Board of Management
Audit & Assurance Committee

Date of Meeting	**Tuesday 11 June 2024**
Paper No.	**AAC4-I**
Agenda Item	**5.4.1**
Subject of Paper	**Internal Audit Report – IT Network Arrangements/Security**
FOISA Status	**Disclosable**
Primary Contact	**Henderson Loggie**
Date of production	**23 April 2024**
Action	**For Discussion and Decision**

1. Recommendations

The Committee is asked to consider and discuss the report and the management responses to the internal audit recommendations.

2. Purpose of report

The purpose of this review is to provide management and the Audit and Assurance Committee with assurance on key controls relating to the curriculum and financial plans in place for City of Glasgow College and their alignment with the regional plan for Glasgow and the college student number targets.

3. Key Insights

This internal audit of IT Network Arrangements/Security provides an outline of the objectives, scope, findings and graded recommendations as appropriate, together with management responses. This constitutes an action plan for improvement.

The Report includes a number of audit findings which are assessed and graded to denote the overall level of assurance that can be taken from the Report. The gradings are defined as follows:

Good	System meets control objectives.
Satisfactory	System meets control objectives with some weaknesses present.
Requires improvement	System has weaknesses that could prevent it achieving control objectives.
Unacceptable	System cannot meet control objectives.

4. Impact and implications

Refer to internal audit report.

