ABERDEEN CITY COUNCIL

COMMITTEE	Audit, Risk and Scrutiny Committee
DATE	26 September 2024
EXEMPT	No
CONFIDENTIAL	No
REPORT TITLE	Internal Audit Report AC2502 - SEEMiS
REPORT NUMBER	IA/AC2502
DIRECTOR	N/A
REPORT AUTHOR	Jamie Dale
TERMS OF REFERENCE	2.2

1. PURPOSE OF REPORT

1.1 The purpose of this report is to present the planned Internal Audit report on SEEMiS.

2. RECOMMENDATION

2.1 It is recommended that the Committee review, discuss and comment on the issues raised within this report and the attached appendix.

3. CURRENT SITUATION

3.1 Internal Audit has completed the attached report which relates to an audit of SEEMiS.

4. FINANCIAL IMPLICATIONS

4.1 There are no direct financial implications arising from the recommendations of this report.

5. LEGAL IMPLICATIONS

5.1 There are no direct legal implications arising from the recommendations of this report.

6. ENVIRONMENTAL IMPLICATIONS

6.1 There are no direct environmental implications arising from the recommendations of this report.

7. RISK

7.1 The Internal Audit process considers risks involved in the areas subject to review. Any risk implications identified through the Internal Audit process are detailed in the resultant Internal Audit reports. Recommendations, consistent with the Council's Risk Appetite Statement, are made to address the identified risks and Internal Audit follows up progress with implementing those that are agreed with management. Those not implemented by their agreed due date are detailed in the attached appendices.

8. OUTCOMES

8.1 There are no direct impacts, as a result of this report, in relation to the Council Delivery Plan, or the Local Outcome Improvement Plan Themes of Prosperous Economy, People or Place.

8.2 However, Internal Audit plays a key role in providing assurance over, and helping to improve, the Council's framework of governance, risk management and control. These arrangements, put in place by the Council, help ensure that the Council achieves its strategic objectives in a well-managed and controlled environment.

9. IMPACT ASSESSMENTS

Assessment	Outcome
Impact Assessment	An assessment is not required because the reason for this report is for Committee to review, discuss and comment on the outcome of an internal audit. As a result, there will be no differential impact, as a result of the proposals in this report, on people with protected characteristics.
Privacy Impact Assessment	Not required

10. BACKGROUND PAPERS

10.1 There are no relevant background papers related directly to this report.

11. APPENDICES

11.1 Internal Audit report AC2502 – SEEMiS

12. REPORT AUTHOR CONTACT DETAILS

Name	Jamie Dale
Title	Chief Internal Auditor
Email Address	Jamie.Dale@aberdeenshire.gov.uk
Tel	(01467) 530 988

Internal Audit

Assurance Review of SEEMiS

Status: Final
Report No: AC2502
Date: 12 September 2024
Assurance Year: 2024/25
Risk Level: Programme and Project level

Net Risk Rating	Description	Assurance Assessment
Moderate	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified, which may put at risk the achievement of objectives in the area audited.	**Reasonable**

Report Tracking	Planned Date	Actual Date
Scope issued	30-Apr-24	30-Apr-24
Scope agreed	07-May-24	21-May-24
Fieldwork commenced	13-May-24	21-May-24
Fieldwork completed	07-Jun-24	29-Jul-24
Draft report issued	28-Jun-24	01-Aug-24
Process owner response	19-Jul-24	26-Aug-24
Director response	26-Jul-24	11-Sep-24
Final report issued	02-Aug-24	12-Sep-24
AR&S Committee	26-Sep-24	

Distribution	
Document type	Assurance Report
Directors	Andy MacDonald, Executive Director – Corporate Services Eleanor Sheppard, Executive Director – Families and Communities
Process Owner	Reyna Stewart, Analytics and Insight Manager
Stakeholders	Martin Murchie, Chief Officer – Data Insights
	Lindsay Simpson, MIS Support Officer
	Shona Milne, Chief Education Officer
	Charlie Love, Quality Improvement Officer - Digital
	Vikki Cuthbert, Interim Chief Officer – Governance*
	Jonathan Belford, Chief Officer - Finance*
***Final Only**	External Audit*
Lead auditor	Farai Magodo, Auditor

1 Introduction

1.1 Area subject to review

Strathclyde Educational Establishments Management Information System (SEEMiS) is used by all Scottish Councils to support electronic education administration within Council headquarters and schools. The system is supplied by a Limited Liability Partnership (LLP) made up of all Scottish Local Authorities, including Aberdeenshire Council.

