

REPORT TO: SCRUTINY COMMITTEE – 25 JUNE 2013

REPORT ON: INTERNAL AUDIT REPORTS

REPORT BY: CHIEF INTERNAL AUDITOR

REPORT NO: 280-2013

1.0 PURPOSE OF REPORT

To submit to Members of the Scrutiny Committee a summary of the Internal Audit Reports finalised since the last Scrutiny Committee.

2.0 RECOMMENDATIONS

Members of the Committee are asked to note the information contained within this report.

3.0 FINANCIAL IMPLICATIONS

None

4.0 MAIN TEXT

4.1 The day-to-day activity of the Internal Audit Service is primarily driven by the reviews included within the Internal Audit Plan. Broadly, on the completion of a specific review, a report which details the audit findings and recommendations is prepared and issued to Management for a formal response and submission of Management's proposed action plan to take the recommendations forward. Any follow-up work subsequently undertaken will examine the implementation of the action plan submitted by Management.

4.2 Executive Summaries for the reviews which have been finalised in terms of paragraph 4.1 above are provided at Appendix A. Within each Executive Summary the prime aim is to provide both Members and Management with key information which includes the reason for undertaking the review, summary financial data and statistics, the areas encompassed within the review and specific areas which were excluded, the principal audit objectives, an audit opinion on the adequacy of the systems and control framework of the area reviewed, the key conclusions based on the audit findings and recommendations and a summary of Management's response to the audit report. The full reports are available to Members on request.

5.0 POLICY IMPLICATIONS

This report has been screened for any policy implications in respect of Sustainability, Strategic Environmental Assessment, Anti-Poverty, Equality Impact Assessment and Risk Management. There are no major issues.

6.0 CONSULTATIONS

The Chief Executive, Director of Corporate Services and Head of Democratic and Legal Services have been consulted on the content of this report.

7.0 BACKGROUND PAPERS

None

Sallie Dailly, Chief Internal Auditor

DATE: 03 June 2013

i) INTERNAL AUDIT REPORT 2011/32

Client	Social Work
Subject	Community Equipment Services

Introduction

A review of the arrangements in place within the Council for the provision of community equipment was part of the planned internal audit work.

In December 2009 the Scottish Government issued national Guidance on the Provision of Equipment and Adaptations. This Guidance was introduced to assist local authorities and their NHS partners to modernise and integrate their equipment and adaptation services within the wider community care context and establish a more consistent approach nationally. A suite of materials, including good practice guides and evaluation toolkits, was also developed to support local equipment services to effectively develop, deliver, manage and monitor the provision of equipment.

Equipment is defined in the Guidance as any item or product system, whether acquired commercially or off the shelf, modified or customised that is used to increase the functional capabilities of individuals with disabilities. Community equipment includes equipment for daily living, people with sensory impairments, communication aids and telecare products.

In Dundee, the community equipment service is progressing towards a joint service, known as the Dundee Joint Equipment Service, delivered by the Council in conjunction with NHS Tayside. This service includes the provision of impartial advice, the assessment of need, ordering and supply of equipment through a joint community equipment store and equipment demonstrations. In addition to key NHS professionals, the Council's occupational therapists are responsible for assessing need, prescribing appropriate community equipment and providing advice.

Expenditure on the community equipment service in 2011/12 and 2012/13 was of the order of £760,000 per annum. NHS Tayside contributes approximately £350,000 per annum towards this.

Scope and Objectives

To carry out a high level review of the arrangements in place for the provision of community equipment against each of the 10 themes contained in the Community Equipment Services Self Evaluation Toolkit, assessing the current status of implementing the requirements of the national Guidance and identifying areas for improvement.

Conclusion

The principal conclusion drawn from this review is that there are weaknesses in the system which should be addressed.

The main areas highlighted in the report are as follows:

- The areas for improvement identified during this exercise should form the basis of an improvement plan for implementation within a reasonable timeframe. Measures that require to be taken include developing the service model to become more outcomes focussed, revising and finalising the Dundee Joint Equipment Store Draft Operational Agreement and developing joint protocols.

Management Response to the Audit Report

The audit findings and recommendations were formally reported to the Director of Social Work and appropriate action agreed to address the matters raised.

ii) INTERNAL AUDIT REPORT 2011/33

Client	Corporate
Subject	Encryption of Laptops

Introduction

A review of the encryption of laptops was part of the planned internal audit work.

