6(i)(c)
12/271

Internal Audit Report
11-09 - Corporate
Information Security
May 2012

Final Report

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

Background and Introduction

This assignment forms part of the Internal Audit plan for 2011/2012, as approved by Audit Sub-Committee on 9 March 2011. Audit testing for the assignment took place during March and April 2012.

The Council maintains an Information Security policy the objective of which is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents. The purpose of the policy is to ensure the confidentiality, integrity and availability of the Council's information assets and ensure they are appropriately protected from all threats. The Council sets standards to support the policy. These standards and policy form the Information Security Management System (ISMS).

The ISMS designate the Depute Chief Executive as the Senior Information Risk Officer (SIRO) for the Council. The SIRO's responsibility is to maintain the policy, provide advice and guidance on its implementation, and to administer the ISMS. The ISMS stipulate that the following officers also have responsibility for the following areas:

- The Head of IT for all ICT infrastructure.
- The Head of Legal Services for advice on compliance with all statutory requirements.
- The Head of Human Resources for personnel issues.
- The Head of Property Management for establishing physical security standards.

In addition the Information Security Manager acts as a specialist adviser to the Council on all aspects of information security.

Acknowledgements

Internal Audit acknowledges with thanks the co-operation of the Chief Executive's and Education and Children's Services during this audit.

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 Objective: To ensure the adequacy of the governance arrangements for the Council's information security infrastructure	
Auditor's Comments: The Council's Information Security Management System (ISMS) is an in depth governance document detailing the Information Security infrastructure and a set of standards to support the Council's Information Security policy. There is scope for reviewing some aspects of the ISMS. The Information Security policy also needs to be approved by the relevant Committee. The take up of an 'essential' e-learning Information Security package is poor with only 31% of users and no elected members having undertaken this training. The training would benefit from updating. There is currently no provision for any information security briefing for temporary staff. Controls are in place to ensure agency staff procured via the procurement framework have signed a confidentiality clause, but no similar control exists for staff recruited from agencies outwith this framework. Controls are in place to remove computer access permission levels for leavers', but some permission levels have not been removed in a timely manner. Similar controls should be introduced for staff transferring posts. The Council's Information Technology Team daily routines include the backing up of data stored on computer servers to discs. There is currently no scheduled test work to evidence the recovery of data stored on these discs.	
Strength of Internal Controls:	Moderate

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.

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 Irons, Depute Chief Executive

J Fyffe, Executive Director (Education & Children's Services)

J Valentine, Executive Director (Environment Service)

D Burke, Executive Director (Housing and Community Care)

B Atkinson, Depute Director of Education & Children's Services

B Renton, Depute Director (Environment Service)

J Walker, Depute Director (Housing, Community Care & Finance)

S MacKenzie, Acting Head of Finance

I Innes, Head of Legal

T Yule, Head of Head of Corporate Business Change and IT

H MacKenzie, Head of Human Resources

D Henderson, Information Compliance Manager

E Sturgeon, Chief Exchequer Officer, Chief Executives - Financial Services

M Cowdery, Senior Exchequer Manager, Chief Executives - Financial Services

K Wilson, IST Business Manager

P Dickson, Complaints & Governance Officer

M Kay, Senior Committee Officer

External Audit

Authorisation

The auditor for this assignment was D McCreadie. The supervising auditor was D Farquhar.

This report is authorised for issue:

Jacqueline Clark
Chief Internal Auditor
Date: 16 May 2012

Appendix 1: Summary of Action Points

No.	Action Point	Risk/Importance
1	Action Plan - Government Information Security Measures	Medium
2	Review by Communications Electronics Security Group	Low
3	Information Security Policy	Low
4	Payment Card Industry Data Security Standards	Medium
5	Information Security Management System (ISMS)	Medium
6	Responsibility for Information Security	Medium
7	Information Security Training	Medium
8	Computer Access Rights	Medium
9	ICT Back Up of Servers	Medium
10	Baseline Personnel Security Standard	Medium

Appendix 2: Action Plan

Action Point 1 - Action Plan - Government Information Security Measure

A report to the Executive Officer Team entitled 'Government Data Handling Reports' of September 2008 details information security measures based on recommendations contained in various Government reports.

