Information Security Checks (March) 2016/17

City of York Council

Internal Audit Report

Service Area: Corporate and Cross-Cutting
Responsible Officer: Assistant Director, Legal and Governance
Service Manager: Information Governance and Feedback Team Manager
Version: Final
Date Issued: 1 June 2017
Reference: 10260/022

	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 were 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 second of these checks in this audit year (the first being in September 2016).

1.2 The previous information security checks were conducted in September and gave an overall opinion of Reasonable Assurance. However, it was also observed that past improvements in information security had not been maintained, with large numbers of cupboards being left unsecured and sensitive, personal and confidential information was insufficiently protected. As a result, it was agreed that this second round of checks would be completed in the 2016-17 audit year.

Scope of the Audit

1.3 As part of this audit the two main council offices, West Offices and Hazel Court, were visited. This was the ninth 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.

1.4 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.

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

1.6 A visit to Yorkcraft also took place in April 2017 as agreed as part of the response to the ICO audit that took place in 2015. This assessed the arrangements for secure storage of archived information at Yorkcraft and arrangements for destruction of confidential information.

Findings

2.1 Overall, the degree to which information was being held securely had improved since the September 2016 checks. The majority of cupboards were locked and most of those that were unlocked did not contain sensitive personal information. These improvements were pleasing to note but there still remained some areas where cupboards had not been adequately secured, some sensitive information was not adequately protected and both information and physical asset were vulnerable to theft.

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. There was only a small number of documents that 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, a significant number of council assets were left unsecured, including laptops, cameras and keys to properties and vehicles.

Whilst the Hazel Court site and building security provides protection against external breaches of information, reliance should not be placed solely on the perimeter security and sensitive information must also be protected from internal breaches.

- xxxxxxxxxx

- xxxxxxxxxx

2.5 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.

2.6 Testing undertaken at Yorkcraft found that there were good systems and processes in place for the secure storage of archived information and the secure destruction of confidential information. No issues requiring action have been raised in relation to the Yorkcraft visit; detailed feedback has been provided to the information governance and feedback team manager and Yorkcraft manager.

Overall Conclusions

3.1 The council remains reasonably well protected against accidental disclosure of information. The vast majority of information is stored in cupboards, cupboard doors are closed and in these checks, the majority of cupboards were locked. The clear desk policy is largely adhered to throughout West Offices but less so at Hazel Court. 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.

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. It was pleasing to note that there was an overall improvement in these checks, from the previous ones done in September 2016.

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 Further information security checks will be undertaken in 2017-18 and these will take place following implementation of new key storage arrangements, which should improve the compliance with the requirement to lock all cupboards. However, this also needs to be supported by a culture that recognises the importance of securing data within the office and within each team area and not to rely solely on perimeter security and recognises all information held by the council as an asset that needs to be protected.

Actions

4.1 Actions to address the weaknesses identified in this report were agreed by the Governance, Risk and Assurance Group (GRAG) in May 2017 and are detailed at Annex 1.

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	September 2017

Agreed Action 2

The detailed findings will be fed back to individual service areas 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.

Audit will provide updates to GRAG on responses received from service areas.

Priority	2
Responsible Officer	Veritau Audit Manager / GRAG
Timescale	June 2017

Agreed Action 3

Further information security checks will be conducted by internal audit in the 2017-18 financial year and following the implementation of the new key storage arrangements.

Priority	2
Responsible Officer	Veritau Audit Manager
Timescale	September 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.

Detailed Findings

Information Security checks Mar17 - conso