Board of Management
Audit & Assurance Committee

Date of Meeting	**Tuesday 23 November 2021**
Paper No.	**AAC2-K**
Agenda Item	**5.5.6**
Subject of Paper	**Internal Audit Report – IT Network Arrangements/Security**
FOISA Status	**Disclosable**
Primary Contact	**Henderson Loggie**
Date of production	**17 November 2021**
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 Arrangements/Security

LEVEL OF ASSURANCE
Satisfactory

City of Glasgow College

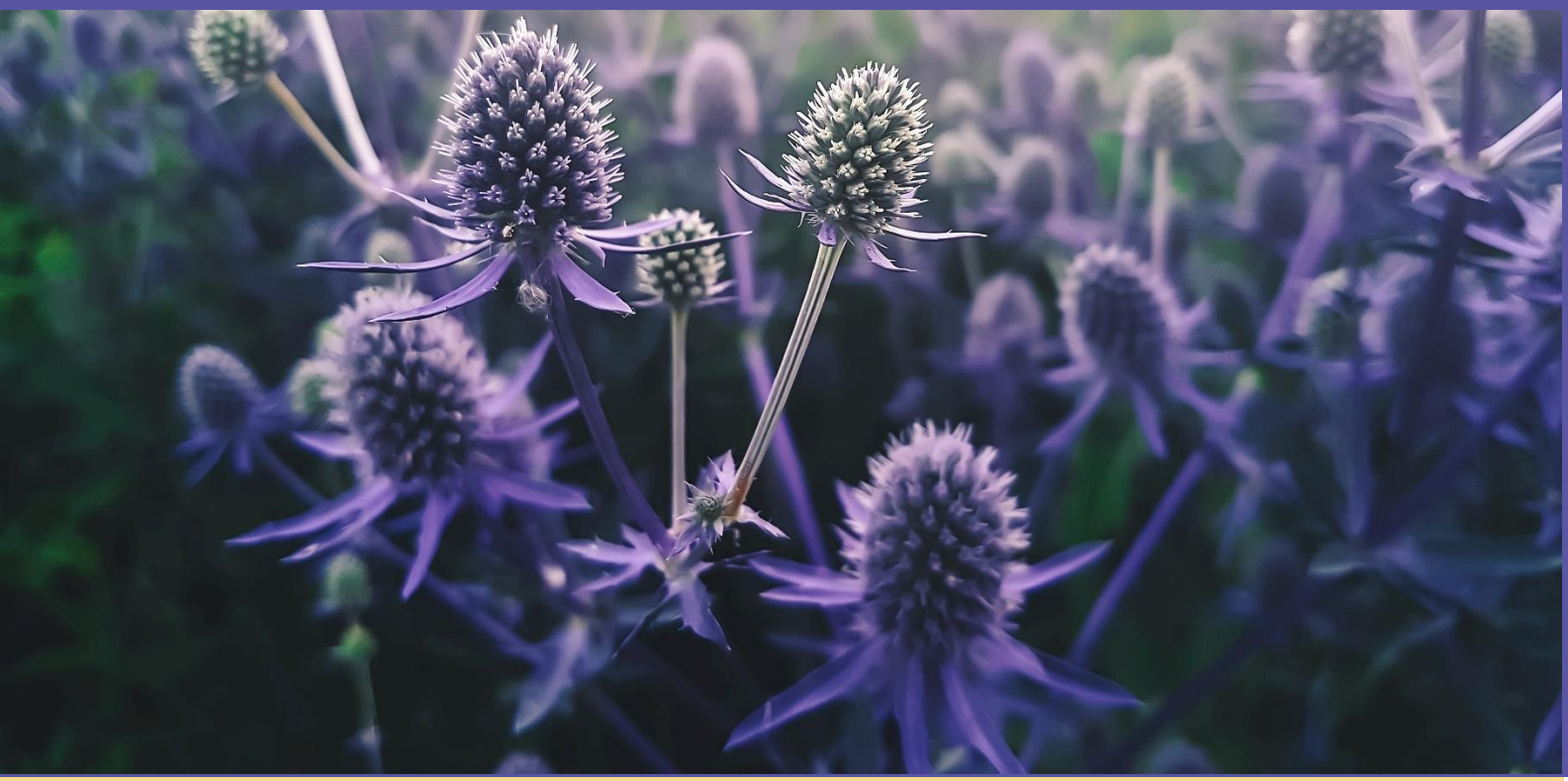
IT Network Arrangements / Security

Internal Audit report No: 2021/05

Draft issued: 16 November 2021

2nd Draft Issued: 17 November 2021

Final issued: 17 November 2021



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:

