Information Security

City of York Council

Internal Audit Report 2014/15

Business Unit: Corporate, Corporate Information Governance Group
Responsible Officer: Director of CBSS (SIRO)
Service Manager: Transparency and Feedback Manager
Date Issued: 13 August 2015
Status: Final
Reference: 10260/010

	P1	P2	P3
Actions	**0**	**3**	**3**
Overall Audit Opinion	Reasonable Assurance		

Summary and Overall Conclusions

Introduction

Information is one of the most valuable assets held by any organisation. A failure to maintain personal and sensitive data securely and to manage it effectively can lead to breaches under the Data Protection Act (DPA) with potential fines of up to £500,000 from the Information Commissioner's Office (ICO).

To help effectively manage information the council has put structures in place, including a Corporate Information Governance Group (CIGG), Directorate Information Governance Champions (DIGC) and a Senior Information Risk Owner (SIRO). The council has also developed a number of policies, strategies and supporting arrangements.

During the time of this audit and up to the end of 2014-15, the council contracted Veritau to provide information governance support. From the 1st April 2015 a new role of Transparency and Feedback Team Manager has been created to provide strategic leadership in the development and delivery of the council's information governance arrangements. Services are in the process of being transferred, with the aim of completing this by September 2015. An update on recent and ongoing work on information governance was reported to the Audit and Governance Committee in June 2015.

In 2011 the council suffered a serious breach in information security, with highly sensitive child protection information being sent to the wrong individual. This resulted in the council signing an undertaking with the ICO to ensure steps were taken to prevent such breaches in future. CIGG developed an action plan to address these weaknesses. This included actions around secure printing and email, incident management processes and physical security measures across council sites, among others. Subsequent internal audit work has followed up on these issues and found that whilst systems had improved, there remained some weaknesses and inconsistencies across the organisation. Therefore, a full information security audit was included in the 2014-15 audit plan.

Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that procedures and controls within the system will ensure that:

- governance arrangements for information security are in place and are appropriate;
- data sharing arrangements are in place and data is shared using appropriate physical or technical measures;
- arrangements are in place to manage risks associated with mobile working;
- information is held with appropriate security measures throughout its lifetime;
- appropriate procedures are in place to identify, manage and respond to information security incidents.

This audit focussed on the governance, procedural and human elements of information security, rather than those specifically or solely associated with the use of IT systems. The audit included visits to a variety of sites other than the two main council offices, including sites such as children's centres, elderly people's homes and those shared with other agencies.

Information security spot checks have also been conducted at West Offices and Hazel Court throughout the year and the results of these have been separately reported.

Key Findings

Overall, there seemed to be an understanding throughout the council of the importance of information security, with staff and managers across all areas reviewed focussed particularly on maintaining customer confidentiality. There was good awareness of the risks of mobile working and the changes to ways of working with the move to West Offices was acknowledged to have reduced the risk by minimising the amount of information taken off council premises (electronically or in hard copy). There was generally good physical security to protect information across the council's external sites and confidential information is securely destroyed across the council.

There were some areas of weakness, including a lack of awareness of some of the corporate information governance measures. In particular, there was a lack of awareness of the information security incident management policy and procedure and a lack of understanding of the full range of events that constitute incidents and should be reported. This seems to be reflected in the incidents log, with some directorates reporting a much greater number of incidents (and it seems unlikely they would be subject to so many more incidents).

There was a lack of awareness of other aspects of information security governance, including the existence and role of Directorate Information Governance Champions (DIGCs), other sources of advice on information governance and the full range of information governance policies and where to find them.

Progress has been made on compiling an information asset register throughout the council but this does not yet adequately identify all personal information held, shared and whether the required privacy and data sharing agreements are in place.

Overall Conclusions

It was found that the arrangements for managing risk were satisfactory with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made. Our overall opinion of the controls within the system at the time of the audit was that they provided Reasonable Assurance.

1 Refresh of policies and raising awareness

Issue/Control Weakness	Risk
Lack of awareness of corporate policies relating to information security.	Employees will not be aware of their responsibilities and expectations of them in relation to information security, increasing the risks of information security breaches.

