Internal Audit Report
Corporate
Software Licences 13-02
October 2013

Final Report

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

Background and Introduction

This audit was carried out as part of the audit plan for 2013/14, which was approved by the Audit Committee on 27 March 2013.

Software applications allow the Council to perform its statutory functions, enable the achievement of political priorities and facilitate the retention and management of records. Software licences document permissions and restrictions on the use of software without necessarily passing ownership to the user. The rights of software owners are protected by the Copyright, Designs and Patents Act 1988 and contract law.

Controls over information assets are documented in the Council's Information Security Management System (ISMS) which comprises the Information Security Policy and supporting standards. These are key governance documents for Information Security within the Council. The Policy sets out the principles and the standards provide supplementary detail regarding various aspects of Information Security, the system controls and the behavioural requirements to maintain the confidentiality, integrity and availability of the Council's information assets. Immediately prior to logging in to any networked computer the user is asked to agree that they are familiar, and will comply, with the Policy.

Under the Policy, it is the responsibility of the Council's Senior Information Risk Officer (SIRO), the Executive Director (Environment) to maintain the ISMS. Operationally, Information Technology (IT) services are provided across the Council by the IT Division in Education and Children's Services.

Acknowledgements

Internal Audit acknowledges with thanks the co-operation of the IST Business Manager and his team and all the officers in all Services who took the time to locate the requested software licences 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 arrangements governing software licences	
Auditor's Comments: The ISMS sets out the responsibilities of members of staff and elected members with regard to Information Security. The ISMS comprises the Information Security Policy and a range of standards which comprehensively cover the topic. Agreement to comply with Information Security Policy, by Council staff and elected members, is part of the logging in process for Council computers. Specifics relating to legislation surrounding software licences, intellectual property and copyrights are contained within the Compliance section of the ISMS as are the responsibilities and internal controls for software assets. In addition, in July 2013, IT issued a paper "Governance of the Council's Software Assets" to members of the Information Technology teams. The document sets out the Council's policy in respect of software copyright, intellectual property rights and the responsibilities of members of IT staff to ensure that all software is properly licensed prior to installation. The document had been produced after consultation with the Federation Against Software Theft (FAST) to ensure that a robust framework for IT workers within the Council is in place. For IT staff, the rules relating to the moving, copying and installation of software contained in the ISMS is endorsed by the Governance Rules for Software Assets. It is anticipated that this document will be developed and further cascaded throughout the Council to reinforce responsibilities for all members of staff in relation to Software Licences. In accordance with the ISMS, acquisition of IT software and equipment should also take Information Security into account. Pages on ERIC for procurement of software did not include reference to IT to confirm the adequacy of licensing arrangements or compatibility with infrastructure. The Information Security Policy and the relevant supporting Standards provide new recruits with the necessary information regarding their responsibilities towards Information Security however it was found that the Policy had been removed from the checklist of document for new starts to be aware of in the review of induction in January 2013. Whilst the ISMS state that employees responsibilities towards Information Security must be included in the Terms and Conditions of Employment it was found that this is not the case. Standard Statements of Employment Particulars and The Code of Conduct for Employees did not include adherence to Information Security Policies.	
Strength of Internal Controls:	Moderately Strong

Control Objective: To ensure that the Council is licence compliant
Auditor's Comments: An annual "True Up" exercise is undertaken to ensure that all Microsoft Office applications are appropriately licensed under the Council's Enterprise Agreement.

Any discrepancy between the MS Office licences purchased and those needed is identified and rectified. Other than this annual True-Up however, there is, no reconciliation undertaken by IT to ensure the adequacy of other licence agreements in place. Due to the Council's Group Permissions Policy, the installation of software onto Council networked machines is inhibited without sufficient authority so that software cannot be copied on multiple machines outwith the terms of the licence agreement. However Internal Audit found that it was possible to successfully install some proprietary software without the required authority. Upgrades of existing software cannot be installed beyond the permissions made available by the supplier which will not be greater than licences which have been purchased. In addition, officers must satisfy IT engineers that there are sufficient licences to enable the installation of software. Due to the historical nature of some of the software applications and changing personnel over time, licence documents were not always available, and engineers sometimes have to accept written confirmation from the Asset Owner only. Under the ISMS, Heads of Service are required to annually submit to IT a record of software assets used under their area of responsibility. No such record is submitted by any of the Heads of Service, is asked for by IT or is confirmed by the Information Compliance Manager. A register of software licences is held on the Asset Register (IT Help Desk). The register currently does not include details of the number of licences held – or the model for the licences (per user, concurrent user, per p.c. etc.). Sample testing of the register details identified that not all systems identified on the register are systems which are, or have been, in use. In accordance with the ISMS, the Council must be in a position to provide proof of claim with regard to its use of software under licence. Of a sample of 36 applications which were recorded on the Asset Register, Services were unable to provide the Auditor with documents for 4 applications (11%). Where licences were held all software applications in use across the Council were shown to be adequately licensed.

