Veritau
Assurance Services for the Public Sector

Information Security Checks 2015/16

City of York Council

Internal Audit Report

Service Area: Corporate and Cross-Cutting
Responsible Officer: Director – CBSS
Service Manager: Transparency and Feedback Team Manager
Date Issued: 01 February 2016
Reference: 10260/015

	P1	P2	P3
Actions	0	4	0
Overall Audit Opinion	Reasonable Assurance		

Summary and Overall Conclusions

Introduction and objectives

1.0 In accordance with the agreed audit plan, regular information security checks will be undertaken at council offices during 2015/16. The purpose of these visits 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 visits this year.

Scope of the Audit

1.1 Both West Offices and Hazel Court were visited as part of this audit. This was the seventh information security visit since the opening of West Offices and the council-wide implementation of a clear desk policy.

1.2 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.

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

Findings

2.0 Across both sites, the improvements identified in the previous checks had been maintained, xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx

2.1 A small number of serious breaches of information security were found and these areas are identified in Annex 2 as 'significant items'. Consolidated findings will be sent to the Transparency and Feedback manager to agree specific action with managers of the services where significant weaknesses were identified.

2.2 There remain a small number of general areas where improvements could be made, and regular reminders should be given to staff to ensure the generally good levels of information security observed in these checks is maintained.

- xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx

- xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx

- xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx

2.3 xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx

- xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx

- xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx

2.4 xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx

Overall Conclusions

3.0 Overall, the council remains well protected against accidental disclosure of information xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx

3.1 xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx

3.2 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**.

Actions

4.1 The consolidated findings were discussed with the Transparency and Feedback manager and the actions at Annex 1 were agreed to address weaknesses identified. The report and action plan will be presented to the Information Management Board in November 2015.

Annex 1

Agreed Action 1.1

xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx

Priority	xxxxxxxxxxxxxxxxxxxxxx
Responsible Officer	xxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxx
Timescale	xxxxxxxxxxxxxxxxxxxxxx

Agreed Action 2.1

The findings from this report will be presented to the Information Management Board.

Priority	2
Responsible Officer	Transparency and Feedback Team Manager
Timescale	Action completed (Nov15)

Agreed Action 2.2

Information Guardians will cascade reminders to their directorates and relevant service managers to ensure weaknesses identified are addressed.

Priority	2
Responsible Officer	Information Guardians
Timescale	28 February 2016

Agreed Action 3.1

A programme of information security checks will be agreed with internal audit to ensure coverage of a wider range of information security risks and to address some of the issues raised in the recent ICO audit report

Priority	2
Responsible Officer	Transparency and Feedback Team Manager
Timescale	Action completed

Annex 2

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

Oct15 Info Sec
Checks - Consolidate