ICT Governance and Cyber Security

City of York Council

Internal Audit Report 2018/19

Business Unit: Customer and Corporate Services Directorate
Responsible Officer: AD, Customer Services & Digital
Service Manager: Head of ICT
Date Issued: 20 June 2019
Status: Final
Reference: 10245/012

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

Summary and Overall Conclusions

Introduction

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."

Councils are making more local public services available digitally, getting more of their workforce online and planning greater collaboration and integration work with partner organisations. This way of delivering services requires access to, and the sharing of, residents’ and business customers’ data.

Ensuring the integrity, availability and confidentiality of this data by reviewing and reinforcing current cyber security arrangements is a priority for the council. The council’s cyber resilience is key to the administration and provision of essential services.

The council is working towards ISO 27001; one of the foremost ICT Standards. Discussions with the council’s ICT management have narrowed the focus of this year’s cyber security audit to a comparative review of the ICT operational environment against the best practice guidance provided in the ISO 27001 framework.

Work undertaken has also included follow up on the actions agreed as part of the 2017/18 ICT Governance and Cyber Security audit.

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:

- ICT operating responsibilities and procedures are documented.
- Changes to ICT facilities and systems are controlled.
- Capacity and performance is managed.
- Development, test and operational systems are separated.
- Malware controls are deployed, including user awareness.
- Appropriate backups are taken and retained in accordance with a backup policy.
- System user and administrator/operator activities, exceptions, faults and information security events are logged and securely protected.
- Software installation on operational systems is controlled.
- Technical vulnerabilities are patched, and there are rules in place governing software installation by users.
- An effective and mandatory cyber risk training programme is in place.

As part of the audit fieldwork, a survey was sent to all council staff members and councillors (not including schools) to gauge the level of cyber awareness at the council. The full survey results are attached at Appendix 1.

Key Findings

Overall, ICT has deployed an effective control architecture to manage the security risks that cyber incidents pose.

The council has a range of ICT policies available to staff via the intranet. These are subject to annual review and version control. Supplementary technical procedures are held by individual teams within ICT and are not held in a central repository. Whilst the council does not have ISO 27001 accreditation, it is a standard towards which they are working. To be compliant with the information security management system (ISMS) requirements of the standard, there are several policies and procedures that would need to be developed, including a formal risk assessment. In addition, the council would need to maintain a central repository of policies and procedures.

The controls in place for managing change requests are robust. The process for requesting a change to a business system is strictly controlled with scrutiny, oversight and authorisation embedded at each stage of the process. There are a limited number of individuals with access to request a change. Before the change is requested, it is subject to a peer review from within the service area. Change requests are reviewed by ICT, the service area and Business Intelligence to ensure alignment between the service area's needs, reporting requirements and technical concerns. At this stage, if any concerns are raised, the change request is taken to the appropriate governance board for a decision to be made. Change management is a standing agenda item at governance board meetings.

The Infrastructure Services Technical Team monitor the use of resources to ensure there is sufficient capacity to run the estate. The team actively monitor the state of all live servers and services, configured with appropriate thresholds to alert on low capacity events.

Discussions with the Infrastructure Services Technical Team Lead confirmed that test and development environments are isolated from the operational environment. The controls appear to be robust. For key systems updates, there are three stages of roll out. The proposed change is tested in the development environment. When the change is ready for user testing, the change is deployed in a test environment where users can check functionality. Only after the change has been tested and approved, will it be rolled out to the live system (sometimes in stages for added risk mitigation). Before the change goes live, a method statement is completed that details all of the work done. In this way, if a roll back is required, there is a trail of what has been done and the issue can be resolved. The change is rolled out to the live system when the changes are approved by the Change Advisory Board (CAB).

The council deploys various controls against the malicious use of software by end users. Antivirus software is run on all endpoints and servers and updated to the latest security signature daily. In addition, desktop computers have AppLocker software installed to prevent unauthorised software from being executed. Citrix Desktops use Ivanti Application Manager software to prevent unauthorised software from being installed. In the event that ICT are informed that potential malicious software has been run by a user either an infrastructure or security team member would investigate using diagnostic tools.

Email traffic is scanned using a cloud based scanner prior to being delivered to an on-premise gateway running a diagnostic tool. This then sends attachments to a sandbox environment which executes the attachments in isolation from the production environment. All web browsing is directed through on-premise proxy servers which scan for malware and other threats. The council utilises web filtering software and the National Cyber Security Centre's DNS system, which blocks access to known bad sites. In addition, the Information Security Incident Team (ISIT) has set up a script to send a warning email when the DNS service is not running as expected.

The council has controls in place to ensure that data is backed up regularly. File based data is backed up using hourly storage level snapshots. Virtual servers are backed up using daily storage level snapshots. Data is replicated to a secondary site over a mile from the primary data centre. In addition, database data is also stored in cloud based UK data centres. Backups are subject to different restoration tests and are held in accordance with retention schedules.

