states that attendance records and exam results, which are both held in SEEMiS, should be destroyed at 23 years and 21 years, respectively, after the pupil's date of birth.

In addition, Schools and Lifelong Learning publishes guidance on records retention within its Quick Guide for Managing Pupil Information and Other Useful Information. Our review identified there is no guidance on how long to retain evidence received in the pupils' admission process, including birth certificates, passports and proof of address.

A similar finding highlighting the requirement to confirm records retention rules for admissions records including birth certificates, and documents confirming address such as council tax statements and birth certificates was raised in the schools admissions, appeals and capacity planning audit completed in February 2020.

Risks

- **Regulatory and Legislative Compliance –** the Council does not dispose of records in alignment with business requirements and data protection guidance and legislation.

Recommendations and Management Action Plan: SEEMiS Records Retention and Disposal

Ref.	Recommendation	Agreed Management Action	Action Owner	Contributors	Timeframe
1.1	A review of records retention periods for individual elements of pupil data held within SEEMiS should be carried out. This review should include establishing clear retention rules for documents received during the pupils' admissions process, e.g. birth certificates, passports, and proof of address. Following the review, there should be liaison with IGU to update the record retention schedule in line with the Council's guidelines, and the Quick Guide for Managing Pupil Information should also be updated. Relevant data should be disposed of in line with the revised Records Retention Schedule and the Council's records disposal guidance	Record retention periods for pupil data will be reviewed and agreed with IGU. Following that, the Council's Records Retention Schedule and Quick Guide for Managing Pupil Information will be updated. A schedule will be created to facilitate a timely, complete disposal of pupil data in line with agreed record retention periods.	Amanda Hatton, Executive Director for Education and Children's Services	Arran Finlay, Senior Education Officer; Sharon McGhee, Quality Improvement Education Officer.	31 May 2023

Internal Audit Report: CW2202– Application Technology Controls (SEEMiS)

Finding 2 – SEEMiS User Access Checks

Finding Rating	Low Priority

Each year a sample of schools are requested to confirm that system access rights for individual school staff remain appropriate, and to provide details of any changes (new starts, leavers, and changes) to the Digital Education Team.

However, only 17 out of 140 schools are covered by this exercise each year, which means that each individual school is only contacted every 7 years on average to confirm that system access rights remain appropriate.

In addition, the Digital Education Team advised that completion of user access checks was often delayed due to slow responses from Business Managers.

Risks

- **Technology and Information** – inappropriate user access rights remain unidentified for a substantial period of time, which could lead to loss or inappropriate access to data.

Recommendations and Management Action Plan: SEEMiS User Access Checks

Ref.	Recommendation	Agreed Management Action	Action Owner	Contributors	Timeframe
2.1	The sample methodology and size for the annual user access check should be reviewed, with consideration given to increasing to number of schools sampled each year.	The sample size for the annual user access check will be reviewed and updated. Additionally, the requirement to review user access rights will be included in the self-assurance pack issued to Head Teachers from Education Services.	Richard Carr, Interim Executive Director of Corporate Services.	Louise Sibbald, Digital Education Team Manager; Jackie Kew, ICT Senior Officer/SEEMiS System Support Officer; Julie Russell, ICT Senior Officer/SEEMiS System Support Officer.	31 March 2023
2.2	1. When emails are sent to schools requesting confirmation of system access rights for individual staff members, school administrators should be copied in, in order to improve response times. 2. Business Managers should be reminded of the need to provide responses in a timely manner.	Agreed to both points.			31 March 2023

Finding 3 – SEEMiS User Access profiles

Finding Rating	Low Priority

There are seven standard SEEMiS access profiles, which are based on individuals' roles, e.g. Principal Teacher, Teacher, and Pastoral. In discussions with officers, Internal Audit was advised that administrators in schools are given 'Office' profiles that enable them to grant bespoke access rights outwith the standard profiles. While this creates opportunity to reflect the unique way that different schools operate, this also leads to inconsistency of user access rights across the Council.

Consideration should be given to performing a review of SEEMiS user access profiles across the Council in order to determine if additional user access profiles should be created to improve standardisation of access rights for staff.

Risks

- **Technology and Information** – user access profiles are not standardised across the Council, leading to inappropriate access to data.

Recommendations and Management Action Plan: SEEMiS User Access Profiles

Ref.	Recommendation	Agreed Management Action	Action Owner	Contributors	Timeframe
3.1	A review of SEEMiS user access profiles should be performed in order to determine if additional user access profiles should be created to improve standardisation of access rights for staff.	This risk will be effectively managed by the exercise performed in action 2.1 and therefore no review of user access profiles will be performed.	N/A	N/A	N/A

Appendix 1 – Control Assessment and Assurance Definitions

Control Assessment Rating		Control Design Adequacy	Control Operation Effectiveness
Well managed	🟢	Well-structured design efficiently achieves fit-for purpose control objectives	Controls consistently applied and operating at optimum level of effectiveness.
Generally Satisfactory	🟢	Sound design achieves control objectives	Controls consistently applied
Some Improvement Opportunity	🟠	Design is generally sound, with some opportunity to introduce control improvements	Conformance generally sound, with some opportunity to enhance level of conformance
Major Improvement Opportunity	🔴	Design is not optimum and may put control objectives at risk	Non-conformance may put control objectives at risk
Control Not Tested	**N/A**	Not applicable for control design assessments	Control not tested, either due to ineffective design or due to design only audit

Overall Assurance Ratings	
Effective	The control environment and governance and risk management frameworks have been adequately designed and are operating effectively, providing assurance that risks are being effectively managed, and the Council's objectives should be achieved.
Some improvement required	Whilst some control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks, they provide reasonable assurance that risks are being managed, and the Council's objectives should be achieved.
Significant improvement required	Significant and / or numerous control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks. Consequently, only limited assurance can be provided that risks are being managed and that the Council's objectives should be achieved.
Inadequate	The design and / or operating effectiveness of the control environment and / or governance and risk management frameworks is inadequate, with a number of significant and systemic control weaknesses identified, resulting in substantial risk of operational failure and the strong likelihood that the Council's objectives will not be achieved.

Finding Priority Ratings	
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
Low Priority	An issue that results in a small impact to the achievement of objectives in the area audited.
Medium Priority	An issue that results in a moderate impact to the achievement of objectives in the area audited.
High Priority	An issue that results in a severe impact to the achievement of objectives in the area audited.
Critical Priority	An issue that results in a critical impact to the achievement of objectives in the area audited. The issue needs to be resolved as a matter of urgency.