55

Internal Audit Report
Corporate & Democratic Services – Corporate IT
IT Application review No. 15-36 SEEMIS
February 2016

Final Report

Chief Executive's Service
Finance Division
Perth & Kinross Council
2 High Street
Perth PH1 5PH

Internal Audit

"Internal Audit is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes". Public Sector Internal Auditing Standards (PSIAS)
On 27th March 2013, the Council's Audit Committee approved the PSIAS as the relevant standard for its Internal Audit activity.

Background and Introduction

This assignment forms part of the Internal Audit plan for 2015/16 and was approved by the Audit Committee on 1 April 2015.

SEEMIS has been used within the Council as the Education Management System for a number of years. The system is used within education establishments to record pupil information including attendance and pastoral notes. The system is modular in nature with the Click & Go module being the primary one. There is also functionality which records and supports business processes relating to free school meals, attainment, Education Maintenance Allowances and Clothing Grants.

Responsibility for maintaining the system is split between the Council and SEEMIS LLP. The Council is responsible for day to day user administration, data input and user access control whereas SEEMIS LLP is responsible for system security, system developments, issue resolution, backup and performance monitoring.

Within the Council's IT division there is a team with oversight of Education and Children's Services business applications (herein referred to as the MIS team). In relation to the SEEMiS system the MIS team is responsible for system administration, implementation of new functionality, operational and statutory reporting and user support and training. Council representatives including MIS team staff are involved nationally in SEEMiS user groups, working groups and governance groups.

Scope and Limitations

In order to arrive at an opinion on the achievement of the control objectives, the audit included interviews with relevant staff in Corporate IT as well as Business Managers at a sample of education establishments.

Control Objectives and Opinions

This section describes the purpose of the audit and summarises the results. A 'control objective' is a management objective that requires the maintenance of adequate and effective internal controls to ensure that it is achieved. Each control objective has been given a rating describing, on the basis of the audit work done, the actual strength of the internal controls found to be in place. Areas of good or poor practice are described where appropriate.

Control Objective1 There are adequate system administration and user procedures.

Auditor's Comments: The MIS team has been established within the Council for the management and oversight of SEEMiS. This includes system administration and management of new developments. In addition, at each of the secondary schools, Business Managers are responsible for managing SEEMiS access within their respective schools. The MIS team is also responsible for day to day administration of SEEMiS for primary schools.

A number of user guides and procedures (prepared by both SEEMiS LLP and Council staff) are available to users. Council created guides are accessible via the Council's intranet ('Eric') whilst those created by SEEMiS LLP are accessible through the system modules and the SEEMiS website. These cover a range of areas - from how to set up new accounts to creating timetables. Whilst a formal review cycle is not in place, we confirmed that these are updated as and when required.

The MIS team also offers training on a formal basis and runs workshop sessions for schools on the use of SEEMiS to support key activities throughout the school year for example, new P1 admissions, P7 – S1 Transfers and placing requests.

Strength of Internal Controls:	Strong

Control Objective 2: There are robust logical access controls

Auditor's Comments: Users are provided with individual user accounts to login to SEEMiS and these are controlled by robust password settings which include a minimum character length of 8 characters, alphanumeric character requirements and forced password changes every 60 days.   After 3 unsuccessful log-in attempts, it was noted that accounts would be automatically locked.

Strength of Internal Controls:	Strong

Control Objective: 3 There is effective user account management which ensures only authorised users have access.

Auditor's Comments: We noted that line managers must authorise access to SEEMiS prior to staff being given access. This would be done through the completion of a form. Once authorisation has been given and accounts have been created, line managers are copied into emails containing SEEMiS login details.

A number of controls are in place in respect of ensuring that user accounts of leavers are removed. At secondary/all through schools, Business Managers are responsible for removing accounts. Due to the nature of their role, they will be aware of all leavers and will remove access as and when necessary.

For all other users, the MIS team receives a report on a weekly basis of accounts that have been disabled in Active Directory (the software which manages access to the Council's network). This will be reviewed by the MIS team to identify any SEEMiS users. They also scan the list for accounts that should be removed by Business Managers and will, where relevant, discuss any anomalies.

Furthermore, as part of the annual staff census, the Council is required to provide information on individual teaching staff to the Scottish Government. This is checked and signed off on a school by school basis to ensure that only current teaching staff are included, thereby acting as a compensating control on the validity of users.

Strength of Internal Controls:	Strong

Control Objective 4: User access levels are appropriate and ensure adequate segregation of duties in relation to the administration and operation of the system.

Auditor's Comments: It was noted that, at schools, role (base) profiles had been established in order to ensure the provision of uniform access to SEEMiS. From our meetings with Business Managers at a sample of secondary and all-through schools we identified that there is limited uniformity across schools in relation to user access profiles for school staff. It is the case that additional profiles, over and above the base profiles, have been created within some 'secondary and all-through' schools. These have been developed locally as there are variations in responsibilities across different establishments. As such access profiles have been customised to meet that requirement.