Appendix – Internal Audit Report – IT Network Atrrangements/Security

LEVEL OF ASSURANCE
Satisfactory

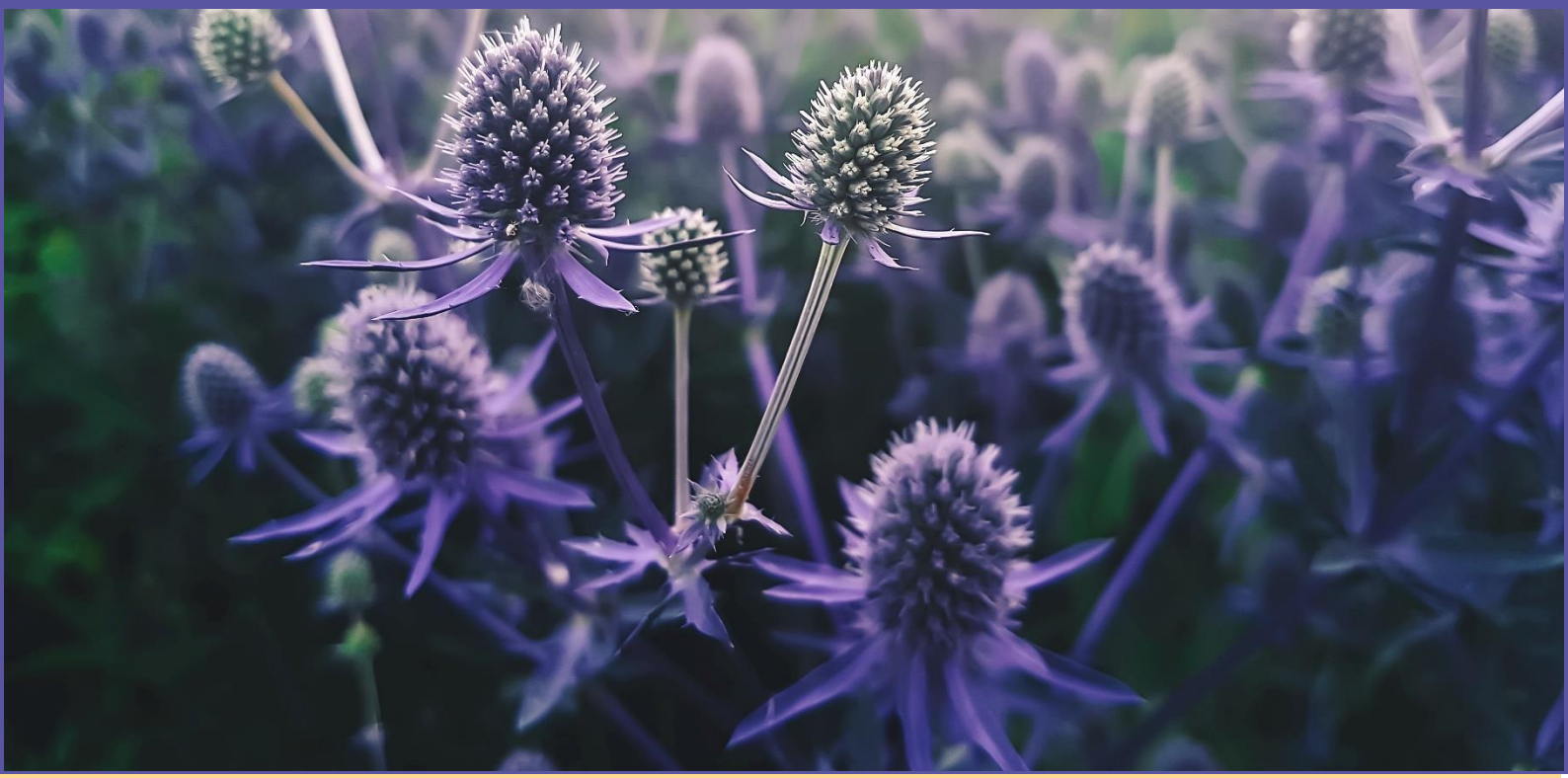
City of Glasgow College

IT Network Arrangements / Security

Internal Audit report No: 2024/08

Draft issued: 2 April 2024

Final issued: 23 April 2024



Henderson Loggie

Contents

Level of Assurance

In addition to the grading of individual recommendations in the action plan, audit findings are assessed and graded on an overall basis to denote the level of assurance that can be taken from the report. Risk and materiality levels are considered in the assessment and grading process as well as the general quality of the procedures in place.

Gradings are defined as follows:

Good	System meets control objectives.
Satisfactory	System meets control objectives with some weaknesses present.
Requires improvement	System has weaknesses that could prevent it achieving control objectives.
Unacceptable	System cannot meet control objectives.

Action Grades

Priority 1	Issue subjecting the organisation to material risk and which requires to be brought to the attention of management and the Audit and Assurance Committee.
Priority 2	Issue subjecting the organisation to significant risk and which should be addressed by management.
Priority 3	Matters subjecting the organisation to minor risk or which, if addressed, will enhance efficiency and effectiveness.

Management Summary

Overall Level of Assurance

Satisfactory	System meets control objectives with some weaknesses present.

Risk Assessment

This review focused on the controls in place to mitigate the following risks on the City of Glasgow College ('the College') Strategic Risk Register (as at March 2024):

- SR12 – Negative impact of statutory compliance failure (Net Score 10, Medium);
- SR14 – Failure of compliance with the General Data Protection Regulations (GDPR) (Net Score 8, Medium);
- SR16 – Failure of business continuity (Net Score 12, Medium); and
- SR18 – Failure of IT system security (Net Score 10, Medium).

Background

As part of the Internal Audit programme at the College for 2023/24 we conducted a review of the College's IT network arrangements, including cyber security controls. The Audit Needs Assessment, agreed with management and the Audit and Assurance Committee on 2 March 2022, identified this as an area where risk can arise and where Internal Audit can assist in providing assurances to the Principal and the Audit and Assurance Committee that the related control environment is operating effectively, ensuring risk is maintained at an acceptable level.

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

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

Cyber security is central to the health and resilience of any organisation reliant on digital technology to function, and this places it firmly within the responsibility of the Board.

The National Cyber Security Centre's (NCSC) 10 Steps to Cyber Security guidance aims to help organisations manage their cyber security risks by breaking down the task of protecting the organisation into 10 components. Adopting security measures covered by the 10 Steps reduces the likelihood of cyber-attacks occurring and minimises the impact to an organisation when incidents do occur.