Where data is stored on laptops in an unprotected state, it potentially increases the risk of a data breach should the hardware be stolen, lost or accessed by an unauthorised individual. This in turn increases the risk of an organisation's reputation being damaged. In addition, the Data Protection Act 1998 states "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data". Encryption is a software tool that uses algorithms to scramble data and make it indecipherable to anyone other than an authorised user with a password. The main purpose of the software is encryption and decryption of data, usually in the form of files on, or sectors of, hard drives.

To protect access to data, enhance data security and mitigate the associated risks, an exercise to encrypt all laptops that were deemed to be part of the Council's corporate network commenced in June 2012. The encryption software solution utilised by the Council is Symantec Endpoint Encryption Full Disk Edition. There are of the order of 650 software licences in use for this product.

Scope and Objectives

To examine the systems operated in respect of the encryption of laptops deemed to be part of the Council's corporate network. For the purposes of this review, the term laptop also encompasses other portable technology such as tablets.

Conclusion

The principal conclusion drawn from this review is that there are weaknesses in the system which should be addressed.

The main areas highlighted in the report are as follows:

- To reduce the potential risk of damage to reputation and the possibility of monetary penalties following the theft or accidental loss of a Council laptop containing sensitive or confidential information, the Council should compile a formal mobile device policy that contains details regarding the appropriate use and security of laptops. The policy should refer, where appropriate, to existing IT policies and guidance and be communicated to staff.
- Whilst it is acknowledged that at the time of the audit fieldwork the laptop encryption roll-out was in the midst of the implementation phase, going forward in order to ensure that the Council's Active Directory and Laptop Inventories are complete and all laptops are encrypted as intended, an exercise to ensure details of all Council laptops have been captured should be carried out by the IT Division in conjunction with departments as appropriate.

Management Response to the Audit Report

The audit findings and recommendations were formally reported to the Director of Corporate Services and appropriate action agreed to address the matters raised.

iii) INTERNAL AUDIT REPORT 2012/22

Client	Corporate
Subject	Follow-up Review of Telecommunications – Mobile Phones

Introduction

As part of the planned internal audit work, a follow-up review of Internal Audit Report 2010/05, Telecommunications, Mobile Phones, was undertaken.

The original internal audit report concluded that there were weaknesses in the system which should be addressed. The main areas highlighted in the original report were as follows:

- To ensure compliance with Council policy, departments should be reminded that, prior to the issue of any mobile phone, an assessment form must be completed. In addition, although current policy requires staff to pay for personal calls given the resources required to assist staff identify personal calls, consideration should be given to discontinuing the use of mobile phones for personal use except in an emergency.
- To ensure that the Council has a complete and accurate database, Telephone Services staff should formally request a list of all mobile phones and the associated data from departments and update the corporate database to reflect the data provided. Thereafter, the relevant details such as the user's name must be recorded for all phones issued.
- To improve controls over mobile phones, T-Mobile should be requested to improve the functionality of the online system and the feasibility of utilising and/or customising the online option should be explored. In addition, international use, roamed calls and calls to premium rate lines should only be made available to staff where there is a clear business need.

Scope and Objectives

To assess whether or not each of the recommendations agreed by management in Internal Audit Report 2010/05 had been implemented within the given timescales. The follow-up review was restricted to areas included in the original report.

Conclusion

The principal conclusion drawn from the follow-up work undertaken is that whilst some action has been taken to strengthen the control weaknesses highlighted in the original review there are still some recommendations which require to be implemented by management.

The main areas where actions agreed by management are still outstanding are as follows:

- At the time of the audit fieldwork the contract for the Council's future mobile communications provider was being tendered. It is intended that once the new tender is in place an assessment will be made of the current policy in conjunction with human resources, amendments made as appropriate and changes communicated to staff.

Management Response to the Audit Report

The audit findings and recommendations were formally reported to the Director of Corporate Services and appropriate action agreed to address the matters raised.

iv) INTERNAL AUDIT REPORT 2012/24

Client	Corporate Services
Subject	Patch Management (Education Network)

Introduction

A review of patch management within the Education network was part of the planned internal audit work.

A patch is broadly defined as a small piece of software that is used to correct a problem within a software program or an operating system. Patches can also be referred to as fixes. Most major software companies will periodically release patches, usually downloadable from the internet, that correct very specific problems in their software programs. Microsoft, for example, typically release their security related patches on 'Patch Tuesday' which is the second Tuesday of each month.