The report is supplemented by the Information Management Strategy 2009 - 2012 which states that by March 2009 the Council had developed an action plan to implement the relevant Government information security recommendations with a target date for implementing the recommendations being December 2011. The Service provided copies of the action plans dated 'Update July 2009'. Testing confirmed the plans stipulated target dates of up to December 2010. The reference numbers in the plans were also linked to the above security recommendations.

The Service provided a more up to date copy of the action plan dated 2011 however, this plan did not refer to the original reference numbers from the original security recommendations or name the responsible officer(s) for actions. The Information Compliance Manager advised that responsibility for monitoring the Information Security action plan had been delegated to the Policy & Governance Group and the 2011 plan was, in fact, the Information Security plan for the Information Security team and included additional actions to those in the 2009 plan.

Management Action Plan

1) The Information Compliance Manager will ensure the 2012 Information Security plan includes completion dates and details progress made with individual actions. The revised plan will be approved by the Policy and Governance Group.

2) The revised Information Management Strategy Information Security section will be updated to reflect the above revised Information Security action plan

Importance:	Medium
Responsible Officer:	D Henderson, Information Compliance Manager
Lead Service:	Chief Executive's Service
Date for Completion (Month / Year):	1) July 2012 2) December 2012
Required Evidence of Completion:	1) Approved 2012 Information Security action plan 2) Extract from revised Information Management Strategy

Auditor's Comments

Satisfactory

Action Point 2 - Review by Communications Electronics Security Group

In August 2011 an assessor from the Communications Electronic Security Group (CESG) having responsibility for providing information assurance to the UK Government, carried out a review of the Council's compliance with the Government Secure Extranet (GSx) Code of Connection.

Their Executive Summary report reads that overall, Perth and Kinross Council demonstrated a reasonable understanding of the requirements and the current connection to the GSx does not appear to represent an unmanageable risk. The Information Compliance Manager provided the Auditor with the recommendations from the review.

At the date of audit testing the report and the recommendations had not been reported for approval to any Group. The Information Compliance Manager advised that an update report detailing these actions will be submitted to a future meeting of the Policy and Governance Group.

Management Action Plan

The Information Compliance Manager will provide an update report detailing the actions from the Communications Electronics Security Group (CESG) review to a future Policy and Governance Group meeting.

Importance:	Low
Responsible Officer:	D Henderson, Information Compliance Manager
Lead Service:	Chief Executive's Service
Date for Completion (Month / Year):	June 2012
Required Evidence of Completion:	Policy and Governance Group Report/Minutes

Auditor's Comments

Satisfactory

Action Point 3 - Information Security Policy

The Council's Scheme of Administration stipulates two of the roles of the Strategic Policy and Resources (SP&R) Committee are 'To determine strategic policy objectives and priorities for the Council' and determine and implement the Council's policies in relation to information systems and technology.

Also, a Policy and Governance Group paper of 17th April 2009 states that once approved the amended Information Security (IS) policy will be presented to SP&R. The Auditor was unable to find evidence of any approval of the IS policy by SP&R, however, the policy was approved by the then Corporate Management Team in March 2004. The Information Compliance Manager had been advised that, as the IS Policy is not considered to be a 'strategic policy'; it was not presented to the Strategic Policy & Resources Committee.

In addition, the Information Security policy refers to the former Corporate Services and states the policy will be reviewed every three years, however the latest published version is dated June 2008.

The policy also stipulates the Head of Legal Services is responsible for the policy maintenance which contradicts the IS policy in the Information Security Management Systems documentation which states this is the responsibility of the Senior Information Risk Officer (the Depute Chief Executive).

Management Action Plan

The Information Compliance Manager will update the Information Security policy to reflect the correct Service title and ensure consistency with regards to the named officer responsible for the maintenance of the Information Security (IS) policy and the changes approved by the Policy and Governance Group.

Importance:	Low
Responsible Officer:	D Henderson, Information Compliance Manager
Lead Service:	Chief Executive's Service
Date for Completion (Month / Year):	June 2012
Required Evidence of Completion:	Revised IS Policy

Auditor's Comments

Satisfactory

Action Point 4 - Payment Card Industry Data Security Standards

The Council's bank and managed service provider require the Council to adhere to the Payment Card Industry Data Security Standard (PCIDSS) to facilitate the processing of debit and credit card payments. To demonstrate adherence with the standards the Council is required to complete a self assessment questionnaire (SAQ) for the Council's bank and managed service provider's bank. At the date of audit testing the SAQ was in the process of being completed for submission.