We also noted that a formal process was developed in 2012 to review all user profiles in use across each establishment. Formal templates and guidance documents have been developed by the MIS team to ensure a consistent approach to the review. We noted that the last reviews were performed in 2014. This covered 12 primary schools, 1 secondary school and three areas of the MIS team which represents approximately 20% of all establishments. It was stated that conducting these reviews is resource intensive and a cyclical review process is being considered. This would see the review process being over an extended timeframe to alleviate the burden on the resources of the MIS team.

We also noted a minor issue in relation to consistency in providing access to supply teachers. In one school, all supply teachers were provided with access immediately, whereas in others they would only be provided with access when it became apparent that their tenure at the school would be more prolonged.

Strength of Internal Controls:	Moderately strong

Control Objective 5 Access to amend system parameters is restricted to authorised users	
Auditor's Comments: Access to amend key system parameters such as password settings is restricted to SEEMiS LLP. Whilst the majority of data requirements are pre-defined and mandatory, there are certain system variables relating to data collection that can be amended at local authority level and certain variables that can be amended at individual school level. The ability to revise school-level variables was found to be restricted to authorised users, such as the MIS team, Business Managers and Senior Management Team. The ability to revise local authority-level variables is restricted to the MIS team.	
Strength of Internal Controls:	Strong

Control Objective 6: All data interfaces ensure complete and accurate transfer of data.	
Auditor's Comments: There are a significant number of data transfers to/from the Council's SEEMiS system. A large percentage of these relate to a two way data transfer between schools and the Scottish Qualifications Authority (SQA). These data transfers ensure pupils are registered with the SQA and entered for the correct subjects at the correct level. In addition all unit passes and estimates are sent to SQA via the SEEMiS interface. We confirmed that detailed timeline driven processes are defined to support schools with these key tasks. MIS team members are responsible for monitoring and supporting specific schools. We walked through one example of a data transfer, this being the data from the SQA in relation to main diet examination results. The data transfer and import to SEEMiS is managed directly by SEEMiS LLP, with Council staff being responsible for various validation and accuracy checks. Examples of checks included: school roll by year group, entries and passes by year group/course level and any exceptional items. PKC level and school level exam analysis reports are also created by the MIS team using data provided directly to the Council by the SQA.	
Strength of Internal Controls:	Strong

Control Objective 7: There are effective data input and validation controls.
Auditor's Comments: In relation to controls within the system which improved data quality, we noted that there was validation in the form of mandatory completion fields and drop down cells which only allowed specific inputs. We also noted that staff are required to update their own personal records and

information held on SEEMiS. It was noted that once a personal record is changed, it must be approved by system administrators before it can be live on SEEMiS.

There are regular reports produced to ensure data quality for the SEEMiS system. For example, at each of the schools sampled, it was noted that an annual check of data held on students takes place. This is done through asking parents/guardians to confirm, in writing, whether key contact information, including contact number and address, held is accurate. Any change of information held must be communicated in writing or in person. Records would then be updated by office staff. It was highlighted that there are also provisions in place for parents/guardians to contact schools in order to have records changed at any time throughout the school year.

In addition the MIS team has created a number of SEEMIS data quality reports which are accessible in every school and allow data to be checked for completeness. At a minimum these reports are run annually during collation of staff census and pupil census data for the Scottish Government.

Strength of Internal Controls:	Strong

Control Objective 8: Adequate backup, recovery and continuity procedures are in place.
Auditor's Comments: Disaster recovery, backups, and continuity of the system is the responsibility of SEEMiS LLP. Discussions with SEEMiS LLP highlighted that backups took place on a daily basis, and there were plans in place to introduce a mid-day backup in the near future. However, it was noted that backups of production data were not subjected to regular testing.   Discussions with Council staff highlighted that whilst the Council had sight of the SEEMiS LLP Backup Policy and Business Continuity Plan there was limited information available to them regarding the success of backups. Each of the secondary and all-through schools that were subjected to review were found to have sufficient continuity arrangements in place, which included reversion to a 'back to paper' system and maintaining paper copies of key information. Each school also had a Recovery plan in place which was subject to annual review.

Strength of Internal Controls:	Strong

Control Objective 9: There are appropriate audit facilities within the system to allow effective and regular monitoring of the application.
Auditor's Comments: Audit functionality within the system was found to be extremely limited. Discussions noted that, whilst it was possible to identify when users had logged in/ what users were logged in, it was not possible to identify what users had accessed a particular record. As a result of audit functionality limitations, there were no processes in place for

> the regular review of audit logs.
>
> We were informed that audit functionality was discussed at the SEEMiS Operational Management Group on 8 December 2015. It was stated that the difficulty of retrospectively adding audit functionality into existing legacy modules was recognised. It is anticipated that audit functionality will be considered as enhancements are requested and will be a feature of the next version of the product which is expected to be in place within the next 3-4 year period.

Strength of Internal Controls:	Weak

Management Action and Follow-Up

Responsibility for the maintenance of adequate and effective internal controls rests with management.

Where the audit has identified areas where a response by management is required, these are listed in Appendix 1, along with an indication of the importance of each 'action point'. Appendix 2 describes these action points in more detail, and records the action plan that has been developed by management in response to each point.