Scope, Objectives and Overall Findings

This audit included a review of the College's current position with regard to information and cyber security in order to advise on areas that should be addressed in line with the latest guidance produced by the NCSC, the UK Government's national technical authority for information assurance.

The table below notes the objective for this review and records the results:

Objective	Findings			
The objective of our audit was to obtain reasonable assurance that:		**1**	**2**	**3**
		No. of Agreed Actions		
1. The internal controls in place which ensure that the security of the ICT network, the configuration of key elements of ICT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users is in line with the NCSC 10 Steps to Cyber Security guidance.	**Satisfactory**	0	1	3
Overall Level of Assurance	**Satisfactory**	**0**	**1**	**3**
		System meets control objectives with some weaknesses present.		

Audit Approach

From discussion with Director of IT and members of the College's IT Team, and review of documentation, we identified the systems and internal controls in place and compared these with expected controls. A walkthrough of key systems was undertaken to confirm our understanding, and this was followed-up with compliance testing where considered necessary. We have reported on areas where expected controls were found to be absent or where controls could be further strengthened. Our approach was based upon the guidance and best practice provided by NCSC which covered the following areas:

- Risk management;
- Engagement and training;
- Asset management;
- Architecture and configuration;
- Vulnerability management;
- Identity and access management;
- Data security;
- Logging and monitoring;
- Incident management; and
- Supply chain security.

Summary of Main Findings

The graphic at Appendix I illustrates the College's current position, based on our assessment, in relation to the NCSC's 10 Steps to Cyber Security guidance.

Strengths

Throughout our review we observed examples of good practice, and we welcomed the willingness of College staff to assist our review and to seek ways to improve security within the College. We have concluded that, overall, the College exhibits a strong awareness of information / cyber security risks and impacts, and that the control environment demonstrates good practice with many of the expected cyber security controls, for an organisation of this size and complexity. These include:

- a risk management regime has been established, which includes identifying cyber security as key strategic and operational risks, and there are structures in place which act as appropriate bodies for evaluating and monitoring information security risks within the College;
- hardware and software inventories have been created along with processes and tools for asset identification;
- processes are in place for applying updates and patches to all College managed devices which connect to the College network;
- the IT architecture protects the College network through use of firewalls and direct connections to untrusted external services, and protects internal IP addresses;
- management of user accounts is linked to the College's starter, leaver and change of role procedures;
- administrator access to network components is carried out over dedicated network infrastructure and secure channels using communication protocols that support encryption;
- Two-factor authentication (2FA) is in place for access to all corporate systems and data;
- data in transit is protected through encryption and secure communication channels;
- standard baseline security builds have been established for all College managed devices to ensure the consistency of security configurations;
- Processes are in place to regularly test and monitor the effectiveness of cyber security training. Training is supported through regular communication of good practice to promote a positive cyber security culture;
- network hosts and endpoints are protected by an antivirus solution, which automatically scans for malware;
- tools are deployed to allow anomalous activity to be detected in a timely manner and the potential impact of events to be understood; and
- the College successfully obtained its recertification for Cyber Essentials Plus in December 2023, demonstrating that recognised security management good practice is being applied which has been subject to external independent scrutiny.

Weaknesses and Opportunities

We identified several opportunities for improving the robustness of the control environment to reduce the potential for cyber-attack and data loss. These include:

- improving monitoring of mandatory cyber security training compliance;
- reviewing external user access to College Microsoft Teams groups and user permissions for external and third-party systems used by the College;
- validating the College's backup and recovery capability through real time restore of back-ups; and
- improving cyber security incident identification and reducing incident response times through automatically prioritising and escalating cyber security incident service desk tickets.