SEEMiS provides the management information needs of all Aberdeenshire Council schools as well as a wide range of central administrative and quality improvement functions. It is used for the maintenance of personal and academic (including SQA) records for pupils; personal information and work records for staff; and attendance records for pupils and staff.

1.2 Rationale for review

The objective of this audit is to provide assurance that appropriate control is being exercised over the schools and education management information system in view of the perceived criticality of the system and the significant volume of sensitive personal data held.

This area was last subject to review in February 2020 in Internal Audit AC2021. Recommendations were made to enhance controls over system access and data protection.

1.3 How to use this report

This report has several sections and is designed for different stakeholders. The executive summary (section 2) is designed for senior staff and is cross referenced to the more detailed narrative in later sections (3 onwards) of the report should the reader require it. Section 3 contains the detailed narrative for risks and issues we identified in our work.

2 Executive Summary

2.1 Overall opinion

The full chart of net risk and assurance assessment definitions can be found in Appendix 2 – Assurance Scope and Terms. We have assessed the net risk (risk arising after controls and risk mitigation actions have been applied) as:

Net Risk Rating	Description	Assurance Assessment
Moderate	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified, which may put at risk the achievement of objectives in the area audited.	**Reasonable**

The organisational risk level at which this risk assessment applies is:

Risk Level	Definition
Programme and Project	This issue / risk level impacts the programme or project that has been reviewed. Mitigating actions should be taken at the level of the programme or project concerned.

2.2 Assurance assessment

The level of risk is assessed as **MODERATE**, with the control framework deemed to provide **REASONABLE** assurance over the Council's approach to the SEEMiS system.

The Management Information System (MIS) Support team is responsible for access control and day-to-day user administration whilst the system supplier is responsible for ensuring system availability, data security and backup, system maintenance, incident resolution and performance reporting.

Reasonable assurance was available over the following areas reviewed:

- **User Guidance and Training** – System users have access to clear guidance and training courses both in the Council's Network Education Aberdeen SharePoint site and through that provided by the system supplier. In addition, the MIS Support team are available to provide user support.
- **System Data Accuracy –** In terms of data accuracy, the Service advised parents / guardians verify the accuracy of pupil data held on SEEMiS annually and this process was last undertaken in August 2024 (example redacted return from parent provided).
- **Cyber Resilience –** In terms of resilience to cyber security threats, the supplier advised Internal Audit in June 2023 as part of a previous review of the system that penetration testing was undertaken on the SEEMiS application and supporting infrastructure in March 2023, by an independent external provider accredited to the CREST scheme, with a 'low risk: pass' outcome. Assurance was also provided by email by the supplier at this time that vulnerability scanning is taking place on a regular basis. The SEEMiS Board also receives an Information Security/Data Protection Update report from the SEEMiS Data Protection Officer/Information Security Manager approximately three times per year and these reports cover patching of operating systems and vulnerability assessment checks.
- **Back-ups and Disaster Recovery –** SEEMiS published System Applications and Environment Technical Guidance in 2024 which confirmed SEEMiS will test a system failover from the Chapel Hall data centre site to the Saughton House data centre. This should provide assurance over the adequacy of backup arrangements.

