



# Glasgow Kelvin College

## Internal Audit 2025-26

Cyber Security

April 2026

### Overall Conclusion

Strong

Item 07c

# Table of contents

Section	Page
1 EXECUTIVE SUMMARY .....	2
2 BENCHMARKING.....	16
3 DETAILED RECOMMENDATIONS.....	17
4 AUDIT ARRANGEMENTS.....	20
5 KEY PERSONNEL.....	21
<b>Appendix</b>	<b>Page</b>
A GRADING STRUCTURE .....	23
B ASSIGNMENT PLAN.....	25

The matters raised in this report came to our attention during the course of our audit and are not necessarily a comprehensive statement of all weaknesses that exist or all improvements that might be made.

This report has been prepared solely for Glasgow Kelvin College's individual use and should not be quoted in whole or in part without prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any third party.

We emphasise that the responsibility for a sound system of internal control rests with management and work performed by internal audit should not be relied upon to identify all system weaknesses that may exist. Neither should internal audit be relied upon to identify all circumstances of fraud or irregularity should there be any although our audit procedures are designed so that any material irregularity has a reasonable probability of discovery. Every sound system of control may not be proof against collusive fraud. Internal audit procedures are designed to focus on areas that are considered to be of greatest risk and significance.

## Overview

### Purpose of review

We undertook a review of the cyber security arrangements in place at Glasgow Kelvin College (the College) to assess whether there were appropriate controls in place to mitigate the loss of business-critical information due to a cyber-attack or failure of key systems or suppliers.

We tested these arrangements against the National Cyber Security Centre's (NCSC) 10 Steps to Cyber Security guidance.

In line with the Institute of Internal Auditors' (IIA) Topical Requirements on Cyber Security, this work will also contribute to the internal audit function's obligation to assess and provide assurance over cyber risk management, including areas such as governance structures, incident response readiness, and supplier assurance processes.

This review will form part of our 2025/26 Internal Audit Plan.

### Scope of review

Our objectives for this review were to assess whether:

- | There was an appropriate risk-based approach to securing data and systems which had been adopted.
- | There was appropriate cyber-awareness training for College staff that has been mandated.
- | The architecture and configuration of key College systems was easily maintained and updated to adapt effectively to emerging cyber threats.
- | There were appropriate solutions in place to control access to the College's information systems.

# 1 Executive summary

- | The systems were appropriately patched to minimise the risk of vulnerabilities being successfully exploited in an attack.
- | There were appropriate solutions in place to protect College data from unauthorised access, modification, and deletion.
- | There were appropriate processes and procedures in place to respond to security incidents that would help prevent further damage.
- | There were appropriate processes in place for vetting suppliers and assessing the adequacy of their cyber security controls.
- | There was an appropriate understanding of all assets that are part of the College's IT network and environment.
- | The College systems were appropriately monitored with information logged and actively analysed.

Our approach to this assignment took the form of discussion with relevant staff, review of documentation and where appropriate sample testing.

## **Limitation of scope**

There was no limitation of scope.

# 1 Executive summary

## Background Information

### The IT Team

The College IT systems are supported by an inhouse IT Team. The IT Team are responsible for ensuring hardware is configured for staff and students and that software is kept up to date. They maintain and manage the local network and ensure all relevant devices are protected by appropriate anti-virus/anti-malware solutions. The IT Team ensures that firewall protection is appropriately monitored should there be an attempted security breach or failure.

### Entry and Exit Process

The College has appropriate entry and exit procedures to systems for new starts and leavers. The IT Team ensure that as staff join the College, they receive the correct permissions and gain access to the relevant services and software applications. If a member of staff is leaving the College, the IT Team will deprovision network access on their last day of employment. Related licences can then be cancelled for that staff member, with the information logged and set as completed.

### HEFESTIS

HEFESTIS is a 'not for profit' shared services organisation, jointly owned by universities and colleges, that provides cyber security, data protection, and information management expertise to institutions across the UK Further and Higher Education sector. It was established to provide cost effective access to specialist capability and operates as a trusted partner, supporting institutions in responding to an increasingly complex cyber threat and regulatory landscape, while recognising the resource constraints common within the education sector.

The College benefits from its partnership with HEFESTIS through ongoing access to specialist cyber security advice, sector intelligence, and external perspective. In addition, HEFESTIS provides the College with access to a Regional Chief Information Security Officer (CISO) for one day per month, who acts in an advisory capacity, supporting areas such as cyber risk management, strategic security planning, incident preparedness, and alignment with sector good practice. This arrangement enhances the College's cyber governance by introducing senior-level security oversight and insight, while retaining clear accountability within the College for the ownership and operation of cyber security controls.

# 1 Executive summary

## Cyber Essentials Plus

The College has demonstrated a strong and commendable commitment to cyber security, most notably through its successful attainment of the Cyber Essentials Plus (CE+) accreditation. Unlike the baseline Cyber Essentials certification, which is largely self-assessed, CE+ involves a rigorous external assessment of technical controls, requiring a far more robust and demonstrable approach to cyber risk management. Achieving CE+ is a significant step up, reflecting not only considerable effort and financial investment, but also the maturity and effectiveness of the College's technical defences. The controls in place are both well-designed and effectively implemented, signalling a security posture that is proactive, resilient, and aligned with best practice.