It is management's responsibility to ensure that the action plan presented in this report is achievable and appropriate to the circumstances. Where a decision is taken not to act in response to this report, it is the responsibility of management to assess and accept the risks arising from non-implementation.

Achievement of the action plan is monitored through Internal Audit's 'follow up' arrangements.

Management should ensure that the relevant risk profiles are reviewed and updated where necessary to take account of the contents of Internal Audit reports. The completeness of risk profiles will be examined as part of Internal Audit's normal planned work.

Acknowledgements

Internal Audit acknowledges with thanks the co-operation of staff within Education & Children's Services and the Corporate & Democratic Services – Corporate IT team during this audit.

Feedback

Internal Audit welcomes feedback from management, in connection with this audit or with the Internal Audit service in general.

Distribution

This report has been distributed to:

B Malone, Chief Executive

J Walker, Depute Chief Executive, HCC (Corporate and Community Development Services) and Chief Operating Officer

J Gilruth, Director of Housing & Community Care

A Taylor, Head of Corporate IT and Revenues

J Symon, Head of Finance

K Wilson, Corporate IT Manager

J Rogers, IT Team Leader (MIS)

K McNamara, Head of Strategic Commissioning and Organisational Development

G Taylor, Head of Democratic Services

P Dickson, Complaints & Governance Audit

External Audit

Authorisation

The auditor for this assignment was F Tahir (Scott-Moncrieff). The supervising auditor was P Kelly (Scott-Moncrieff).

This report is authorised for issue:

_____

Jacqueline Clark
Chief Internal Auditor
Date: 25 February 2016

Appendix 1: Summary of Action Points

No.	Action Point	Risk/Importance
1	User access profiles	Medium
2	Disaster recovery and backup test reports	Medium
3	Audit logging	High

Appendix 2: Action Plan

Action Point 1 - User access profiles

System administration at school level rests with Business Managers at secondary schools and in 'all through' schools with the MIS team responsible for primary schools.

At an individual school level, roles and responsibilities will vary. As a result, user profiles have been developed in response to specific needs at each school.

A formal process was developed in 2012 to review all user profiles in use across each establishment. We noted that the last reviews were performed in 2014. This covered 12 primary schools, 1 secondary school and three areas of the MIS team which represents approximately 20% of all establishments.

We also noted a minor issue in relation to consistency in providing access to supply teachers. In one school, all supply teachers were provided with access immediately, whereas in others they would only be provided with access when it became apparent that their tenure at the school would be more prolonged.

Management Action Plan

User profiles in Secondary and All Through Schools, which can be amended by Business Managers, will be reviewed on a rolling two year cycle.

Primary school, special school and central team user profiles, which can only be amended by the MIS team, will be reviewed based on a sample of schools/teams on an annual basis.

All user profile changes carried out by the MIS Team will be recorded on the IT Service Desk.

All user profile reviews will also be recorded on the IT Service Desk.

Importance:	Medium
Responsible Officer:	Jacquie Rogers, IT Team Leader
Lead Service:	Corporate & Democratic Services
Date for Completion (Month / Year):	May 2016
Required Evidence of Completion:	Annual User Profile Review Report

Auditor's Comments

Satisfactory

Action Point 2 - Disaster recovery and backup test reports

IT disaster recovery planning for the SEEMiS application and data backups are the responsibility of SEEMiS LLP. We noted that there is no requirement for SEEMiS to provide the Council with a report which identifies the level of backup success/failure or that they have appropriate and tested IT disaster recovery plans in place. Therefore, the Council has no assurance that the plans are suitable or that the system and all data can be restored from backup media.

Management Action Plan

The Council will write to the Chief Executive, SEEMiS LLP to request regular reports of backup and disaster recovery activities.

Importance:	Medium
Responsible Officer:	Jacquie Rogers, IT Team Leader
Lead Service:	Corporate & Democratic Services
Date for Completion (Month / Year):	May 2016
Required Evidence of Completion:	SEEMiS LLP response

Auditor's Comments

Satisfactory

Action Point 3 - Audit Logging

We found that the audit logging functionality within the system was ineffective. Whilst audit logging was capable of identifying and reporting when a user had logged in, it was not possible to identify specific user activity.

The limitations with regards to audit logging had been identified by the Council's MIS team. The issue had been raised at the SEEMiS Operational Management Group meeting on 8 December 2015, which was attended by representatives from each of the five SEEMiS User Groups and representatives from SEEMiS LLP. During the meeting it was agreed that additional audit logging would be considered for all new functionality.

The difficulty of retrospectively adding audit functionality into existing legacy modules was recognised. It is anticipated that audit functionality will be considered as enhancements are requested and will be a feature of the next version of the product which is expected to be in place within the next 3-4 year period.

Management Action Plan

The Council will write to the Chief Executive, SEEMiS LLP requesting that audit functionality is included in future system developments.

Importance:	High
Responsible Officer:	Jacquie Rogers , IT Team Leader
Lead Service:	Corporate & Democratic Services
Date for Completion (Month / Year):	May 2016
Required Evidence of Completion:	Response from SEEMiS LLP

Auditor's Comments

Satisfactory