Findings

The council's information governance policies were compared to a minimum set of policies that the Local Government Association (LGA)'s data handling guidelines state should be in place. Overall, the council does have policies covering all the required areas but some of these policies are due to be reviewed and updated. In addition, the implementation of a new (and temporary) intranet site seems to have resulted in some policies no longer being available on the intranet.

The number of information security policies and the overlap between them means that it can be difficult to find the right policy or be sure which policy covers which issues. A map of the policies and how they all relate to each other has been produced and is included in the Information Governance strategy. This is very useful from a corporate governance perspective but is unlikely to be meaningful to the majority of staff.

Through discussion with officers throughout the council it was apparent that awareness of corporate information governance policies was limited. Some 'external sites' (i.e. not West Offices or Hazel Court) have their own policies in place and others follow procedures specific to the site. Similarly, many services take their lead from existing practices within their service area and the requirement of legislation and regulations governing their areas specifically, rather than from corporate policies.

iComply was acknowledged by many officers to be potentially useful in raising awareness of policies (and in having evidence available corporately that policies have been seen and read). However, there was also a feeling that this alone would not be effective in directing behaviour and may simply be treated like a 'tick box' exercise. Many officers felt that shortened and simplified documents containing key messages relevant to all officers would be more effective than simply requiring the existing policies to be read.

Agreed Action 1.1

a) Information governance policies will be reviewed and updated.
b) Awareness of information security policies and procedures will be raised through learning and development requirements and a variety of communication methods. Information governance is included as a specific subject area in the CYC compliance training framework, which will be rolled out during 2015-16.

Priority	2
Responsible Officer	Transparency and Feedback Manager
Timescale	October 2015

Agreed Action 1.2

a) The iComply ‘introduction to information security’ was rolled out in May 2015 and will be included in the induction package for new starters.
b) The information governance section of the council induction package (‘Welcome to York’) will be reviewed and updated.
c) Further training on data protection, FOIs, SARs will be developed with the Workforce Development Unit. This will include a mixture of iComply material, eLearning and group sessions for managers.

Priority	2
Responsible Officer	Transparency and Feedback Manager
Timescale	October 2015

2 Role of CIGG, DIGCs and other support and guidance available on information governance

Issue/Control Weakness	Risk
Lack of awareness of information governance roles, where to seek advice and weaknesses in dissemination of information from CIGG.	Appropriate advice is not sought in the event of an information security incident or application of policies and procedures; potentially leading to an increased likelihood of information security being breached and/or in the event of a breach an increased impact of this breach. Relevant information is not disseminated from CIGG effectively.

Findings

A Senior Information Risk Owner (SIRO) has been appointed. This is the Director of CBSS. He chairs the Corporate Information Governance Group (CIGG); is the contact for referrals to the Information Commissioners Office (ICO); receives internal audit reports relating to information security; owns actions plan relating to information governance and commissions information governance work.

Directorate Information Governance Champions (DIGCs) have also been appointed (these are at Assistant Director level). They attend meetings of CIGG and are responsible for disseminating information relating to their directorate. During 2014 there was no consistency of attendance at CIGG meetings, with none of these meetings having representation from every council directorate and only a small number of attendees being at every one of these meetings. This has improved in the early months of 2015. All of the people spoken to at external sites and most of those within the main council offices were unaware of the existence of the role of DIGC or who the individual DIGCs were. There is no information available on the intranet relating to DIGCs.

Some people were aware of the existence of the Information Governance officer (Veritau) though this was usually through having dealt with an incident and been directed towards this team by someone else (or due to a recent exercise on compiling an information asset register).

All people spoken to indicated that their manager would be the first person they would speak to for information security advice. This seems appropriate and indicates that if the council can ensure service managers and team managers are aware of where they can seek advice and refer information security issues to this would go a long way to ensuring that in case of any incident the appropriate guidance and advice would be sought.

Agreed Action 2.1

The Terms of Reference (ToR) for CIGG will be reviewed and updated. This will include reviewing and agreeing the membership (including substitutes) and roles and	**Priority**	3
	Responsible Officer	Transparency and

responsibilities for monitoring and reporting on information governance matters. Following this, a communications plan will be developed to raise and maintain awareness through a variety of communication methods.	Feedback Manager
Timescale	October 2015

3 Awareness of Incident Management policy and procedure

Issue/Control Weakness	Risk
Lack of awareness of Incident Management policy and procedure.	Incidents are not identified, increasing the risk that appropriate action is not taken and also that corporate records and review of incidences are based on incomplete records.