The standard requires that to ensure compliance with the PCIDSS the Council annually monitors the compliance status of service providers who process debit and credit card payments on their behalf. At the date of audit testing the Service had not yet obtained such confirmation of compliance; however the Service subsequently stated that this has now been rectified.

In March 2012 the Service emailed debit and credit card regulations to staff, these regulations detailed the expected standards when processing card payments. However, staff were not required to confirm receipt of the regulations. The Service subsequently advised that Read Receipts had been requested from staff to evidence receipt of the regulations.

Management Action Plan

1) The Service will complete and submit the Self Assessment Questionnaire relating to the Payment Card Industry Data Security Standards (PCIDSS).

2) The Service will devise a checklist to be completed annually to evidence that each service provider supplies assurances that they are compliant with the PCIDSS. The Service will also introduce a checklist to evidence read receipts are obtained when debit and credit card regulations are emailed to relevant staff.

Importance:	Medium
Responsible Officer:	M Cowdery, Senior Exchequer Manager
Lead Service:	Chief Executive's Service
Date for Completion (Month / Year):	1) December 2012 2) July 2012
Required Evidence of Completion:	1) Two completed SAQs 2) Checklist regarding provider's PCIDSS compliance & obtain read receipts.

Auditor's Comments

Satisfactory

Action Point 5 - Information Security Management System (ISMS)

The Information Compliance Manager explained the Council's ISMS are a set of standards produced to support the Council's Information Security Policy.

Audit testing revealed scope to improve how the ISMS are communicated, for example:

- The lack of introduction in the relevant intranet page.
- No reference to the ISMS in the Information Security training package.

The ISMS refers to the following titles:

- An Information Security Management Forum whose Council title is the Policy and Governance Group
- Job titles of Information Security Manager and Information Security Officer with no such titles in the Council's 'contacts on-line' directory. (The closest titles being Information Officer (Information Security) and Information Compliance Manager)

The Service advised the ISMS titles were based on ISO 27000 definitions.

Also, the ISMS 'Policy' tab includes an introduction which is not clear from the menu and the header tab is confusingly 'SecureAware 4.1.3' not the ISMS. The Information Compliance Manager advised the ISMS is a software package and that the policy tab or title cannot be amended.

The ISMS omits responsibility for Information Security training and stipulates that every two years the Information Security Officer should instigate a review by an appropriate third party, with relevant certification, skills and experience of 'the implementation of information security within the Council' this is 'to provide assurance that organizational practices comply with the policy' The Auditor was unable to find evidence of any such review.

The ISMS further states the Senior Information Risk Officer should oversee the development of an information risk policy. The Auditor was unable to identify any such policy. The Service advised that although there is no information risk policy details of what such a policy would contain are already included in the ISMS.

Management Action Plan

The Information Compliance Manager is drafting a three year information security awareness plan that will include how the ISMS are communicated. This plan will be approved by the Policy and Governance Group.

The Information Compliance Manager will update the relevant intranet site page to include an introduction to the Information Security Management System (ISMS).

The ISMS will be updated to include responsibility for Information Security training and clarify the titles of Information Security Management Forum, Information Security Manager and Information Security Officer.

The Information Compliance Manager will amend the wording in the ISMS to clarify that the requirement for the Information Security Officer to instigate a review by an appropriate third party is only required where the Information Compliance Manager deems this action appropriate. The ISMS requirement for a dedicated information risk policy will also be reviewed or removed.

Importance:	Medium
Responsible Officer:	D Henderson, Information Compliance Manager
Lead Service:	Chief Executive’s Service
Date for Completion (Month / Year):	July 2012
Required Evidence of Completion:	Revised intranet page, updated ISMS and approved information security awareness plan.

Auditor’s Comments

Satisfactory

Action Point 6 - Responsibility for Information Security

The Council's Information Security Management System (ISMS) stipulates that Employees' responsibilities for information security be included in the terms and conditions of contracts of employment. Audit testing revealed the terms and conditions pages on the intranet site makes no reference to information security. Also, there is no reference to information security responsibilities in the Statement of Employment Particulars (SEP), but the SEP includes confidentiality clauses.