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 Fyffe, Executive Director (Education & Children’s Services)

J Valentine, Executive Director (Environment)

A Taylor, Head of Service IT

J Symon, Head of Finance

K Wilson, Corporate IT Manager

I Innes, Head of Legal Services

D Henderson, Information Compliance Manager

K Ridley, Senior Personnel Manager

G Boland, Senior Business & Resources Manager

G Taylor, Head of Democratic Services

P Dickson, Complaints & Governance Officer

External Audit

Authorisation

The auditor for this assignment was A Gallacher. The supervising auditors were D Farquhar and J Clark.

This report is authorised for issue:

_____

Jacqueline Clark
Chief Internal Auditor
Date: 1 October 2013

Appendix 1: Summary of Action Points

No.	Action Point	Risk/Importance
1.	Software Asset Register	Medium
2.	Software Licence Records	Medium
3.	Proof of Claim	Medium
4.	Software Installation	Medium
5.	Annual Reconciliation	Low
6.	Software Procurement	Medium
7.	Governance Guidance	Low
8.	Terms & Conditions	Medium
9.	Information Security - Induction Process	Medium

Appendix 2: Action Plan

Action Point 1 - Software Asset Register

The Asset Register which is held as part of the IT Help Desk holds details of systems that are actively or historically employed by the Council. Such details include the name of the system, the Service, the responsible manager, the costs of support and maintenance, and whether the system is active. Whilst the ISMS does not provide guidance as to the required format for software licence records, details which are not included on the Asset Register are the number of licences or the model of the licence (e.g. per device, per user, per concurrent user). Without these details being recorded on the register, it would be difficult to establish or confirm compliance with licence requirements and restrictions.

It is understood that the Register is to be further developed during 2013 and that, as a bespoke system, these fields could be added.

Management Action Plan

IT will:

- Create bespoke fields within the Council's Service Desk System Application configuration item (CI) template to record improved software licence information.
- Ensure existing procedures for the recording of ICT assets in the Service Desk are updated to reflect changes to the System Application (CI) template.

Importance:	Medium
Responsible Officer:	S Cannon, IT Team Leader, Customer and Business Services
Lead Service:	Education& Children's Services
Date for Completion (Month / Year):	October 2013
Required Evidence of Completion:	• Revised System Application CI template • Service Desk Procedures updated to reflect revised System Application CI template

Auditor's Comments

Satisfactory

Action Point 2 - Software Licence Records

The ISMS has a number of requirements with regard to Software Asset records. These include:

- records must be kept linking software licences to the computers on which the software is used;
- records of transfer or deletion of licensed software must be kept for at least 2 years;
- these records must take the form of an entry on the software asset register, and that a software asset register should be kept up to date at a departmental level; and
- Heads of Service are responsible for returning the software asset register with their hardware asset register on an annual basis to I(S)T;

Enquiries were made of a number of Heads of Service for licence records of 36 selected software applications, taken from the Asset Register. The following issues of non-compliance with the ISMS were identified:

None of the licence details provided for any of the systems was linked to a particular device;

Some of the applications of the selected systems which were listed on the Asset Register had either never been in use or had not been in use for more than two years; and

IT confirmed that no Services submitted a register of software assets annually, that IT did not request such a register and that the Information Compliance Manager did not confirm that this was being done.

Management Action Plan

a) Nominated Service IT representatives will:

- Write to staff in their Service to remind them of their responsibilities in respect of software and system licensing, as defined in the Council's ISMS.
- Ensure that a process is in place within their Service to timeously share information about changes to their Service's system landscape with the Head of IST, to support maintenance of a current Council Asset Register.

b) IT will:

- Annually ask Executive Directors to validate the system licence data for their Service held on the Council's ICT Asset Register and update the register based on Services' responses.