Findings

Across, the council, there is little awareness of the council's Information Security Incident Management policy and procedure. Most officers across the council were not aware there was a policy and procedure and where it could be found.

Discussions with officers revealed incidents that should have been reported under the incident management policy had not been because staff were not aware of the requirement to report issues. Generally, this seemed to be instances of low-level incidents not being reported, which indicates that there is a lack of understanding about what constitutes an information security incident.

However, it should be noted that all officers did indicate that in the event of a serious incident (e.g. a breach with sensitive information or a breach where action could not easily be taken to recover the information) they would inform senior managers and ensure that action was taken to recover the initial situation and try to prevent it happening again in future.

Agreed Action 3.1

The incident management policy and procedure will be reviewed in line with ICO guidance. It will also specifically include the role of the Caldicott Guardian.

The launch of the new version will be included in the communications plan (action 3.1) and ongoing monitoring of information security incidents will be included in the CIGG ToR (action 2.1).

Priority	3
Responsible Officer	Transparency and Feedback Manager
Timescale	October 2015

4 Monitoring of compliance with Incident Reporting policy

Issue/Control Weakness	Risk
Lack of management information on compliance with the incident management policy.	Trends will not be identified, potentially resulting in weaknesses in incident reporting and leading to failure to respond adequately, thus increasing the chances of further incidents occurring and potential censure from the ICO.

Findings

Quarterly summaries of information security incidents are produced and reported to CIGG meetings.

These reports summarise each incident individually, including the cause (e.g. human error) and a brief description of every incident reported in the last quarter. This means that in order to identify trends in information security incidents a detailed review of each incident within the report is required. Other aspects of compliance with the information security incident policy and procedure (such as the timeliness with which incidents are reported and whether appropriate action has been taken in response to the incident) are not reported on.

It may be more useful and appropriate for CIGG to receive monitoring reports that analyse incidents and the reporting of them at a higher, more summarised level (e.g. information on the number of incidents reported by directorate, the speed of reporting and the proportion of incidents where it has been confirmed that appropriate action has been taken). This kind of management information would enable CIGG to receive assurance on compliance with the incident management policy and more easily identify where action was needed to address weaknesses or non-compliance.

Agreed Action 4.1

In addition to the actions previously identified (action 3.1), a system will be developed for oversight and monitoring of information security incidents, through CIGG, Council Management Team (CMT) and Directorate Management Teams (DMTs).

Priority	3
Responsible Officer	Transparency and Feedback Manager
Timescale	October 2015

5 Information Asset Register

Issue/Control Weakness	Risk
Lack of detailed and consistent assessment of risks.	Risks are not thoroughly assessed, leading to inadequate or inappropriate mitigation measures being put in place and increasing the chances of breaches of information security.

Findings

The Information Asset Register requires Information Asset Owners (IAOs) to assess the risks of the different types of information they hold.

Some IAOs have done this in detail relating to security risks, the impact on the service and in some cases the impact on reputation, time to re-collate or deal with loss or corruption. Some seemed to have only assessed the security risks relating to the information (and not any operational risk that would arise from the loss of the information).

However, many entries simply state the risk as Low, Medium or High, with no indication of any criteria used and no distinction between information that has a greater likelihood of loss or corruption and information that would have a greater impact from any loss. Without a proper assessment of the risks of different types of information held it is unlikely that efficient and effective measures will be put in place to manage the risks, increasing both the likelihood of information security breaches and their impact.

Agreed Action 5.1

The guidance and training provided to IAOs will be reviewed to identify training needs for IAOs and the Information Asset Register will be updated.
A risk register process will be produced for IAOs to follow in assessing the risks for the information assets they own.

Priority	2
Responsible Officer	Transparency and Feedback Manager
Timescale	October 2015

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.

Where information resulting from audit work is made public or is provided to a third party by the client or by Veritau then this must be done on the understanding that any third party will rely on the information at its own risk. Veritau will not owe a duty of care or assume any responsibility towards anyone other than the client in relation to the information supplied. Equally, no third party may assert any rights or bring any claims against Veritau in connection with the information. Where information is provided to a named third party, the third party will keep the information confidential.