- Risk number 12 – Failure of Business Continuity (risk rating: medium);
- Risk number 24 – Failure of compliance with the GDPR (risk rating: medium); and
- Risk number 25 – Failure of IT system security (risk rating: medium)

Background

As part of the Internal Audit programme at the College for 2020/21 we conducted a review of the College's IT network arrangements, including cyber security controls. The Audit Needs Assessment identified this as an area where risk can arise and where Internal Audit can assist in providing assurances to the management and the Audit 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.

This 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

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

Objective	Findings			
The objective of our audit was to:		**1**	**2**	**3**
		No. of Agreed Actions		
1. Review the College's current position with regard to information and cyber security to advise on areas that should be addressed in line with the latest guidance produced by the NCSC. This also included a high-level review of the College's ICT Business Continuity and Disaster Recovery arrangements.	**Satisfactory**	0	0	7
Overall Level of Assurance	**Satisfactory**	**0**	**0**	**7**
		System meets control objectives with some weaknesses present.		

Audit Approach

From discussion with the IT Director 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 any 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

Strengths

Throughout our review we observed examples of good practice and we welcomed the willingness of the 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, as shown within the graphic at Appendix I of this report. 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.
- 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.
- mandatory cyber security awareness training is in place for all staff and processes are in place to test and monitor the effectiveness of 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.

Weaknesses

Using the latest guidance available from the NCSC we identified some weaknesses across the ICT environment and noted potential for cyber-attack and data loss through several avenues. The implementation of the recommendations in this report will reduce the College's current risk position; reinforce the College's preparations for Cyber Essentials certification and will enhance the College's ability to manage IT security risks on an on-going basis.

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.

Acknowledgment

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: Review the College's current position with regard to information and cyber security to advise on areas that should be addressed in line with the latest guidance produced by the NCSC. This also included a high-level review of the College's ICT Business Continuity and Disaster Recovery arrangements.

Risk Management
A risk-based approach to securing data and systems should be adopted. Taking risks is a natural part of doing business. Risk management informs decisions so that the right balance of threats and opportunities can be achieved to best deliver your business objectives. Risk management in the cyber security domain helps ensure that the technology, systems, and information in the College are protected in the most appropriate way, and that resources are focussed on the things that matter most to the College's business. A good risk management approach will be embedded throughout the College and complement the way in which other business risks are managed. To be fully effective, an information risk management regime should be supported by an empowered governance structure, which is actively supported by the Board and senior management. Our review identified that there are appropriate structures in place for evaluating and monitoring information security risks within the College, for example the Change Advisory Board and Digital Transformation Group, as well as regular meeting between IT and college departmental leads.

Observation	Risk	Recommendation	Management Response	
At a corporate level, a risk management regime has been established with a Strategic Risk Register, which identifies IT security as a key risk, which is monitored by the Audit and Assurance Committee and the Executive Team in line with the College's risk management framework. Cyber security risks are recorded on a separate cyber risk register and monitored by the IT team, although these are not formally reported to the Executive Team or to the Board.	Cyber security risks and vulnerabilities are not formally monitored, and information is not available to inform and improve decision making regards responding effectively to new threats as they emerge.	**R1** To effectively communicate the College's risk management approach to staff and decision makers, so that they understand how cyber security risks should be managed and to help them make decisions about them, updates on the threat landscape, events, actions, and plans surrounding cyber security within the college and the sector should be reported to the Executive and to the Board regularly. Reporting should include a summary of the top-rated risks on the College's cyber risk register and details of mitigations already in place and those further required.	**Completed** Dedicated section to Cyber Security & Risk now included in the Finance & Physical Resources Committee IT Update.	
			Grade	**3**

Objective 1: Review the College's current position with regard to information and cyber security to advise on areas that should be addressed in line with the latest guidance produced by the NCSC. This also included a high-level review of the College's ICT Business Continuity and Disaster Recovery arrangements (continued).