However, the review identified some areas of weakness where enhancements could be made to strengthen the framework of control, specifically:

- **System Access** – Schools have discretion to determine their own system access levels risking inconsistencies across job types in the level of access to sensitive data e.g. via full access to the Wellbeing module which contains data relating to health and personal circumstances. It was not possible to determine what officers by job title had full Wellbeing module access to determine if this was appropriate due to system reporting limitations and since this is not

monitored centrally presently. It was also noted that the level of personal data requested to grant system access is extensive and unnecessary for non-school staff. Both these issues risk a breach of data protection legislation and enforcement action by the ICO.

- **Business Continuity Planning** – It was noted the Education business continuity plan (BCP) and ten school BCPs, did not describe alternative arrangements for relevant SEEMiS system functionality, including pupil registration and procedures for conveying wellbeing concerns to relevant staff, should the system become unavailable. This potentially risks pupil health and wellbeing and completion of relevant statutory duties including census submission required by the Statistics and Registration Service Act 2007.
- **Contract Register** – The recent direct award contract extension for the system supplier complied with Scheme of Governance Committee approval requirements and the related 2024/25 purchase order is accurate based on the contract. However, under the Procurement Reform (Scotland) Act 2014, a regulated contract requires to be included on the Council's contracts register. Whilst the contract with the system supplier is included on the Council's contracts register, the recorded value and end date were incorrect and the duration the contract can be extended was absent, based on the direct award approved by Finance and Resources Committee, in breach of procurement legislation.

Recommendations have been made to address the above risks, including minimising personal data recorded for system access; standardising system access profiles by job type and monitoring access; reviewing and updating business continuity plans where necessary; reviewing and updating the contracts register; and risk assessing interfaces to determine if any additional controls are required over data completeness and accuracy.

2.3 Severe or major issues / risks

No severe or major issues/risk were identified as part of this review.

2.4 Management response

Education
We have received and reviewed the Assurance Review of SEEMiS and we agree with the findings and recommendations. We appreciate the thorough and constructive feedback from the audit team and we are committed to implementing the recommendations to improve our service delivery.

Data Insights (HDRCA)
We welcome the assurance provided through this review and are engaging with the SEEMiS team nationally and the Council's Information Asset Owner to discharge the recommendations.

3 Issues / Risks, Recommendations, and Management Response

3.1 Issues / Risks, recommendations, and management response

<table>
<tr><th>Ref</th><th>Description</th><th>Risk Rating</th><th>Moderate</th></tr>
<tr><td>1.1</td><td colspan="3">
Contracts Register – Under the Procurement Reform (Scotland) Act 2014, a regulated contract requires to be included on the Council's contracts register and must include the following:

Date of Award
Name of the Contractor
Subject Matter
Estimated Value
Start Date
End date provided for in the contract (disregarding any option to extend the contract) or, where there is no date specified, a description of the circumstances in which the contract will end.
Duration of any period for which the contract can be extended.

The current contract was most recently extended for the period 1 April 2024 to 31 March 2025 by direct award at an estimated cost of £230k, with the option to extend the contract until 31 March 2029 for a total estimated cost of £1.150m, following approval of the related Business Case by Finance and Resources Committee in May 2024, in line with the Council's Scheme of Governance. In addition, on reviewing the purchase order for 2024/25, this had been raised in line with the charges prescribed by the contract.

However, the contract with the system supplier is included on the Council's contracts register, the recorded value (£500k) and end date (31 March 2026) are incorrect based on the direct award approved by Finance and Resources Committee in May 2024 (£230k for one year to 31 March 2025) and the absence of the period the contract can be extended by to 31 March 2029.

This should be resolved to improve accountability for contractual commitments and to comply with procurement legislation.

IA Recommended Mitigating Actions

The system entry within the Council's contract register system should be reviewed and updated where necessary.