Summary of Main Findings (Continued)

Weaknesses and Opportunities (continued)

In Internal Audit report 2021/05 – IT Network Arrangements / Security, which was issued in November 2021, it was reported that the security of the College IT network was at risk of compromise due to the building access and CCTV systems, which are managed by FES, being connected to the College network. It was previously identified that those systems had not been patched or updated since they were first installed in 2016. We noted that the College has since raised these concerns with FES at a senior level and patching issues have been resolved. The College is planning a further reconfiguration of its network later in 2024, at which point FES will move the buildings access and CCTV systems to a separate network.

The implementation of the recommendations in this report will reduce the College's current risk position; and will enhance the College's ability to manage IT security risks on an on-going basis.

Acknowledgments

We would like to take this opportunity to thank the staff at the College who helped us during our audit review.

Main Findings and Action Plan

Objective 1: The internal controls in place which ensure that the security of the ICT network, the configuration of key elements of ICT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users is in line with the NCSC 10 Steps to Cyber Security guidance.

Education and Training
People should be at the heart of any cyber security strategy. Good security considers the way people work in practice and doesn't get in the way of people getting their jobs done. People can also be one of your most effective resources in preventing incidents (or detecting when one has occurred), provided they are properly engaged and there is a positive cyber security culture which encourages them to speak up. Supporting your staff to obtain the skills and knowledge required to work securely is often done through the means of awareness or training. This not only helps protect your organisation, but also demonstrates that you value your staff, and recognise their importance to the business.

Mandatory cyber security training forms part of induction training for new staff. All staff receive mandatory baseline and refresher cyber security training. New staff have three months to complete the full induction training pack, including mandatory training. Cyber security training can be completed up to three months after a user is given a College owned device and has access to the College's systems and data. Whilst not a significant risk for low level users, such as cleaners, it is an elevated risk for users in high volume processing roles and / or those with access to personal and sensitive data, for example finance and student records.

Mechanisms have been established for testing the effectiveness and value for money of the security training provided to staff with tailored ethical phishing campaigns run regularly. Remedial training and guidance are issued to staff that fail tests through demonstrating risky behaviours, e.g. clicking on suspicious attachments or links, or entering sensitive data.

The College assessment of the risk associated with high volume processing roles, or those with access to personal/sensitive data, is that this risk is considered minimal, due to the level of training involved before the individual would process on their own. The line manager is responsible for making sure these risks are mitigated by ensuring mandatory training is completed and, where required, in a suggested order.

The College has established processes and checks/security software in place to prevent cyber-attacks and currently it is not deemed a priority to change the induction process.

Objective 1: The internal controls in place which ensure that the security of the ICT network, the configuration of key elements of ICT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users is in line with the NCSC 10 Steps to Cyber Security guidance (Continued).

Observation	Risk	Recommendation	Management Response	
We reviewed the College's approach to cyber awareness training and noted that the College issues regular communications and guidance to staff on cyber security: via the College intranet; by email; as part of the staff development days; ad hoc training for staff groups; and advice provided to individual staff members. As noted above, mandatory cyber security training is also in place for all staff. Completion of mandatory cyber security training is monitored by the Organisational Development (OD) team with reports then passed to line managers to follow-up with staff. The College uses an e-learning training package which contains a suite of cyber modules which staff are required to complete on a rolling monthly basis. We obtained a copy of a report from the College's OD team, showing completion rates for the cyber security e-learning module. We noted from this report, that there were 657 users listed, out of 1,140 users, where the user had not completed the training. This indicates that either not all staff are completing the mandatory training; that results are not being accurately recorded when staff are completing the training; and / or there are weaknesses in the process for reviewing completion data and following up with staff to ensure that mandatory training is being completed in line with the College policy.	Organisations that do not effectively support users through education and awareness may be vulnerable to a range of risks, including: • introduction of malware and data loss through inappropriate use of systems; • legal sanctions due to loss of sensitive data; • external attacks due to email phishing and social engineering; and • data loss or corruption due to an internal attack by a dissatisfied employee.	**R1** Line managers should be reminded of the need to ensure that staff complete all mandatory training, in accordance with the College policy. Data on completion rates of the mandatory cyber security e-learning module should be shared with the Director of IT and reported to the People & Culture Committee, as part of existing cyber security reporting, and trends in completion rates should be monitored over time.	Completion reports for all mandatory training to be shared at SMT on a monthly basis. A high level overview of mandatory training completion rates currently goes to the People and Culture Committee as part of the HR Staff Metric Report. This report is also tabled at SMT. **To be actioned by:** OD Manager **No later than:** 30 September 2024	
			Grade	**2**

