

Information Security Checks 2014/15 City of York Council Internal Audit Report

Service Area: Corporate and Cross-Cutting

Responsible Officer: Director – Customer and Business Support Services

Date Issued: 10 March 2015

Reference: 10260/011

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 2014/15. 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. The second of this year's visits has recently been completed.

Scope of the Audit

- 1.1 Both West Offices and Hazel Court were visited as part of this audit. This was the fifth 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, categorised according to the reasons for the breach and the action needed to address these weaknesses.
- 1.4 Detailed findings are set out in the attached annex 2.

Findings

- 2.0 Further progress seems to have been made since the checks undertaken in September 2014. Some areas showed significant improvement following actions taken in response to the findings last time. Many areas have also maintained their previously good levels of information security.
- 2.1 However, there do remain some areas where further improvement can be made:

Overall Conclusions

3.1

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

- 4.0 Directorate Information Governance Champions should ensure that the detailed findings in Annex 2 are cascaded to their directorates, along with reminders about maintaining appropriate information security, including:
- 4.1 Internal audit have confirmed actions to be taken in relation to those areas where the risks are greatest;

Audit Opinions

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.

Detailed Findings



Info Sec Findings -Annex 2 for report.xl