Audit logs recording exceptions and other relevant security events are produced and kept for a period defined by the ICT team. Events from domain controllers (for example, all logons and authenticated activity) are collected by a real-time, web based Active Directory (AD). Only named users have access to this system using domain user accounts[1] , the use of which are recorded and available for interrogation if required, audited. The group granting access is monitored and sends email alerts if the group membership is modified. The Infrastructure Services Technical Team utilise Password Manager Pro to provide secure access to a password vault which enables the checkout of passwords, access to servers using the checked out passwords and full auditing including video recording of session use. This system is protected by two factor authentication.

There are strong controls in place to facilitate effective vulnerability management. The council employs a vulnerability management system configured to include asset groups against which vulnerabilities are logged. Weekly reports are sent from the Security Team to ICT team leaders with a breakdown of vulnerabilities that need patching. The vulnerability management system performs a weekly scan to assess the status of identified vulnerabilities and deletes those that have been fixed. Users can also change the vulnerability status. For example, if a vulnerability cannot be patched immediately, Trend Deep Security is installed to plug the vulnerability and the status is set to deferred until support is available from the supplier.

The results of the Cyber Awareness survey highlighted an opportunity to establish a cyber-aware culture at the council. The survey highlighted that many council employees are not confident in their knowledge about cyber arrangements at the council, nor their role in preventing incidents and reporting them when they do occur. Training and end-user awareness forms one of the strongest defences in an organisation's cyber defence toolkit, and the first step the council is taking is the development of mandatory cyber awareness training. The full survey results can be viewed at Appendix 1.

---

[1] A domain user account enables the service to take full advantage of the service security features of Windows and Microsoft Active Directory Domain Services. The service has whatever local and network access is granted to the account, or to any groups of which the account is a member. The advantage of using a domain user account is that the service's actions are limited by the access rights and privileges associated with the account. Unlike a LocalSystem service, bugs in a user-account service cannot damage the system. If the service is compromised by a security attack, the damage is limited to the operations that the system allows the user account to perform.

There were two actions from the 2017/18 audit that were partially completed at the date of reporting. These have been included in the findings section and updated where appropriate.

There are no security incident related risks captured on the corporate risk register and whilst service level risks for ICT are currently housed on Magique they are out of date as they have not been refreshed recently.

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 the council's Governance, Risk and Assurance Group (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 Services & Digital attends GRAG and could therefore be the solution to the lack of formal ICT representation.

Agreed Action 1.1

GRAG ToR have been updated and will be ratified by 31 March 19. The Head of ICT attends GRAG as required. Corporate risk register updates are in hand and will be completed by 31 Mar 19 and then ongoing. ICT risk registers are updated as appropriate.

Priority	2
Responsible Officer	AD, Customer Services & Digital
Timescale	31 August 2019

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

A full walkthrough of the IT Security Incident Procedure was carried out in May 2019. Once the results have been written up, amendments will be made to the incident response procedure based on the lessons learned from the test. Once this has been completed a full walk through of the amended incident response procedure will be carried out. The council will also be attending a wider security incident management walkthrough with colleagues from the regional WARP (Warning, Advice and Reporting Point) in March 2019.

Priority	3
Responsible Officer	Head of ICT
Timescale	31 August 2019

3 Mandatory Cyber Security Training

Issue/Control Weakness	Risk
At the time of the audit, there was 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

In order to assess the level of cyber awareness at the council, a survey was developed with the input of the Information Security Incident Team and sent out to all council employees and members. 311 responses were received, a response rate of 10%, and the full survey results are attached. The responses indicate that there are inconsistencies in the level of cyber awareness at the council.

Whilst 16% felt they were extremely or very knowledgeable, 20% of respondents felt they were not very knowledgeable about the council's information security policies and practices, with 5% feeling they were not at all knowledgeable. 18% of respondents did not know where to access ICT Policies and Procedures. 47% of those surveyed did not know if the council has an ICT Strategy that addresses cyber risks.

Should an incident occur, 34% of those who took the survey did not know that the correct procedure would be to report it to ICT Service Desk. 69% did not know if the council provided formal cyber awareness training, yet 55% believed this training was required by some or all employees. 50% of respondents indicated that they had never received cyber awareness training, from the council or a previous employer.

When asked to rate the threat of data and information systems breaches to the council on a sliding scale of 0 (no threat) to 5 (high likelihood), the average number chosen was 4. 87% of respondents felt that the council should prioritise cyber security as a key corporate risk.

Respondents were welcomed to leave their thoughts and comments about the survey and cyber security in the context of the council. These responses have been included with the full survey results as an appendix to the report.

Agreed Action 3.1

Cyber security/ incident security is now be included as part of mandatory training for staff. Approval for mandatory status has been approved and the Workforce Development Unit informed accordingly to roll-out via MYLO (the council's e-learning system).

ISIT and Veritau will also host a Cyber Awareness Week in summer, including drop in sessions for staff and communications on screens and in kitchens.

Priority	3
Responsible Officer	AD, Customer Services & Digital
Timescale	31 August 2019

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.

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.