Encryption and User Access

City of York Council

Internal Audit Report 2013/14

Business Unit: Customer & Business Support Services,
Responsible Officer: Assistant Director, Governance and ICT
Service Manager: Head of ICT
Date Issued: 3rd March 2015
Status: Final
Reference: 10245/003.bf

	P3	P2	P1
Findings	1	1	0
Overall Audit Opinion	Substantial Assurance		

Summary and Overall Conclusions

Introduction

ICT plays a key role in the efficient delivery of services to the public, and is also vital to the effective internal operation of the council. New technologies bring clear benefits, but also bring with them new obligations and areas of risk exposure.

For example, organisations must ensure that electronic information is held securely, and this falls within the scope of the Data Protection Act 1998. Compliance with the principles in the Act is monitored by the Information Commissioner's Office, which since 2010 has regularly imposed fines on organisations for failure to comply.

Ensuring that access to data is restricted to only authorised persons is therefore of vital importance to organisations. In the event of an information security breach, they must be able to demonstrate that as far as possible they had put appropriate technological security measures in place to manage risks.

Objectives and Scope of the Audit

The purpose of the audit was to provide assurance to management that the controls which it has put in place to manage key risks relating to network access and the security of data held on portable devices are effective.

The audit covered the following key risks:

- that data held on council-owned portable devices is not effectively encrypted; and
- that user access is not controlled effectively, leading to information security breaches and fines or other penalties by the Information Commissioner's Office.

Key Findings

Effective processes to grant new users access to the Council network were found to be in place. The Council has defined which devices should be encrypted, and uses suitable proprietary encryption methods to secure its data on its equipment.

However, users are currently able to save data from a citrix session to their own machines. The council has no control over the security of these machines, or over how users may further process the data. Devices are unlikely to be encrypted, and the council cannot ensure that they are disposed of securely when no longer required.

Several laptops have been authorised to be exempt from encryption, despite the business cases not complying with the conditions for exemption.

Overall Conclusions

It was found that the arrangements for managing risk were good with few weaknesses identified. An effective control environment is in operation but there is scope for improvement in the areas identified. Our overall opinion of the controls within the system at the time of the audit was that they provided **Substantial Assurance**.

Area Reviewed: Laptop security

1 Issue/ Control Weakness	Risk
Several laptops have been authorised to be exempt from encryption, despite the business cases not complying with conditions for exemption.	Unauthorised access to personal data on unencrypted machines, leading to reputational damage and fines or other sanctions from the ICO.

Findings

The auditor was advised that there are approximately 30 laptops which have been exempted from encryption following the submission of a business case by managers.

The business case forms state that "I understand that should this exemption be granted that the device / devices will not be permitted to connect to the City of York Council network" and "I agree that no personal information about an individual of any kind will be stored on the laptop. I understand that a failure to comply with these policies may result in substantial reputational damage to the Council and/or fines of up to £500,000".

Three business cases were provided to the auditor to review. One of these states that the laptop will be used for making copies of evidence and another states that the laptop will be used to connect to the network via entrust. Both of these therefore contradict the terms of the exemption.

1.1 Agreed Action

We will review the wording on the forms, and cases for unencrypted laptops will be reviewed every 12 months. We are also currently reviewing the encryption method and it is likely that we will move to Bitlocker.

Priority	2
Responsible Officer	ICT Support Manager
Timescale	30 April 2015

Area Reviewed: Local drive mapping in Citrix

2	Issue/ Control Weakness	Risk
	Data can be saved to a local drive from a Citrix session, including to devices not owned or controlled by the council.	Unauthorised persons gain access to personal data, leading to reputational damage and fines or other sanctions from the ICO.

Findings

While measures are in place to prevent data being saved to unencrypted media, users can save council data from a Citrix session onto their own devices' local drives when working from home. The Information Systems Security and Acceptable Use Policy prohibits this, but there is no technical solution in place to prevent it. There does not appear to have been a review undertaken to confirm whether there is a continuing business need for this function which outweighs the associated risks.

2.1 Agreed Action

We will continue to work to implement measures for secure internal-external file sharing. We will also review the necessity of users being allowed to save data to local drives.	Priority	3
	Responsible Officer	ICT Support Manager
	Timescale	30 April 2015

Annex 1

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.