Importance:	Medium

Responsible Officer:	a) (i) E. Sturgeon, Chief Exchequer Officer (ii) J. Cockburn, Finance Manager (iii) S. Strathearn, Business Improvement Manager (iv) N. Ballantine, TES CAM Team Leader (b) S Cannon, IT Team Leader, Customer and Business Services
Lead Service:	(a) (i) Chief Executive's Service (ii) Education & Children's Services (iii) Housing & Community Care (iv) The Environment Service (b) Education & Children's Services
Date for Completion (Month / Year):	(a) (i) – (iv) November 2013 (b) November 2013
Required Evidence of Completion:	(a) • Communication to staff in each service re: ISMS. • Communication in each Service re the process for transmission of system application update information to IT Service. (b) Documented process for annual system application validation check.

Auditor's Comments

Satisfactory

Action Point 3 - Proof of Claim

The Council's ISMS states that the "Council must be in a position to prove its claim with regard to software licences" and provides examples of circumstances where the council will have rights to use software, under licence arrangements.

A sample of 36 applications was selected from the Council's Asset Register and Services were asked to provide appropriate records. In 4 instances, Services were unable to provide sufficient documentation with regard to licences to support their current use of software applications.

Of the remainder, in at least 5 instances, enquiries had to be made to suppliers for licence details as they could not be found within the Council.

Management Action Plan

Nominated IT Service representatives will

- Identify all rights and entitlements conferred by system applications for which they are responsible;
- Share information about their Service's system application rights/ entitlements with IT to support maintenance of the Council's Asset Register.

Importance:	Medium
Responsible Officer:	(i) E. Sturgeon, Chief Exchequer Officer (ii) J. Cockburn, Finance Manager (iii) S. Strathearn, Business Improvement Manager (iv) N. Ballantine, TES CAM Team Leader
Lead Service:	(i) Chief Executive's Service (ii) Education & Children's Services (iii) Housing & Community Care (iv) The Environment Service
Date for Completion (Month / Year):	November 2013
Required Evidence of Completion:	Extract of System Application configuration Items within the PKC ICT Asset Register

Auditor's Comments

Satisfactory

Action Point 4 - Software Installation

It is the Council's policy that Council Hardware Assets are configured to prevent the installation of software not licensed to the Council.

As part of testing, and with the knowledge of IT, the Auditor found that proprietary software could, in some instances, be installed in Council desktop hardware.

IT Management stated that for practical operational purposes, the current PKC desktop images allow individual users to install some proprietary software in exceptional, low-risk circumstances. In these instances, the software writes to individual users' profiles rather than the network, thus mitigating associated technical risk.

IT carry out testing to assess and manage this risk.

Management Action Plan

It is the responsibility of individual staff to read and comply with the licence terms and conditions specific to the software they are seeking to install. An amendment will be made to the Council's Software Governance Approach document to clarify this responsibility.

Importance:	Medium
Responsible Officer:	Susan Cannon, IT Team Leader, Customer and Business Services
Lead Service:	Education & Children's Services
Date for Completion (Month / Year):	31 December 2013
Required Evidence of Completion:	Minutes of CRG re approval of Software Governance Approach

Auditor's Comments

Satisfactory

Action Point 5 - Annual Reconciliation

An annual reconciliation (True Up) is undertaken by IT to ensure that Microsoft Office software estate installed on computers and in general use across the Council is properly licensed in line with the Council's portfolio of Microsoft Agreements.

Currently there is no systematic routine confirmation, by either IT or by Services reporting to IT, that there are adequate licences for the use of service-specific applications.

Management Action Plan

IT will:

- Seek Corporate Resources Group approval for a Software Governance Approach paper to clarify Services' roles and responsibilities in respect of software asset management.
- Write annually to all Executive Directors to reiterate their responsibility for software compliance within their Service. As part of this communication, Executive Directors will be asked to confirm to IT, for systematic recording purposes, that a true up reconciliation of entitlements-v-deployments has been completed in respect of any ICT system for which they are responsible.

Importance:	Low
Responsible Officer:	S Cannon, IT Team Leader, Customer and Business Services
Lead Service:	Education& Children's Services
Date for Completion (Month / Year):	December 2013
Required Evidence of Completion:	• Minutes of CRG • Emails to Executive Directors

Auditor's Comments

Satisfactory

Action Point 6 - Software Procurement

In accordance with the ISMS, acquisition of IT software and equipment should also take Information Security into account and software licensing forms part of the Information Security regime. The ISMS also states that Services should ensure that they purchase the required software licences.