Management Actions to Address Issues/Risks

Agreed.
<table>
<tr><th>Risk Agreed</th><th>Person(s)</th><th>Due Date</th></tr>
<tr><td>Yes</td><td>Category Manager</td><td>Implemented</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Ref</th><th>Description</th><th>Risk Rating</th><th>Moderate</th></tr>
<tr><td>1.2</td><td colspan="3">System Access – Access to systems, which contain high volume and sensitive personal data, must be suitably controlled and restricted to ensure compliance with data protection legislation.</td></tr>
</table>

Ref	Description	Risk Rating	Moderate
	Positive Assurance Data Insights advise SEEMiS has an automated security functionality to lock a system user's account after a period of 100 days inactivity and passwords are reset for all system users every 90 days. New and Amended System Access – New User Form Under the UK General Data Protection Regulation (GDPR) data minimisation principle, personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. To gain access to the system, a SEEMiS User Access Request Form must be approved by the prospective user's line manager and submitted to the MIS Support team for processing. However, it was noted that the level of personal data requested to grant system access is extensive including the following: • National Insurance number • Date of birth • Gender • Home address • Mobile phone number • Working days and hours • Emergency contact name, gender, home address, mobile number • Ethnic origin • National identity Whilst some of this information is necessary for teachers for the ScotXed staff census information, this includes sensitive personal data that will not require to be collected for all SEEMiS users, risking a breach of data protection legislation due to unnecessary personal data processing, and enforcement action by the ICO, including reprimand, an enforcement notice, and / or monetary penalty. School Access Amendment Once the account ("staff record") has been created, one or more work records are set up for each position filled by the staff member, such as Head Teacher, Teacher, Support Staff. School administrators are then responsible for assigning profiles to the work record which permit access to the modules and reports deemed appropriate by the relevant school. The access available to a particular work record can only be amended by the MIS team within Data Insights. However, access by job type has not been standardised across schools and schools have discretion over system access (work profiles) assigned to staff, increasing the risk of inconsistencies in access levels by job type. Data Insights advised Support Role access to the Wellbeing module provides no access to personal confidential data and just allows documents to be uploaded to the Wellbeing module by support staff. However, full access to the Wellbeing module is high risk since it permits access to sensitive personal data relating to pupils' health and personal circumstances, and E&CS advise should only be available to Head Teachers, Depute Head Teachers, and Guidance Teachers. It was not clear who had full Wellbeing access at the time of review since this is not centrally monitored and the ability to report on this access is not easily achieved without manual data manipulation of system data. Monitoring of Leavers / Changes of Employee Posts Data Insights have the role of monitoring staff whose employment with the Council has ceased. This has been a manual process and was dependent upon the availability of a singleton post. However, Data & Insights has advised that a PowerBI report has been set up which identifies these leavers and this is now used to manage / remove access to SEEMiS where necessary. It was confirmed that changes in staff posts and therefore responsibilities		

Ref	Description	Risk Rating	Moderate

are not currently monitored centrally by Data Insights for the purposes of amending SEEMiS access where necessary. This increases the risk staff who have changed post will continue to have unnecessary access to confidential records within SEEMiS.

In the absence of standardisation of access by job type, there is a greater risk of inappropriate unnecessary access to sensitive personal data in breach of data protection legislation or there is a risk necessary information required by school staff is unavailable risking pupils' health and wellbeing.

IA Recommended Mitigating Actions

a) Data Insights should review the User Access Request Form and related retained records for non-school staff and ensure only necessary personal data is being collected and retained for the purposes of granting system access. If the level of necessary personal data differs by job type the User Access Request Form should make this clear. It is understood this is SEEMiS's user access form / process, therefore SEEMiS should be consulted as necessary prior to implementing local changes.

b) Data Insights should work with Education to create a list of defined system profiles whose access rights are standardised and minimised based on job responsibilities and remove any non-standard profiles. If feasible an exception report should be developed flagging any users with access to sensitive system data which is not in line with the standard.

c) Officer role changes, and leavers should be monitored for the purposes of restricting system access where necessary and the existing PowerBI reporting should be developed if possible, to cover this where necessary.

Management Actions to Address Issues/Risks

a) It is agreed that the level of personal data required for non-school staff to grant system access is excessive. This will be raised with SEEMiS since these fields are mandatory.

b) Agreed.

c) Agreed.