Architecture and Configuration

The technology and cyber security landscape is constantly evolving. To address this, organisations need to ensure that good cyber security is baked into their systems and services from the outset, and that those systems and services can be maintained and updated to adapt effectively to emerging threats and risks. The impact of a security compromise should be reduced by preventing lateral movement across infrastructure and systems and by making it easier to recover from a security incident. After an initial compromise, attackers will typically attempt to gain access to other systems and data. The College network infrastructure should be designed to make it harder for an attacker to reach their target once in the network by protecting data and communications, and ensuring critical components are more isolated using segregated networks or adopting a zero-trust architecture.

Observation	Risk	Recommendation	Management Response	
We noted that the security of the College IT network is at risk of compromise due to weaknesses in network segmentation resulting from systems being connected to the College network which are owned and managed by a third party, which the College has no direct control of. For example, the building access and CCTV systems are managed by FES, who are responsible for the maintenance of the campus buildings, and the College IT team have identified that these systems have not been patched or updated since they were first installed in 2016. Unpatched systems represent a significant threat to network security and whilst good practice would be to improve network segmentation to reduce the risk to College systems and data, full removal of vulnerable systems would be best practice. We noted that the College has raised these concerns with FES at a senior level but to date these issues have still to be resolved. Further discussions with FES regarding this issue are required in order to inform the College's future network infrastructure design and investment decisions.	Security vulnerabilities in third party systems connected to the College infrastructure are used to disrupt or access College systems or data.	**R2** Discussions with FES regarding upgrading and patching of systems operating on the College IT network should consider the following options: • transferring ownership of the buildings access and CCTV systems to the College; • FES developing a programme of upgrading and patching of systems in line with the system vendor requirements and providing confirmation of upgrades and patches to the College IT team; and • removing the building access and CCTV systems from the College IT network and transferring them to a separate dedicated network (optimal solution).	The College have made some progress on this issue by obtaining agreement with FES\GLQ to migrate aspects of the building management system at Riverside moving it to a own dedicated segmented area of our network. Further discussions and changes will be required. **To be actioned by:** Director of IT **No later than:** 30 June 2022	
			Grade	**3**

Objective 1: Review the College's current position with regard to information and cyber security to advise on areas that should be addressed in line with the latest guidance produced by the NCSC. This also included a high-level review of the College's ICT Business Continuity and Disaster Recovery arrangements (continued).

Architecture and Configuration (continued)

Observation	Risk	Recommendation	Management Response	
Security testing can take many forms including configuration review and penetration testing. Penetration Testing is the practice of testing computer systems, networks, and applications to find vulnerabilities that an attacker could exploit. Penetration Tests simulate how an attacker would review and attack a system, which is different from the use of vulnerability scanning solutions. A vulnerability scanner produces a prioritised list of vulnerabilities whereas a penetration test considers all vulnerabilities as well as identifying misconfigurations and system flaws, which may be exploited. We noted that penetration was undertaken by a third party earlier in 2021 as a requirement of the College's cyber insurance arrangements. No evidence was presented to demonstrate that security testing takes place as part of application development, both in-house and external, prior to implementation of new systems.	Without performing penetration testing, the College is at risk of releasing code and systems that contain vulnerabilities which can be used to attack users or the College's systems and data.	**R3** Ensure that penetration or security testing is performed on all internally developed systems and applications to ensure that existing vulnerabilities are identified and suitably remediated prior to implementation. Confirmation of similar testing should be obtained from third party developers.	IT Team will ensure that all future internally developed systems are penetration tested as part of system testing. Retrospective Testing of the main internally developed Enquirer system will be conducted in 2 phases; internally by the IT Team and then externally by a Technology partner to verify test outcomes. Penetration Testing to be completed by March 2022 Remedial work planned & completed by September 2022. **To be actioned by:** Director of IT **No later than:** 30 September 2022	
				Grade **3**

Objective 1: Review the College's current position with regard to information and cyber security to advise on areas that should be addressed in line with the latest guidance produced by the NCSC. This also included a high-level review of the College's ICT Business Continuity and Disaster Recovery arrangements (continued).
Architecture and Configuration (continued)