Objective 1: The internal controls in place which ensure that the security of the ICT network, the configuration of key elements of ICT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users is in line with the NCSC 10 Steps to Cyber Security guidance (Continued).

Identity and Access Management

Access to data, systems and services need to be protected. Understanding who or what needs access, and under what conditions, is just as important as knowing who needs to be kept out. You must choose appropriate methods to establish and prove the identity of users, devices, or systems, with enough confidence to make access control decisions. In developing appropriate identity and access management policies and processes, ensure that these do not just cover systems within the College's direct control, but also wherever College identities can be used (for example, websites or online services where staff create an account by using their work email address).

Objective 1: The internal controls in place which ensure that the security of the ICT network, the configuration of key elements of ICT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users is in line with the NCSC 10 Steps to Cyber Security guidance (Continued).

Observation	Risk	Recommendation	Management Response
An increasing amount of College data is held within a Microsoft (MS) Teams structure for internal use, however external users can be invited into internal Teams groups. IT staff do not have full visibility of the data held within MS Teams or are able to control who has access to MS Teams Groups, as this is the responsibility of departmental managers or MS Teams group owners. We noted that there is a need for more robust guidance for staff relating to granting and revoking user access rights in MS Teams, particularly for external user access. IT has sight of all networked services which are accessed using approved staff user accounts and credentials, which are protected by multi-factor authentication (MFA) and encryption. Across the College, there may be instances where departments use third party systems or cloud services using College email addresses to set up accounts for those services which IT do not have full sight of. For College controlled services, a Human Resources driven starter, leaver and change of role procedure is in place which allows IT to revoke or change user access when notified by Human Resources. For third party or cloud services, IT is reliant on line managers revoking or amending user access when staff leave or change role, however there is no formal procedure or guidance to manage this process.	Individuals or systems obtain unauthorised access to data or services, resulting in system security being compromised, data breaches or fraud. Reputational damage to the College and reduced trust from staff, students, and other stakeholders.	**R2** It is recommended that an audit is undertaken of external, or guest accounts, associated with College MS Teams groups to identify any instances where external access is no longer required, and action should be taken to revoke access, as required. An audit of cloud and third-party systems in use across the College estate, which are not directly linked to College Active Directory or Office365 accounts, should also be undertaken to identify instances of staff using College logins and email accounts and put in place procedural guidance for line managers to revoke user access to such accounts, and to ensure two-factor authentication (2FA) is used and promote good password management.	IT will follow Microsoft best practise to review guest user access across all Microsoft 365 groups, using the Azure AD Access review feature. Group owners will receive review notifications with Azure admins (IT) being able to monitor the activity. **To be actioned by:** Director of IT **No later than:** 30 September 2024 An annual audit of cloud and third-party systems to be completed and include checks on 2FA and good password management. A procedural guide for revoking user access to such accounts will be designed as well as a password guidance procedure. **To be actioned by:** Director of IT **No later than:** 30 September 2024
			Grade **3**

Objective 1: The internal controls in place which ensure that the security of the ICT network, the configuration of key elements of ICT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users is in line with the NCSC 10 Steps to Cyber Security guidance (Continued).

