

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: 22 May 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 third 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 sixth 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 While previous checks have shown only gradual progress in improving information security across the council's main offices, these checks revealed a significant improvement from the last visit. Across both sites, more cupboards were locked, and some areas that were previously weak had successfully addressed these weaknesses. In particular, there was a significant improvement at Hazel Court in adherence to the clear desk policy and in securing sensitive information. Many areas have also maintained the good levels of information security observed previously.
- 2.1 There remain a small number of 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.
- 2.2 A small number of serious breaches of information security were found and these areas are identified in Annex 2 as 'significant items'. Individual feedback will be sent to service managers and specific action will be discussed and agreed with service managers to address these issues.
- 2.3 Items listed under 'general feedback' in Annex 2 relate to less serious breaches of information security. These should be addressed by reminders about taking appropriate measures to keep personal, confidential or sensitive information secure. Directorate

representatives of Corporate Information Governance Group (CIGG) should take this forward within their directorate.

Overall Conclusions

- 3.0 Overall, the council is well protected against accidental disclosure of information. The vast majority of information is stored in cupboards and most cupboard doors are closed. The clear desk policy is largely adhered to throughout West Offices and this now appears to be the case for most teams at Hazel Court. In addition, the reception building (and therefore, the site as whole) was more secure, though there were still some improvements that could be made.
- 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 This report will be presented to the Corporate Information Governance Group (CIGG) in order to agree actions to be taken at a corporate and directorate level to address the issues identified.
- 4.2 Internal audit will also agreed specific actions with service managers in relation to those areas where the risks are greatest; either because of the nature of the documents left unsecured or because the weaknesses in information security are a recurring issue (those items listed as 'significant items' in Annex 2).
- 4.3 A series of information security checks will be conducted in 2015-16. Discussions will be held with the Transparency and Feedback manager to agree how these will be conducted, with a view to varying the locations visited and method, scope and objectives of the checks.

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



March Sweep findings - consolidate