Audit testing confirmed the adequacy of the processes in place to ensure contracts for agency staff employed via the Council's eprocurement route contains confidentiality clauses. However, Services may employ staff via agencies not included in the eprocurement system which could result in the lack of any such confidentiality clause for these staff.

In addition, there is no standard induction training for agency/temporary staff that refers to information security or the need to maintain confidentiality.

Management Action Plan

1) The Human Resources PEP Team will liaise with the Information Compliance Manager to arrange for the intranet's (ERIC) Terms and Conditions Pages to refer to Information Security. The Human Resources Workforce Management Team will also liaise with the Information Compliance Manager to arrange for guidance to be issued to Managers regarding the specific need to ensure confidentiality clauses are checked when agencies not on the eprocurement list are used.

2) The Human Resources Workforce Management Team will liaise with the Information Compliance Manager to arrange for the short term resourcing toolkit to include Managers guidance in relation to information security requirements and a model induction checklist for agency/contract/short term staff incorporated in this.

Importance:	Medium
Responsible Officer:	K Ridley, Personnel Manager
Lead Service:	Chief Executive's Service
Date for Completion (Month / Year):	1) June 2012 2) December 2012
Required Evidence of Completion:	1) Updated ERIC page and guidance regarding confidentiality clause 2) Short term resourcing toolkit

Auditor's Comments

Satisfactory

Action Point 7 - Information Security Training

The introduction to the Information Security elearning package launched in December 2007 stipulates elected members and employees of Perth and Kinross Council should complete the training. Audit testing revealed no elected members and only 1279 of 4134 elearning users had undertaken this ‘essential’ training.

The e-learning training package is also in need of review as evidenced by:

- The training including statistics from 2005.
- No reference to the Council’s Information Security Management System.
- The anti virus section stating delete spam emails without forwarding which contradicts spam email guidance on the Council’s intranet site.
- The training states take care with data stored in a USB, but doesn’t refer to the intranet guidance regarding security for certain data stored on a USB.

In line with Action Point 5 testing revealed the elearning training refers to the roles of the Information Security Manager and the Information Security Officer. However, there are no such job titles in the Council’s ‘contacts on line’ directory.

Audit testing revealed the intranet elearning page contained a hyperlink to a Corporate Training Directory which had not been used since 2010. The Service (Organisational Development) subsequently removed this hyperlink.

In addition, the ISMS stipulate the Senior Information Risk Officer (SIRO) should undertake strategic information risk management training annually. The Auditor was unable to identify evidence of any such training. The Information Compliance Manager advised that a new SIRO was due to be appointed in the summer of 2012.

Management Action Plan

1) The Information Compliance Manager will remind all Services via the Policy and Governance Group of the need for the Information Security training to be undertaken. The Information Compliance Manager will remind elected members that they need to undertake the Information Security training.

2) The Information Compliance Manager will meet with the new SIRO to discuss the SIRO role, the need to update the e-learning package and progress the ISMS requirement that the SIRO should undertake strategic information risk management training annually.

3) The Information Compliance Manager will arrange for the replacement of e-learning Information Security training package to be included in the 3 year Information Security Plan.

4) Once funding is available the e-learning Information Security training package will be updated and will refer to the Council’s Information Security standards linked to corresponding Information Security guidance on the Council’s intranet site.

Importance:	Medium
Responsible Officer:	D Henderson, Information Compliance Manager
Lead Service:	Chief Executive's Service
Date for Completion (Month / Year):	1) June 2012 2) & 3) September 2012 4) March 2013, for review of progress
Required Evidence of Completion:	1) Confirmation Members are informed of need to undertake training and extract from P&G minutes regarding training in Services 2 & 3) Confirmation Information Compliance Manager met with SIRO and discussed risk management training requirements and copy of 3 year plan. 4) Updated e-learning package

Auditor's Comments

Satisfactory

Action Point 8 - Computer Access Rights

Line managers are responsible for the prompt submission of termination documentation to ensure the removal of leavers' computer access rights. Audit testing of core Active Directory User permission access levels for 20 randomly selected leavers' revealed 4 such permission levels had not been removed.

