Information Security Checks (September) 2016/17

City of York Council

Internal Audit Report

Service Area: Corporate and Cross-Cutting
Responsible Officer: Assistant Director, Legal, Civic and Democratic
Service Manager: Information Governance and Feedback Team Manager
Date Issued: 8th December 2016
Reference: 10260/017

	P1	P2	P3
Actions	**0**	**3**	**0**
Overall Audit Opinion	**Reasonable Assurance**		

Summary and Overall Conclusions

Introduction and objectives

1.1 In accordance with the agreed audit plan, information security checks will be undertaken during 2016/17. The purpose of these checks is to assess the extent to which confidential, personal or sensitive data is stored securely and to ensure that data security is being given sufficient priority within council departments. This was the first of these checks in this audit year.

Scope of the Audit

1.2 As part of this audit the two main council offices, West Offices and Hazel Court, were visited. This was the eighth of these information security checks since the opening of West Offices in 2013 and the council-wide implementation of a clear desk policy. The increasing number of non council staff who share West Offices makes it more important for each service to recognise the importance to secure the information they hold within their area of the building. The previous information security checks were conducted in October 2015 and an opinion of Reasonable Assurance was given.

1.3 The buildings were visited after most staff had left for the day. This enabled auditors to assess the extent to which data is being left out overnight without appropriate security. Instances of information being left unsecured were recorded where these posed risks to the council, either because they contain personal or confidential information. Instances of general security weaknesses, including assets and controlled stationery were also recorded.

1.4 The findings are summarised below and detailed findings are set out in the attached Annex 3.

Findings

2.1 Overall, improvements in information security that were seen in the checks done in October 2015 had not been maintained. Whilst information held in West Offices was generally stored away in closed cupboards, the majority of these cupboards were not locked. Many of these cupboards contained basic personal information and some contained sensitive personal information that should not be left unsecured at the end of the day.

2.2 The general areas where information was not kept secure and improvements should be made include:

- In West Offices some cupboards containing sensitive, personal or confidential information were unsecured and some documents were not stored in cupboards (i.e. on top of cupboards, on desks, in boxes under or around desks).

- At Hazel Court, some cupboards containing personal and sensitive information were left unlocked and some sensitive information was left on desks or on open storage (i.e. shelving).

- Across both sites, some council assets were left unsecured, including laptops, cameras and keys to properties and vehicles.

2.3 xxxxxxxxxxxxxxxxxxxxxxx:

- Xxxxxxxxxxxxxxxxxxxxxx

- Xxxxxxxxxxxxxxxxxxxxxx

- xxxxxxxxxxxxxxxxxxxxxx

2.4 All individual items of information found during these checks have been rated according to the level of risk they pose if this information was accessed inappropriately, disclosed or lost. All items recorded pose some risk and action should be taken. Specific attention should be paid to those rated as medium and high risk in the attached detailed findings, Annex 3.

2.5 xxxxxxxxxxxxxxxxx:

- xxxxxxxxxxxxxxxxxxxxxx.

- xxxxxxxxxxxxxxxxxxxxxx.

- xxxxxxxxxxxxxxxxxxxxxx.

- xxxxxxxxxxxxxxxxxxxxxx.

Overall Conclusions

3.1 The council remains reasonably well protected against accidental disclosure of information. The vast majority of information is stored in cupboards and cupboard doors are closed. The clear desk policy is largely adhered to throughout West Offices and increasingly by most teams at Hazel Court as well. Access to West Offices and Hazel Court buildings is controlled, though at West Offices there is a risk of unauthorised access by people who legitimately have access to the building. An audit of office security is currently in progress and any implications for information security arising from that work will be factored into future assessments of risks.

3.2 There remain improvements to be made to protect against deliberate unauthorised access by ensuring all personal and sensitive information is locked away across all areas of the council. Action is also required to ensure that confidential information (e.g. financial data) is kept securely. In some cases, a lack of improvement following previous checks suggests that sufficient priority is not being given to the security of information. It was disappointing to note that significant improvements that were seen in the previous audit checks had not been maintained this time.

3.3 Overall, there is currently satisfactory management of risk but a number of weaknesses were identified. An acceptable control environment is in operation but there are a number of improvements that should be made. Our opinion of the controls within the system at the time of the audit was that they provided **Reasonable Assurance**.

3.4 There are further information security checks planned for 2016-17. The findings from this audit suggest that a further round of out of hours checks at the main offices may be worthwhile to confirm whether there is any improvement as a result of actions taken following this audit.

3.5 From patterns observed through these checks over the last four years and some anecdotal evidence from the response to these reports and conversations with officers around information security there seems to be two main barriers to improvement in information security:

- The first is the practicalities over key management, so that it can be ensured all cupboards containing personal or confidential data can always be locked at the end of the day and keys are accessible to everyone in the team to open the cupboards the following day. It is planned to put a key management process in place for the whole of West Offices; this should be done as a priority and audit checks could be undertaken following this to check that all teams are utilising the new system.
- The second issue seems to still be a lack of recognition of the importance of securing data within the office and within each team area. In some areas it seems that reliance is being placed on perimeter security for the buildings and on trust that people with access to the building but not in that team would not inappropriately access information. It does not seem to be recognised that external partners in West Offices increase the information security risks or that personal information held by service areas should not be able to be accessed by council staff in other service areas.

Actions

4.1 This report was discussed with the Information Governance and Feedback Team Manager and presented to the Governance, Risk and Assurance Group (GRAG) in November 2016. The actions below were agreed by GRAG.

Agreed Action 1

A system for secure key storage will be implemented in West Offices to ensure teams can only access their own keys. All teams will be expected to lock their cupboards at the end of the day and put their keys into this secure storage.

Priority	2
Responsible Officer	Information Governance & Feedback Team Manager
Timescale	March 2017

Agreed Action 2

The detailed findings will be fed back to individual service areas and where information found was of a personal and sensitive nature (i.e. priority 1 and 2 findings in the spreadsheet attached at Annex 3). For priority 1 findings officers will be asked to respond with details of what action will be taken to address the issue and these will be followed up by internal audit.

Priority	2
Responsible Officer	Veritau Audit Manager
Timescale	November 2016

Agreed Action 3

Further information security checks will be conducted by internal audit in the 2016-17 financial year to check whether improvements have been made.

Priority	2
Responsible Officer	Veritau Audit Manager
Timescale	March 2017

Audit Opinions and Priorities for Actions

Audit Opinions	
Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit. Our overall audit opinion is based on 5 grades of opinion, as set out below.	
Opinion	**Assessment of internal control**
High Assurance	Overall, very good management of risk. An effective control environment appears to be in operation.
Substantial Assurance	Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified.
Reasonable Assurance	Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made.
Limited Assurance	Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation.
No Assurance	Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse.

Priorities for Actions	
Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.

Annex 3

Detailed Findings

Information Security checks Sep16 - conso