Observation	Risk	Recommendation	Management Response
To make compromise and disruption difficult the potential attack surface should be reduced by removing or disabling configurations and features that aren't required. This should include applying secure configurations to end user devices to restrict the options available to an attacker. There has been no formal assessment of business requirements for staff users' connecting input/output devices and removable media (including Smart phones and USBs) to College devices. The use of removable media, such as USBs, is currently unrestricted for staff and there is no requirement to ensure that only encrypted and approved USBs are used by staff. With the availability of secure remote connections and provision of file transfer tools such as One Drive for staff there is now a reduced business need for the continued use of USBs by staff. During Covid, the College has been able to successfully demonstrate that it can adopt and deploy applications and tools which enable remote working practices and cloud solutions. Staff have been able to successfully demonstrate that they can adapt to and embrace these new working practices. The continued use of USBs appears to persist as a matter of user culture. As removable media is a popular attack vector for introducing malicious programmes into the computer network, restrictions on the use of these devices should be considered to provide further protections to the College systems and data. We acknowledge that a greater degree of flexibility may be required in the short term for students when using removable media devices, however the risks to compromise of College systems and data arising from students using USBs are reduced due to their limited access to College networked services.	Removable media is a popular attack vector for introducing malicious programmes into the computer network. Loss of USBs resulting in loss of potentially sensitive data and breach of data protection legislation.	**R4** It is recommended that awareness of the risks arising from the use of removable media is re-enforced to staff and students. This should then be followed up with the introduction of a College-wide requirement for all staff and students to use encrypted USBs only, leading to a restriction in the use of USBs enforced by policy (through whitelisting of devices and port restrictions) and ultimately over time, the full removal of the ability to use such devices.	The removal of USB drives has been a Strategic Aim of the IT Team which has now been facilitated by the adoption of Office 365 & Teams \OneDrive over the past 18 months (for both staff & students). Phase 1: engage with Digital Transformation Group to explain USB removal plan (December 2021) and seek support to eliminate USBs or allow only encrypted USBs (IT would support full ban on USBs however could impact Student Learning). Phase 2: explore option to only allow encrypted USBs (February 2022) Phase 3: unencrypted USB storage blocked from College devices (September 2022) **To be actioned by:** Director of IT **No later than:** 30 September 2022
			Grade **3**

Objective 1: Review the College's current position with regard to information and cyber security to advise on areas that should be addressed in line with the latest guidance produced by the NCSC. This also included a high-level review of the College's ICT Business Continuity and Disaster Recovery arrangements (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. A good approach to identity and access management will make it hard for attackers to pretend they are legitimate, whilst keeping it as simple as possible for legitimate users to access what they need.

Observation	Risk	Recommendation	Management Response
We noted that external interfaces are vulnerable to attack due to user authentication for remote users accessing networked services only relying on staff username and password controls. Due to the increasing prevalence of phishing and malware attacks, passwords are no longer sufficient to maintain an adequate level of security for business-critical infrastructure and services. Two-factor authentication (2FA) should be considered the minimum acceptable level of access control. Although 2FA has been made available for all users, it is not yet enabled by default for all users, devices and systems. We noted that there are staff who access College systems remotely who have not been issued with a College mobile phone and have yet to adopt 2FA. 2FA is used as an additional layer of protection for all administrative accounts which have privileged access to critical systems, data, and infrastructure.	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.	**R5** Ensure that the use of 2FA is extended to all remaining staff and on all accounts which access College services in order to protect against password guessing and theft. Where appropriate, and to provide flexibility, offer users a choice of factors to self-authenticate, as no single method will suit everyone (or all environments or devices). These may include SMS or email messages, biometrics, or physical tokens.	College is keen to extend the roll out of 2FA and is in discussion with the Trade Unions to gain support. This is a standing agenda item for the Local Negotiating Committee (LNC) which IT have already presented to. Since this meeting, the College Data Protection Officer has conducted a Data Privacy Assessment to further re-assure Staff\Trade Unions on the safety of personal data (personal mobile phone number) supplied as part of the 2 FA process to Microsoft. Currently a number of key Support Departments already use 2FA (IT, Finance, SMT & ELT) and all students now have 2FA for Office 365. **To be actioned by:** Director of IT **No later than:** 30 September 2022
			Grade **3**

Objective 1: Review the College's current position with regard to information and cyber security to advise on areas that should be addressed in line with the latest guidance produced by the NCSC. This also included a high-level review of the College's ICT Business Continuity and Disaster Recovery arrangements (Continued).

Data Security
Data needs to be protected from unauthorised access, modification, or deletion. This involves ensuring data is protected in transit, at rest, and at end of life.