Risk Agreed	Person(s)	Due Date
a) Yes b) Yes c) Yes	Analytics and Insight Manager	a) December 24 b) August 25 c) August 25

Ref	Description	Risk Rating	Moderate
1.3	**Business Continuity** – Should a critical system such as SEEMiS cease to function, it is essential pupil and teacher personal data can be recovered to avoid reputational damage and potential significant financial penalty for breach of data protection legislation. In addition, clear plans are necessary to maintain service delivery and to commence system recovery to avoid educational disruption. <u>Contractual Assurance</u> The system supplier Service Agreement adequately covers the supplier's own business continuity arrangements; the four weekly maintenance and patching schedule; and a detailed backup policy, including details of daily and weekly backups and offsite storage arrangements.		

Ref	Description	Risk Rating	Moderate

Business Continuity Planning

The Civil Contingencies Act 2004 places a duty on the Council as a "Category 1 Responder" to maintain Business Continuity Plans (BCP's) to minimise as far as possible service disruption in particular critical services.

The critical nature of the SEEMiS system is highlighted in the business case for the direct award extension of the contract of the system reported to Finance and Resources Committee in May 2024 where the justification included meeting statutory requirements and the delivery of education. Related functionality that was highlighted included maintenance of pupil records, including attendance; absence and exclusion recording; wellbeing; bullying and equalities; pupil reporting; timetabling; SQA examination entry; and management and monitoring of progress and achievement.

However, for the Education BCP and ten school BCPs, alternative arrangements for relevant SEEMiS system functionality were not included e.g. how to check pupil attendance and alternative procedures for conveying wellbeing concerns to relevant staff. This potentially risking pupil health and wellbeing and completion of relevant statutory duties e.g. census submission as required by the Statistics and Registration Service Act 2007. In addition, the Data Insights BCP is under review, risking system recovery delay.

IA Recommended Mitigating Actions

a) Education should ensure the Education BCP and school BCPs adequately cover relevant procedure to enable service and school level business continuity in the event SEEMiS becomes unavailable, covering relevant critical school tasks undertaken using SEEMiS.

b) The Data Insights BCP should be reviewed to ensure it adequately covers SEEMiS system recovery.

Management Actions to Address Issues/Risks

a)(i) All schools have been reminded that a paper copy of contact information for all pupils and staff must be printed off termly and kept in the emergency response bag (in the event that SEEMiS is unavailable). This information has been shared with all head teachers by email prior to the start of the new term in August 2024 and will be included in BCP format and guidance moving forward. The school pro-forma BCP will be updated to cover relevant alternative procedures for school tasks normally undertaken using SEEMiS and shared with Head Teachers.

a)(ii) Agreed. The BCP will be updated to cover system recovery procedure including the requirement to raise a ticket with D&T to establish if issue is a local one prior to ticket being logged with SEEMiS.

b) Agreed.

Risk Agreed	Person(s)	Due Date
a)(i) Yes	a)(i) Quality Improvement Manager	a)(i) Implemented.
a)(ii) Yes – Education BCP	a)(i) Quality Improvement Officer – Digital	a)(ii) October 2024
c) Yes – Data Insights BCP	c) Analytics and Insight Manager	c) October 2024

<table>
<tr><th>Ref</th><th>Description</th><th>Risk Rating</th><th>Minor</th></tr>
<tr><td>1.4</td><td colspan="3">
System Interfaces – Where data is transferred into or out of a system via a system interface (or similar) it is prudent to ensure control over data accuracy and completeness. In the case of SEEMiS such controls help avoid breaches of data protection legislation due to personal data being inaccurately processed or EMA payment / free school meal eligibility errors.