Information Technology (IT) Service advised that since November 2011 a leavers' report had been produced by the Employment Services Team to assist in ensuring such access levels for leavers were removed in a timely manner. Previously the IT Service relied on individual Services to advise them of their staff leavers. However, audit testing revealed the December 2011, January and February 2012 reports were not actioned at the date of audit testing. IT advised there had been a delay in receiving these reports.

No similar reports are produced in relation to staff transferring posts. IT relies on individual Services advising them of their staff transfers on a case by case basis. The lack of a systems generated report detailing staff transfers may result in staff being granted incorrect computer access levels.

There is a need to have an automated process for generating staff leavers/transfer reports and a robust IT process to action these reports in a timely manner as failure to remove permission levels may result in unauthorised access to Council systems.

Management Action Plan

1) The IT Service will liaise with the Employment Services Team (EST) to agree a timetable of events that ensure leavers reports are produced on a monthly basis. These reports will be emailed by EST to IT Helpdesk to start the IT process for User Maintenance in a timely manner. The IT Service will ensure that thereafter each of these reports is actioned in a timely manner.

2) The IT Service will liaise with EST with a view to agreeing the parameters to develop a monthly exception report that details staff having transferred duties. The IT Service will ensure that thereafter these reports are actioned in a timely manner.

Importance:	Medium
Responsible Officer:	J Cochrane, Team Leader Application Support
Lead Service:	Education and Children's Services
Date for Completion (Month / Year):	1) June 2012 2) Dec 2012
Required Evidence of Completion:	1) Confirmation access rights for 4 leavers removed. Recently actioned leavers report 2) Transferring staff report.

Auditor's Comments

Satisfactory

Action Point 9 - IT Back Up of Servers

The stated objective of the Council's Information Security policy is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents.

Audit testing confirmed IT scheduled work includes the daily backing up of data stored on computer systems to dedicated disk storage pools.

There is no scheduled work that evidences recovery of data stored on these disks as the physical recovery of such data only takes place if a Service highlights issues with their system(s), or a scheduled back up fails.

There is a risk data on computer systems might not be recoverable if planned work does not include the scheduled test restoration of such data.

Management Action Plan

The Service will develop a schedule to ensure that all servers have their backup and recovery processes tested on an annual basis.

Importance:	Medium
Responsible Officer:	C Watson, Principal Development Engineer
Lead Service:	Education and Children's Services
Date for Completion (Month / Year):	June 2012
Required Evidence of Completion:	Extract from schedule showing test recoveries.

Auditor's Comments

Satisfactory

Action Point 10 - Baseline Personnel Security Standard

The Information Security Management System require all new employees to be validated to Government 'Baseline Personnel Security Standard' which comprises verification of the following four main elements:

- Verification of identity
- Employment history
- Nationality and immigration status
- Unspent criminal record.

Whilst the Council's recruitment processes cover most of the above elements the process does not specifically stipulate the checking of nationality and immigration status. The Service advised the recruitment application form requests this information, but accepted that further guidance could be issued to Managers in respect of checking the nationality of applicants.

The recruitment procedures states that employees doing regulated work with children or vulnerable adults need to have a disclosure check carried out. The Information Compliance Manager advised the ISMS requirement for a disclosure check was intended to refer to employees with access to the UK Government Secure Extranet (GSx users).

Management Action Plan

1) The Service will update the process map used by Managers to assist in the recruitment process to stipulate the need for Managers to check the nationalities of new employees to their passports and the immigration status/ID cards for non European Economic Area (EEA) applicants. A Managers Factsheet will also be issued giving guidance in this respect.

2) The Information Compliance Manager will update the Information Security Management System standard to clarify that Baseline Personnel Security Standard needs to be carried out for employees with access to the UK Government Secure Extranet site (GSx users).

Importance:	Medium
Responsible Officer:	1) K Ridley, Personnel Manager 2) D Henderson, Information Compliance Manager
Lead Service:	Chief Executive's Service
Date for Completion (Month / Year):	1) & 2) June 2012
Required Evidence of Completion:	1) Recruitment process map 2) Updated ISMS re BPSS for GSx users.

Auditor's Comments

Satisfactory