The key aim of having a patch management programme in place is to create a consistently configured environment that is secure against known vulnerabilities in the operating system and application software. Such a programme also assists in maintaining operational efficiency and stability. Patching is therefore an important element in information security management and is best considered as a preventative measure which is undertaken to reduce potential risks in this area.

This review focussed specifically on the Education network within the Council's information technology infrastructure which consists of around 150 servers and of the order of 5,000 desktop PCs. Currently there are approximately 21,000 users of this network.

Scope and Objectives

To review the methodology applied to patch management within the Council's Education network and provide assurance that the risk of potential threats is dealt with appropriately.

Conclusion

The principal conclusion drawn from this review is that whilst there is basically a sound system of control there are some areas where it is viewed improvements can be made.

The main areas commented upon in the report are as follows:

- In order to further improve the effectiveness of the approach to patch management across the Education network, staff within the IT Division should ensure that the process is formally documented to reflect current working practices as soon as practicable. In addition, in respect of the decision making process as to which patches should be tested prior to deployment, this should be formalised utilising a risk based approach.

Management Response to the Audit Report

The audit findings and recommendations were formally reported to the Director of Corporate Services and appropriate action agreed to address the matters raised.

v) INTERNAL AUDIT REPORT 2012/25

Client	Corporate
Subject	Information Security Management Systems

Introduction

A review to assess the Council's framework in terms of Information Security Management Systems (ISMS) was part of the planned internal audit work.

Delivering good governance in local government has gained increasing prominence over the last few years and it is essential that governance arrangements should not only be sound but be seen to be sound. During this period there has also been an exponential growth in the dependence upon information technology which now underpins and supports almost every aspect of the Council's activities. As a result IT governance is recognised as a specific area within the governance agenda. A fundamental aspect of IT governance is the protection of information, which is now considered a business critical asset, particularly in respect of its availability, confidentiality and integrity.

The globally recognised standard for information security is ISO 27001. This standard has been prepared to provide a model framework for ISMS and is based on a process approach. The approach covers such areas as establishing, implementing, operating, monitoring, reviewing, maintaining and improving and it adopts a 'Plan-Do-Check-Act' framework for all ISMS processes. The standard does however recognise the principles of proportionality and risk in terms of the implementation of ISMS and that in practice it should be scaled according to the complexity and needs of the organisation.

The Council's approach to ISMS is based upon the international standard and the principles of ensuring availability, confidentiality and integrity of the Council's information assets underpins local policies and procedures. Whilst the lead officer for ISMS for the Council is based within the IT Division of the Corporate Services Department it is widely-recognised that in order for information security to be effectively embedded across the organisation it needs to be part of the everyday thinking of all staff.

Scope and Objectives

To evaluate compliance with information security good practice standards to ensure that there is a systematic approach to managing information securely.

Conclusion

The principal conclusion drawn from this review is that there are weaknesses in the system which should be addressed.

The main areas highlighted in the report are as follows:

- To improve the robustness of the Council's approach to ISMS, the governance arrangements should be reviewed to define and communicate roles and responsibilities. Thereafter steps should be taken to ensure that a comprehensive risk assessment of the Council's information assets is undertaken to determine which of these should be included within the scope and incorporated into the ISMS documentation.
- Going forward and in line with recognised good practice, ISMS documents should be reviewed annually and incorporate an appropriate version control process, the framework to capture and record corrective action in respect of ISMS reviews, audits and reported security incidents should be reassessed and an appropriate security training and awareness programme for relevant staff should be implemented.

Management Response to the Audit Report

The audit findings and recommendations were formally reported to the Director of Corporate Services and appropriate action agreed to address the matters raised.

vi) INTERNAL AUDIT REPORT 2012/35

Client	Corporate
Subject	Corporate Complaints

Introduction

A review of the complaints handling procedure was part of the 2012/13 internal audit plan.

In June 2012 a report was submitted to the Council's Policy and Resources Committee on the implementation of the Model Complaints Handling Procedure for Local Authorities. The report advised Committee about the development of guidance by the Scottish Public Services Ombudsman on a model complaints handling procedure which would provide a standardised approach for dealing with customer complaints within local authorities and their services across Scotland, with the exception of Social Work. It was agreed that the Council would adopt the model procedure with effect from September 2012 and update its procedures accordingly.

One of the key changes implemented by the Council was to move from a three stage to a two stage approach involving frontline resolution and investigation, in line with the model procedures. These two stages have targets for the resolution of complaints of 5 and 20 days respectively. In addition, the model procedures also included an increased emphasis on ensuring rigour around the recording of complaints resolved at the frontline stage, more frequent monitoring of complaints statistics and more systematic recording of lessons learned from complaints.