Procurement pages on ERIC which provide guidance on purchasing of IT products were found not to reinforce these requirements, to direct users to IT as a route to procurement and to ensure the compatibility with the infrastructure.

The IT Buyers Guide focuses on IT equipment although it discusses software and identifies 2 educational software packages "which do not require installation or have licensing implications and do not need to be included on the Council's Asset Register." This is misleading as licensing restrictions apply to both named packages.

Procurement pages on ERIC identify 6 suppliers of Educational Software as being under contract but there are no notices on the page to ensure that prospective purchasers are to inform IT in advance to ensure compliance with ISMS thereby confirming the adequacy of licensing arrangements.

Management Action Plan

a) IT will update the IT Buying Guide to reflect the requirements of ensuring that IT are involved with the purchasing of all IT products.

b) Procurement pages on ERIC for ICT ordering will be amended to reflect the requirements of Services in relation to the purchasing of the required licences

Importance:	Medium
Responsible Officer:	a) S Cannon, IT Team Leader, Customer and Business Services b) L Prentice, eProcurement Manager
Lead Service:	a) Education & Children's Services b) Housing & Community Care
Date for Completion (Month / Year):	a) October 2013 b) October 2013
Required Evidence of Completion:	a) Revised IT Buyers Guide b) Updated Procurement Pages

Auditor's Comments

Satisfactory

Action Point 7 - Governance Guidance

The governance document issued to IT engineers states that any IT staff member carrying out software installation activities must request confirmation from a customer of available entitlements/licences before carrying out any installations at their request. However, enquiries revealed that licence documents were not always made available, and engineers sometimes have to accept written confirmation of the entitlements and licences from the Asset Owner only.

It is accepted that purchases of many of the Council's software applications are historical, however the rights bestowed through licensing to the Council should be checked prior to any installations/upgrade to ensure that all licence terms are met.

Management Action Plan

IT will write to all Executive Directors to remind them of their responsibilities under the ISMS for software compliance within their Service.

Importance:	Low
Responsible Officer:	S Cannon, IT Team Leader, Customer and Business Services
Lead Service:	Education & Children's Services
Date for Completion (Month / Year):	October 2013
Required Evidence of Completion:	Emails to Executive Directors

Auditor's Comments

Satisfactory]

Action Point 8 - Terms & Conditions

Whilst the ISMS states that employees' responsibilities towards Information Security must be included in the Terms and Conditions of Employment, this was found not to be the case.

For employees whose terms and conditions are subject of the Single Status agreement, the Statement of Employment Particulars makes no reference to Information Security, although the statement does refer to the Employee Code of Conduct. The Statement of Employment Particulars for Teachers makes no specific reference to either Information Security or the Employee Code of Conduct.

Moreover, the Employee Code of Conduct does not refer to Information Security directly, only the Communications Security Policy. This policy which forms part of the ISMS does not address the behavioural requirements set out in the ISMS, which is comprehensive. Similarly, there is no direct reference in the Achieving and Maintaining Standards policy and procedure to Information Security.

Management Action Plan

Human Resources are in the process of revising the Code of Conduct to include reference to the Information Security Policy. Statements of Employment Particulars will be amended for Single Status and Teachers to include the revised Code of Conduct.

Importance:	Medium
Responsible Officer:	K Ridley, Personnel Manager
Lead Service:	Chief Executive's
Date for Completion (Month / Year):	September 2013
Required Evidence of Completion:	Revised Statement of Employment Particulars and Revised Code of Conduct

Auditor's Comments

Satisfactory

Action Point 9 - Information Security - Induction process

The induction process for new starts includes checklists which set out a number of topics and documents with which new starts are to familiarise themselves at the start of their employment. Information Security and the Information Security Policy was removed from the checklist during a review in January 2013.

Management Action Plan

Human Resources will revise the Induction Checklist to include the Information Security Policy as a Day 1 to Day 3 activity.

Importance:	Medium
Responsible Officer:	K Ridley, Personnel Manager
Lead Service:	Chief Executive's
Date for Completion (Month / Year):	September 2013
Required Evidence of Completion:	Revised Checklist available on ERIC

Auditor's Comments

Satisfactory