Observation	Risk	Recommendation	Management Response
To protect data at rest, users should minimise the amount of information stored on a mobile device to only that which is needed to fulfil the business activity that is being delivered when working outside the normal office environment. If the device supports it, encrypt the data at rest through full disk encryption. Most staff are using College managed devices to connect remotely to the College's systems; however the devices are not protected by full disk encryption. Authentication protocols also allow staff to use personal devices to connect to College networked services and such IT do not have visibility, or control, of the security configurations of those devices. Mobile device management software is deployed which can identify and remotely wipe College managed devices in the event of loss or theft, however the same process cannot be applied to staff personal devices. The College is currently piloting the use of Microsoft's Intune cloud service which allows IT to securely manage both College and users' personal devices remotely, as Intune allows users to protect work data by isolating it from personal data. Following successful completion of the pilot, it is anticipated that a further phased roll out of InTune will commence at the start of the 2022/23 academic session.	Data at rest, located on College managed devices, is not adequately protected increasing the risk of a data breach if devices are lost or stolen.	**R6** Full disk encryption should be deployed on all College managed devices to prevent data loss in the event of loss or theft of the devices. Other protections, such as the use of Intune, should be applied to personal devices that are used to access College data and systems.	As described, the IT Team have commenced testing & initial pilot of Microsoft InTune to provide enhanced Mobile Device Management (MDM), of which device encryption is a key aspect. MDM is now vital to the College due to hybrid working and blended learning. On completion of the initial pilot, this will be rolled out across all College mobile devices (both staff & students). **To be actioned by:** Director of IT **No later than:** 30 September 2022
			Grade **3**

Objective 1: Review the College's current position with regard to information and cyber security to advise on areas that should be addressed in line with the latest guidance produced by the NCSC. This also included a high-level review of the College's ICT Business Continuity and Disaster Recovery arrangements (Continued).

Logging and Monitoring
Collecting logs is essential to understand how your systems are being used and is the foundation of security (or protective) monitoring. In the event of a concern or potential security incident, good logging practices will allow you to retrospectively look at what has happened and understand the impact of the incident. Security monitoring takes this further and involves the active analysis of logging information to look for signs of known attacks or unusual system behaviour, enabling organisations to detect events that could be deemed as a security incident, and respond accordingly in order to minimise the impact.

Observation	Risk	Recommendation	Management Response
A lack of visibility of security threats and incidents across the IT infrastructure is recorded as a significant risk on the College's cyber risk register. Although there is a centralised logging solution in place, capability is reduced due to limitations in real time reporting and alerting of security events, threats and suspicious behaviours or processing activities. By way of alternative mitigating controls, we noted that all local systems logs are enabled, as well anti-virus logging enabled on all endpoints. The CISCO umbrella web filtering tool logs and blocks unidentified URLs and the network boundary firewall includes an Intrusion Prevention System. Security Information and Event Management (SIEM) is a software solution that aggregates and analyses activity from many different resources across the entire IT infrastructure. SIEM collects security data from assets such as network devices, servers, and domain controllers, and stores, normalises, aggregates, and applies analytics to that data to discover trends, detect threats, and allow IT staff to investigate any alerts.	Unusual or malicious network traffic or incoming and outgoing activity that could indicate an attack (or attempted attack) is not identified. An incident may occur that requires investigation, and the college is unable to complete this efficiently or effectively.	**R7** Upgrades to the current centralised logging solution, or alternative tools such as a SIEM, should be explored which provide improved monitoring of network traffic for unusual or malicious incoming and outgoing activity, or critical system processing activity that could be indicative of an attack or an attempted attack. Alerts generated by the system should be promptly managed by the IT team.	The IT Team introduced a basic level of SIEM 12 months ago to address the threat of internal network security. Further discussions have been taken place with potential Technology Partners (including JISC) to upgrade the SIEM capability within the College however due to the size of the College, the costs have been prohibitive. An options paper will be brought to SMT\ELT with full costings to potentially upgrade the current SIEM capability within the College if agreed. **To be actioned by:** Director of IT **No later than:** 31 March 2022
			Grade **3**

Objective 1: Review the College's current position with regard to information and cyber security to advise on areas that should be addressed in line with the latest guidance produced by the NCSC. This also included a high-level review of the College's ICT Business Continuity and Disaster Recovery arrangements (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.