The following system interfaces are in operation:
<table>
<tr><th>Name</th><th>High Level Description</th></tr>
<tr><td>Scottish Government - EMA Yearly Feed</td><td>Payments and income feed to Scottish Government (SG).</td></tr>
<tr><td>Glow</td><td>Data Feed to Glow digital learning platform.</td></tr>
<tr><td>GroupCall Messenger</td><td>Messenger product messages to GroupCall e.g. used for contacting parents.</td></tr>
<tr><td>NHS - Health Board Feeders</td><td>Data sent to NHS for National Child Health Programme.</td></tr>
<tr><td>ParentPay - Online School Payments</td><td>Free school meal eligibility and other pupil data sent to ParentPay for cashless catering provision.</td></tr>
<tr><td>Salesforce</td><td>SEEMiS Helpdesk system calls from system administrators.</td></tr>
<tr><td>Scholar</td><td>Pupil and staff registration details for Scholar educational application.</td></tr>
<tr><td>ScotXed (various)</td><td>Authentication of SEEMiS credentials and pupil and staff census data.</td></tr>
<tr><td>Skills Development Scotland - Opportunities for All</td><td>16+ Survey.</td></tr>
<tr><td>Acer AWS EU - SNSA</td><td>Scottish National Standardised Assessment data.</td></tr>
<tr><td>Giglets - SNSA-Gaelic</td><td>Scottish National Standardised Assessment data.</td></tr>
<tr><td>SQA</td><td>SQA registration and related responses from SQA.</td></tr>
</table>
Controls over Education Maintenance Allowance (EMA) payments and free school meal eligibility transfer to the cashless catering system were considered as part of the recent Internal Audit review AC2501 Allowances and so are not considered further as part of this review.

An adequate system of exception reporting is in operation for data exported to the Scottish Government for the purposes of the Scottish Exchange of Data (ScotXed) pupil and staff census data e.g. highlighting year on year variances, data not meeting response parameters.

However, controls were not evident over the accuracy and completeness of other data transfer arrangements via system interfaces. Whilst it was advised that the responsibility for interface success lies with the system supplier and issues are investigated by exception, in the absence of oversight via relevant reconciliations or where feasible exception reports, there is a greater risk transferred data will be inaccurate or incomplete.
</td></tr>
</table>

<table>
<tr><th>Ref</th><th>Description</th><th>Risk Rating</th><th>Minor</th></tr>
<tr><td></td><td colspan="3">Since these interfaces have not been reviewed in detail by IA and no related errors were identified during the review, the following recommendation is for consideration for improvement purposes only.</td></tr>
<tr><td></td><td colspan="3">IA Recommended Mitigating Actions</td></tr>
<tr><td></td><td colspan="3">Education should review and risk assess system interfaces and determine if any additional controls are necessary to gain assurance data is being transferred as required.</td></tr>
<tr><td></td><td colspan="3">Management Actions to Address Issues/Risks</td></tr>
<tr><td></td><td colspan="3">Agreed. This is accepted and will be considered and discussed with SEEMiS.</td></tr>
<tr><td></td><td>Risk Agreed</td><td>Person(s)</td><td>Due Date</td></tr>
<tr><td></td><td>Yes</td><td>Quality Improvement Officer – Digital</td><td>December 24</td></tr>
</table>

4 Appendix 1 – Assurance Terms and Rating Scales

4.1 Overall report level and net risk rating definitions

The following levels and ratings will be used to assess the risk in this report:

Risk level	Definition
Corporate	This issue / risk level impacts the Council as a whole. Mitigating actions should be taken at the Senior Leadership level.
Function	This issue / risk level has implications at the functional level and the potential to impact across a range of services. They could be mitigated through the redeployment of resources or a change of policy within a given function.
Cluster	This issue / risk level impacts a particular Service or Cluster. Mitigating actions should be implemented by the responsible Chief Officer.
Programme and Project	This issue / risk level impacts the programme or project that has been reviewed. Mitigating actions should be taken at the level of the programme or project concerned.