Incident Management
Incidents can have a huge impact on an organisation in terms of cost, productivity, and reputation. However, good incident management will reduce the impact when they do happen. Being able to detect and quickly respond to incidents will help to prevent further damage, reducing the financial and operational impact. Managing the incident whilst in the media spotlight will reduce the reputational impact. Finally, applying what you've learned in the aftermath of an incident will mean you are better prepared for any future incidents.

To reduce the impact of compromise of network and systems security, it is good practice to plan for backup and recovery. Plans should include data and services, such as relevant configurations and accounts, and that you have tested your plans so that you are able to respond effectively in the event of a major incident such as a ransomware attack. You should have backups that remain protected and can be accessed in the event of a significant incident.

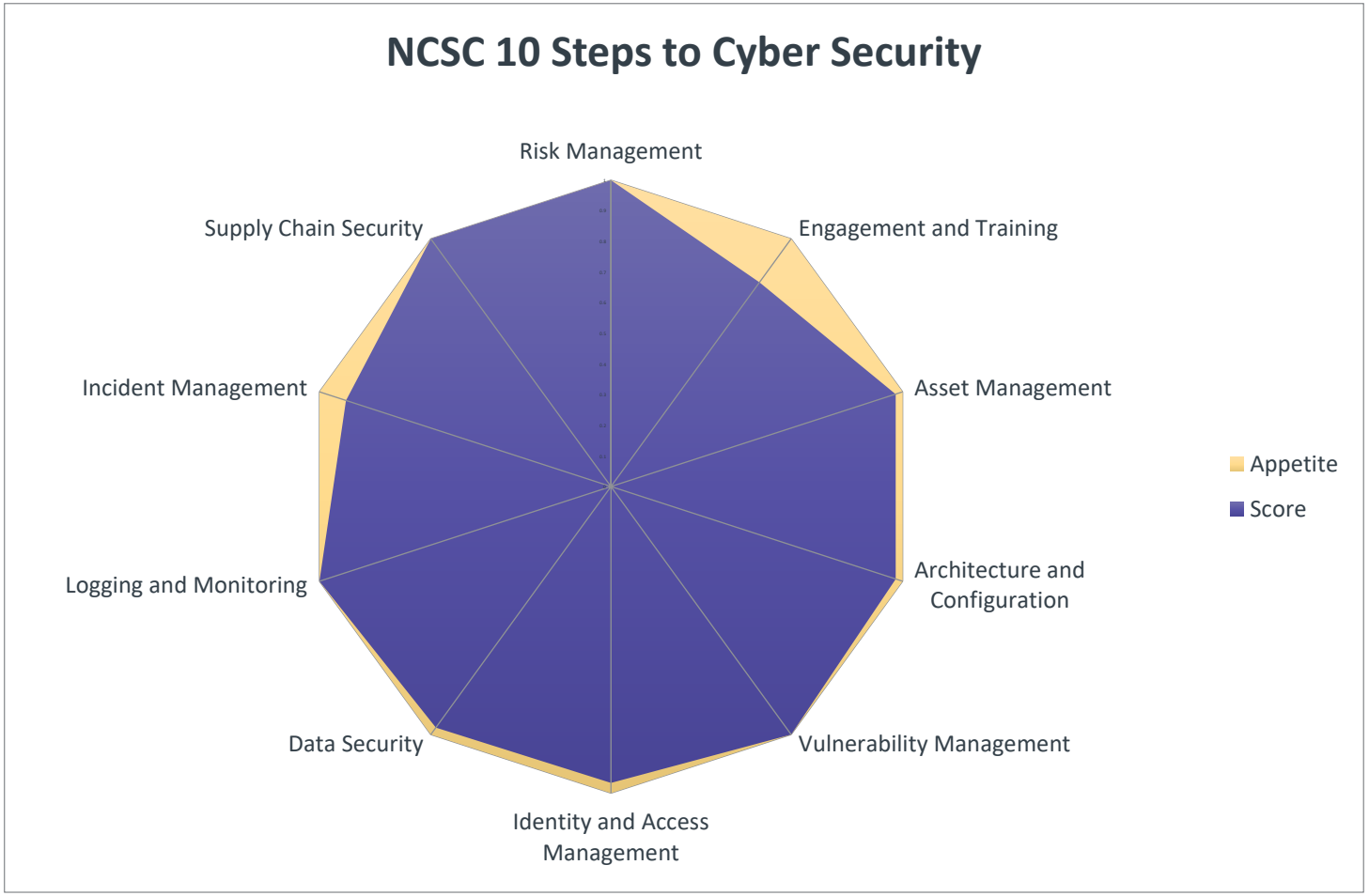
Observation	Risk	Recommendation	Management Response	
We noted that backup solutions are in place, including backups taken daily and weekly, backups are protected through encryption and are not connected to the main domain, and multiple copies are retained across several sites, including physical tape backups. Whilst back-ups have been partially tested in the past, through recovery of files, a full system and data restore has not been undertaken to provide assurance that a full restore would work as per the College's Business Continuity and Incident Response plans and can be restored in line with the expected recovery time objectives (RTOs).	Incident response capability is compromised due to inadequate backup and recovery plans.	**R3** A full, real-time test of the College's backup and recovery capability should be planned and undertaken to test the robustness of the College's recovery plans and to provide assurance that the RTOs outlined in those plans are both realistic and achievable. Testing should be scheduled for a time that minimises any potential disruption to the College's operations.	An annual exercise will be conducted with an external body with a lesson's learned follow up, to test our backup and recovery capability. **To be actioned by:** Director of IT **No later than:** 30 May 2025	
			Grade	**3**

