ICT Governance and Cyber Security 2017-18

City of York Council

Internal Audit Report

Business Unit: Customer and Corporate Services
Responsible Officer: AD, Customer Services & Digital
Service Manager: Head of ICT
Date Issued: 25 June 2018
Status: Final
Reference: 10245/011

	P1	P2	P3
Actions	**0**	**1**	**2**
Overall Audit Opinion	Substantial Assurance		

Summary and Overall Conclusions

Introduction

The governance of ICT is a key contributor to strategic organisational success. Proper alignment between ICT and the organisation means:

1) senior organisation management understands the potential and limitations of ICT;
2) the ICT function understands the objectives and corresponding needs of the organisation; and
3) this understanding is applied and monitored throughout the organisation via an appropriate governance structure and accountability.

Understanding the value and the cost of ICT is important for members, senior management and ICT management. The effectiveness of the ICT governance structure and processes are directly dependent upon the level of involvement of the members and senior management, which will form the basis of this audit.

The Council's cyber resilience is key to the administration and provision of essential services, which now relies on the integrity of cyberspace and on the infrastructure, systems and data which underpin it. The National Cyber Security Strategy describes 'cyber security' as: "the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures."

UK local authorities have been subjected to at least 98 million cyber attacks between 2013 and 2017. During the month of November 2017, the Council blocked 1,009,475 potential cyber incidents.

With councils making more local public services available digitally, getting more of their workforce online and planning greater collaboration and integration work with partner organisations – which requires the sharing of residents' and business customers' data – reviewing and reinforcing current cyber security arrangements is a key priority for local authorities.

Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that:

- Organisational roles and groups are suitably allocated and support ICT's objectives.
- Cyber risk appetite has been formally documented, with clear risk ownership at the strategic level.
- An incident response plan has been developed and tested.
- An effective cyber risk training programme is in place.

This audit did not include an operational review of cyber security, but rather a strategic overview of how cyber risks are identified and recorded. The effectiveness of cyber security systems will be tested in line with ISO 27001 as part of the 2018/19 internal audit plan.

Key Findings

The Council has made positive steps to include ICT governance in the corporate governance structure, including the development of various groups dedicated to ICT issues. These groups include the ICT Board, the Digital Steering Group (DSG) and the Digital Services Steering Group (DSSG). The representation at these groups is varied and attended by a good mix of senior management (including the Chief Executive) and operational management (such as the Head of ICT). The governance structure aims to ensure alignment between ICT, CMT and DMT whilst allowing for sufficient oversight at an organisation-wide level.

The ICT Strategy has been developed and is broadly aligned to the Council Plan, with emphasis on the end-user experience (both internal and external) and aiming towards a high standard of IT-enabled service provision.

The Council has a Corporate Risk Register which contains risks related to information security. However, there are no risks that relate to security incidents or ICT systems failure. Currently, ICT is not formally represented at the Governance, Risk and Assurance Group (GRAG). However, the Assistant Director Customer Experience & Digital Services attends the group, providing an opportunity to ensure adequate ICT representation at GRAG. This is discussed in Finding 1.

The Council has a designated ICT Security Incident Team (ISIT). There is an up-to-date Security Incident Management Policy and corresponding procedure document. The Policy applies to Council staff and contains a significant amount of information on what an incident might look like and what responsibilities the end user has. The procedure document applies to ICT staff and contains more streamlined information (including a Basic Incident Response Process Flow Diagram and an Appendix with Roles and Responsibilities and numerous contact details). At the date of the audit, this procedure had not been formally tested. The Policy states that "The ICT Security Incident Coordinator(s) will test the ICT Security Incident management procedure on a regular basis." This is discussed in Finding 2.

Finally, the Council's cyber security training was assessed. There is currently no mandatory cyber security training for staff; however there is a new training system being implemented imminently although the mandatory modules are yet to be decided on. This is outlined in Finding 3. The ISIT has recently started sending out instructional emails to employees as good examples of security incidents captured by the team, a positive step forward in ensuring that the Council's employees are the best last line of defence against any potential incidents.

Overall Conclusions

The arrangements for managing risk were good with few weaknesses identified. An effective control environment is in operation, but there is scope for further 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.

1 Corporate Risk Register and Representation at GRAG

Issue/Control Weakness	Risk
Cyber risks have not been formally documented at a strategic level (on the corporate risk register). Lack of formal consideration of ICT risks at GRAG.	Cyber risks have not been formally documented, exposing the Council to cyber risks that have not been quantified, assigned mitigating actions or given a risk owner. Risk of more severe fall out and down time in the event of a cyber-related incident.

Findings

There are no security incident related risks captured on the Corporate Risk Register. The Corporate Risk register needs to be brought in line with the changing risk environment, which is ever increasingly rooted in cyber-enabled service provision and working practice. At the corporate level, there needs to be formal acknowledgement of the serious risk a potential security incident poses the Council.

Service level risks for ICT currently housed on Magique are out of date as they have not been refreshed recently (those with review dates go back to 2011 and 2008).

Whilst the Council has made positive steps to prioritise ICT issues at a corporate level, GRAG does not currently have any formal representation from ICT and the group's Terms of Reference (ToR) do not include ICT as an area of responsibility. However, the Assistant Director Customer Experience & Digital Services attends GRAG and could therefore be the solution to the lack of formal ICT representation.

Agreed Action 1.1

GRAG's ToR to be updated to include ICT. ICT to be represented by AD Customer Experience & Digital Services. Head of ICT/ ICT management to be invited to GRAG when necessary. Corporate Risk Register will be reviewed and risks related to cyber incidents put forward for inclusion. The ICT service risk register will be updated as appropriate.

Priority	2
Responsible Officer	AD, Customer Services & Digital
Timescale	December 2018

2 Testing the Security Incident Management Policy and Procedure

Issue/Control Weakness	Risk
There is an incident response procedure in place; however this has not been tested to ensure its efficacy.	Without an incident response plan, there is the risk that in the event of a cyber incident there are no systems, or processes in place to adequately respond. This could maximise the potential damage of an incident and cause significant reputational damage.

Findings

There is an up-to-date Security Incident Management Policy and corresponding procedure. The policy applies to Council staff and contains a significant amount of information on what an incident might look like and what responsibilities the end user has. The procedure applies to ICT staff and contains more streamlined information (including a Basic Incident Response Process Flow Diagram and an Appendix with Roles and Responsibilities and numerous contact details).

At the date of the audit, this procedure had not been formally tested. The Policy states that "The ICT Security Incident Coordinator(s) will test the ICT Security Incident management procedure on a regular basis." The draft suggests that this takes place annually. In order to gauge the appropriateness of the current procedure and ensure that all roles are clearly understood in the event of a real incident, the Policy and Procedure should be tested regularly.

Agreed Action 2.1

The ICT Security Incident Management Procedure to be tested annually going forward.

Priority	3
Responsible Officer	Head of ICT
Timescale	December 2018

3 Mandatory Cyber Security Training

Issue/Control Weakness	Risk
There is currently no mandatory cyber security training for staff.	Without continued and effective training in place, staff who encounter potential cyber attacks may not have the tools to identify the malicious activity or deal with it in the safest manner.

Findings

Employees are an organisation's strength or weakness in regards to cyber defences. There is currently no mandatory cyber security training for staff; however there is a new training system being implemented imminently. The mandatory modules are yet to be decided on.

Agreed Action 2.1

Cyber security/ incident security to be included as part of mandatory training for staff.

Priority	3
Responsible Officer	AD, Customer Services & Digital
Timescale	December 2018

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.

This page is intentionally left blank