Net risk rating	Description	Assurance assessment
Minor	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.	**Substantial**
Moderate	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified, which may put at risk the achievement of objectives in the area audited.	**Reasonable**
Major	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.	**Limited**
Severe	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.	**Minimal**

Individual issue / risk	Definitions
Minor	Although the element of internal control is satisfactory there is scope for improvement. Addressing this issue is considered desirable and should result in enhanced control or better value for money. Action should be taken within a 12 month period.
Moderate	An element of control is missing or only partial in nature. The existence of the weakness identified has an impact on the audited area's adequacy and effectiveness. Action should be taken within a six month period.
Major	The absence of, or failure to comply with, an appropriate internal control, such as those described in the Council's Scheme of Governance. This could result in, for example, a material financial loss, a breach of legislative requirements or reputational damage to the Council. Action should be taken within three months.
Severe	This is an issue / risk that is likely to significantly affect the achievement of one or many of the Council's objectives or could impact the effectiveness or efficiency of the Council's activities or processes. Examples include a material recurring breach of legislative requirements or actions that will likely result in a material financial loss or significant reputational damage to the Council. Action is considered imperative to ensure that the Council is not exposed to severe risks and should be taken immediately.

5 Appendix 2 – Assurance Scope and Terms of Reference

5.1 Area subject to review

Strathclyde Educational Establishments Management Information System (SEEMiS) is used by all Scottish Councils to support electronic education administration within Council headquarters and schools. The system is supplied by a Limited Liability Partnership (LLP) made up of all Scottish Local Authorities, including Aberdeenshire Council.

SEEMiS provides the management information needs of all Aberdeenshire Council schools as well as a wide range of central administrative and quality improvement functions. It is used for the maintenance of personal and academic (including SQA) records for pupils; personal information and work records for staff; and attendance records for pupils and staff.

5.2 Rationale for review

The objective of this audit is to provide assurance that appropriate control is being exercised over the schools and education management information system in view of the perceived criticality of the system and the significant volume of sensitive personal data held.

This area was last subject to review in February 2020 in Internal Audit AC2021. Recommendations were made to enhance controls over system access and data protection.

5.3 Scope and risk level of review

This review will offer the following judgements:

- An overall **net risk** rating at the Programme and Project level.
- Individual **net risk** ratings for findings.

Please see Appendix 1 – Assurance Terms and Rating Scales for details of our risk level and net risk rating definitions.

5.3.1 Detailed scope areas

As a risk-based review this scope is not limited by the specific areas of activity listed below. Where related and other issues / risks are identified in the undertaking of this review these will be reported, as considered appropriate by IA, within the resulting report.

The specific areas to be covered during the visits are:

- Written Procedures
- System Access and Security
- Data Input and Interfaces
- Data Protection
- Contingency Planning and Disaster Recovery

5.4 Methodology

This review will be undertaken through interviews with key staff involved in the process(es) under review and analysis and review of supporting data, documentation, and paperwork. To support our work, we will review relevant legislation, codes of practice, policies, procedures, and guidance.

Due to hybrid working arrangements, this review will be primarily undertaken remotely.

5.5 IA outputs

The IA outputs from this review will be:

- A risk-based report with the results of the review, to be shared with the following:
    - Council Key Contacts (see 1.7 below)

- Audit Committee (final only)
- External Audit (final only)

5.6 IA staff

The IA staff assigned to this review are:

- Farai Magodo, Auditor **(audit lead)**
- Andy Johnston, Audit Team Manager
- Jamie Dale, Chief Internal Auditor **(oversight only)**

5.7 Council key contacts

The key contacts for this review across the Council are:

- Andy MacDonald, Executive Director – Corporate Services
- Eleanor Sheppard. Executive Director – Families and Communities
- Martin Murchie, Chief Officer – Data Insights
- Reyna Stewart, Analytics and Insight Manager **(process owner)**
- Shona Milne, Chief Education Officer
- Charlie Love, Quality Improvement Officer - Digital

5.8 Delivery plan and milestones

The key delivery plan and milestones are:

Milestone	Planned date
Scope issued	30/04/24
Scope agreed	07/05/24
Fieldwork commences	13/05/24
Fieldwork completed	07/06/24
Draft report issued	28/06/24
Process owner response	19/07/24
Director response	26/07/24
Final report issued	02/08/24