Objective 1: The internal controls in place which ensure that the security of the ICT network, the configuration of key elements of ICT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users is in line with the NCSC 10 Steps to Cyber Security guidance (Continued).

Observation	Risk	Recommendation	Management Response	
The IT service desk plays a critical role in cybersecurity incident management, and its involvement in the incident detection and response process is essential. By integrating the IT service desk into its cybersecurity incident response, the College can reduce the response time and minimise the impact of a cybersecurity attack and protect its assets. Automatically flagging cybersecurity incidents in IT service desk tickets is crucial for several reasons: • Early Detection: Service desks often serve as the first point of contact for users experiencing issues. Automatic flagging can help in the early detection of unusual activities that may indicate a security breach. • Quick Response: By flagging incidents, the College can ensure a swift response to potential threats, reducing the time attackers have to cause damage. • Coordination and Communication: It helps in coordinating the response among different teams and ensures that all relevant parties are informed and involved in the resolution process. We noted that there is no classification of cyber security incidents within service desk tickets that allows automatic prioritisation and escalation to senior IT staff.	A cyber security incident may go unnoticed for an extended period, allowing the attack to cause more damage, disruption and greater loss of data.	**R4** The IT service desk should be configured to allow cyber security incidents to be automatically prioritised and escalated to senior IT staff.	IT will create a dedicated Cyber Incident Service within our service desk that will alert all members of the Computer Emergency Response Team (CERT) and IT Senior Management. **To be actioned by:** Director of IT **No later than:** 30 June 2024	
			Grade	**3**

Appendix I – NCSC 10 Steps to Cyber Security

The Graphic below illustrates the College's current position, based on our assessment, in relation to the NCSC's 10 Steps to Cyber Security guidance.



Henderson Loggie

Aberdeen 45 Queen's Road AB15 4ZN
Dundee The Vision Building, 20 Greenmarket DD1 4QB
Edinburgh Ground Floor, 11-15 Thistle Street EH2 1DF
Glasgow 100 West George Street, G2 1PP

T: 01224 322 100
T: 01382 200 055
T: 0131 226 0200
T: 0141 471 9870

F: 01224 327 911
F: 01382 221 240
F: 0131 220 3269