From 2013/14 local authorities will be required to assess complaints handling performance around a range of high level performance indicators. These performance indicators have been developed by the Scottish Public Services Ombudsman in consultation with local authority stakeholders and Audit Scotland. Local authorities will be required to report these complaints statistics at least quarterly.

Scope and Objectives

Review to assess compliance with the implementation of the revised Complaints Handling Procedures within the Council.

Conclusion

The principal conclusion drawn from this review is that whilst there is basically a sound system of control there are some areas where it is viewed improvements can be made.

The main areas commented upon in the report are as follows:

- To further improve the current complaints handling framework steps should be taken to incorporate the link to the Council's complaints handling procedures on the front page of the website, ensure that completion of the planned service improvements field within the database is made mandatory and standardised templates for responding to complaints are compiled and for these to be included within the staff guidance. In addition, to ensure that complaints are addressed within the target timescales and the Complaints Handling Procedures are followed, independent periodic checks of a sample of completed complaints should be performed.

Management Response to the Audit Report

The audit findings and recommendations were formally reported to the Chief Executive and appropriate action agreed to address the matters raised.

vii) INTERNAL AUDIT REPORT 2012/40

Client	Corporate
Subject	Tayside Procurement Consortium

Introduction

A review of the governance arrangements of Tayside Procurement Consortium (TPC) was part of the planned internal audit work.

TPC is a shared procurement service created by Dundee City, Angus, and Perth & Kinross councils in association with Tayside Contracts. Its function is to act as the strategic lead for its members as well as a central purchasing body for regionally procured commodities. TPC was formally launched in September 2007. The governance arrangements for the shared service are set out in a Memorandum of Understanding.

In April 2008, the Council's Policy and Resources Committee approved the development of TPC, adoption of the first Tayside Procurement Strategy, proposed corporate governance framework, delegated authorities and Memorandum of Understanding.

Within the Memorandum of Understanding, it stated that the Head of Procurement post would be reviewed in October 2013 along with the whole shared service organisation, including staffing structure and operating model. This review was undertaken early and resulted in the permanent establishment of the TPC structure being approved in March 2012.

The TPC central procurement team is located in Dundee City Council. There are also area procurement teams in each of the constituent councils and Tayside Contracts.

Scope and Objectives

To carry out a review of TPC's governance arrangements. Whilst the fieldwork for this review was undertaken by Angus Council's Internal Audit Service, the content of their report was reviewed and considered in context of the Council's relationship with TPC and its local arrangements.

Conclusion

The principal conclusion drawn from this review is that whilst there is basically a sound system of control there are some areas where it is viewed improvements can be made.

The main areas commented upon in the report are as follows:

- The Council should ensure, going forward, that the Procurement Programme Annual Report is formally presented to the Policy and Resources Committee. In addition, the Memorandum of Understanding should be updated to reflect the permanent establishment of the TPC structure and recent changes in council structures.

Management Response to the Audit Report

The audit findings and recommendations were formally reported to the Director of Corporate Services and appropriate action agreed to address the matters raised.

viii) INTERNAL AUDIT REPORT 2013/01

Client	Corporate Services
Subject	Payment of Pensions for Former Employees of ex List D Schools

Introduction

Pension payments to former employees of ex List D schools can have funded and unfunded elements. Funded pension is the amount to which the employee is entitled by virtue of his/her contributions to the pension fund. This element depends on length of service and final salary and the cost is borne by Tayside Superannuation Fund. Unfunded pension relates to pension increases and any enhancements which have been provided to staff when the employee retires before 65 e.g. in the case of redundancy. These costs are recoverable from the Scottish Government and Pensions Administration staff invoice the Scottish Government on a regular basis. It is a requirement of the payment for unfunded pensions that the claims are audited annually by the Internal Audit Service at the end of each financial year.

Scope and Objectives

To provide assurance to the Chief Internal Auditor for completion of the annual auditor's report that the information provided by the Pensions Section in support of the claim for payment of pensions for former employees of ex List D Schools is correct and in accordance with the relevant legislation.

Conclusion

On the basis of examining the accounts and records of this grant claim, obtaining such explanations and carrying out such tests as deemed necessary, it is considered that the entries in the claim form are fairly stated, and that the sums claimed are properly due and have been used in accordance with the terms and conditions of the Offer of Grant.