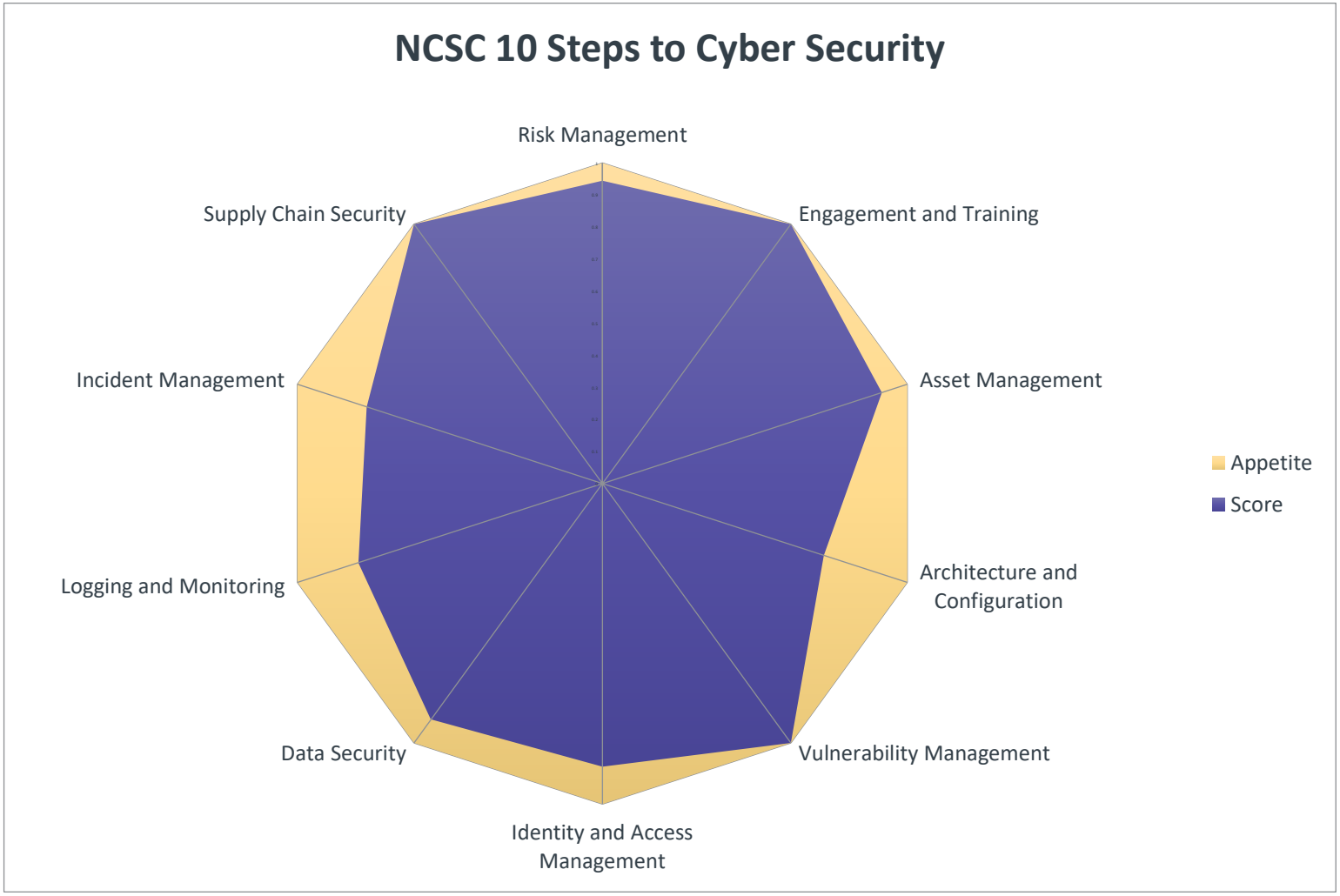
To reduce the impact of compromise of network and systems security, it is good practice to plan for backup and recovery. Plans should include data and services, such as relevant configurations and accounts, and that you have tested your plans so that you are able to respond effectively in the event of 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.

We noted that backup solutions are in place, including backups taken daily and weekly, backups are protected through encryption and are not directly accessible on the main network, back-ups are protected from being over-written, and multiple copies are retained across several sites. Whilst back-ups have been partially tested in the past, through ad-hoc requests for recovery of files, and restore of tape back-ups, a full system and data restore of SAN (storage area network) back-ups 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).

Business Continuity and Disaster Recovery Plans are in place. A scenario-based ICT disaster recovery testing exercise is planned for later in 2021 which is expected to include a full restore or SAN snap-shot back-ups to provide assurance that recovery of data from the SAN works to minimise the disruption to College operations.

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