## Cyber Assessment Framework (CAF)

In addition to achieving Cyber Essentials Plus accreditation, the College has proactively chosen to align its cyber security arrangements with the National Cyber Security Centre's Cyber Assessment Framework (CAF). The CAF is a UK Government framework designed to help organisations understand how well they are managing cyber risk across key areas such as governance, protection, detection, and incident response. Unlike technical certifications that focus on specific controls, the CAF takes a broader, outcomes-based view, helping organisations assess whether their overall approach to cyber security is effective, proportionate, and resilient.

The College is not required to adopt the CAF, and its decision to do so represents a strong commitment to good governance and continuous improvement. By aligning to the CAF, the College is demonstrating maturity in its approach to cyber risk management, moving beyond compliance and towards a more strategic understanding of cyber resilience. This provides additional assurance to the Senior Leadership Team and Board of Management that cyber security risks are being actively identified, managed, and reviewed in line with nationally recognised best practice.

## Security Information and Event Management

The College has strengthened its cyber security posture by investing in Jisc's Security Information and Event Management (SIEM) service, which includes the Cyber Security Threat Monitoring (CSTM) capability. This proactive approach enables real-time monitoring and early detection of potential threats, helping to safeguard critical systems and data. By leveraging expert analysis and automated alerts, the College significantly reduces risk and enhances confidence in the security of its digital environment.

# 1 Executive summary

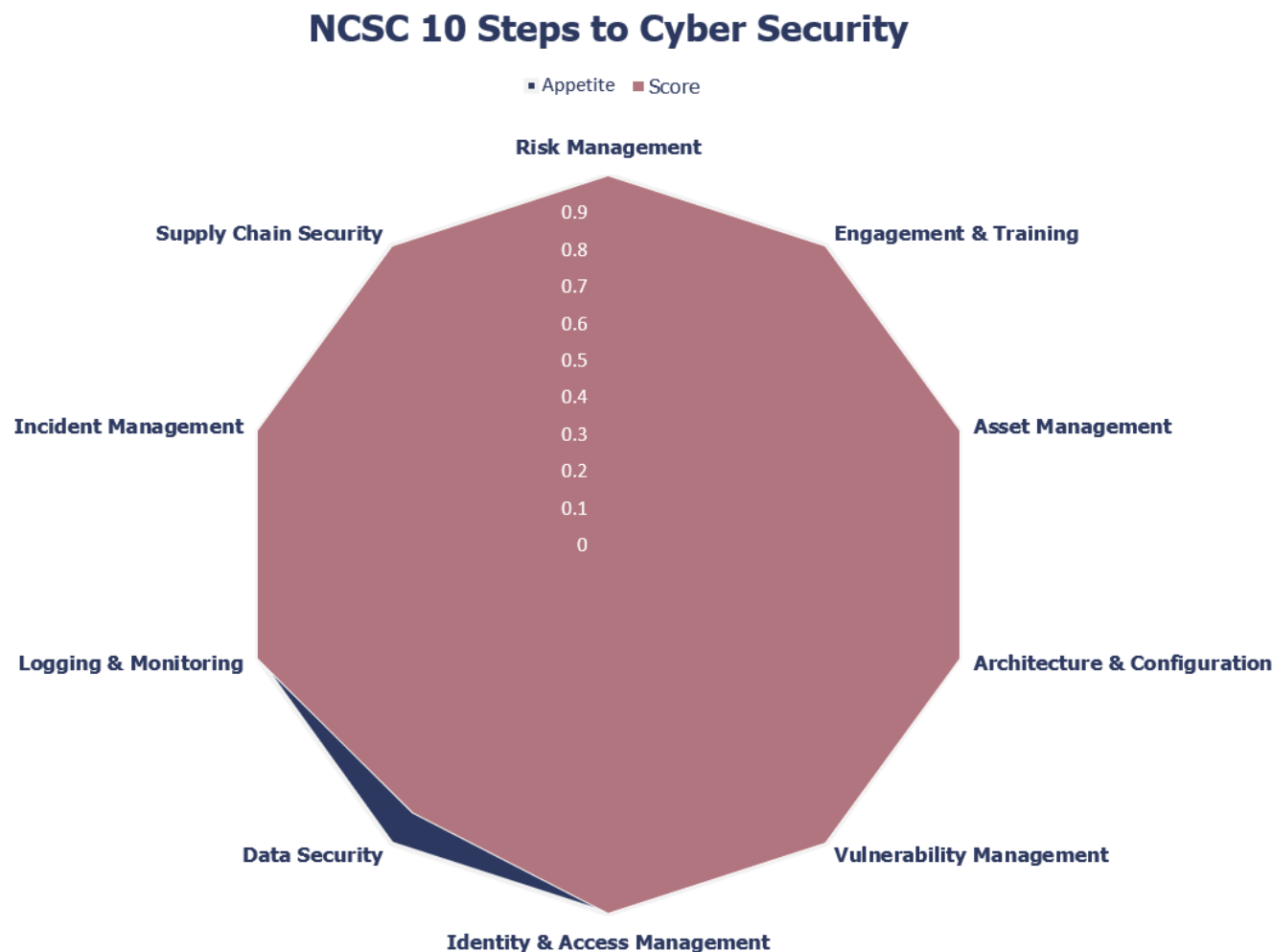
## National Cyber Security Centre 10 Steps to Cyber Security

The National Cyber Security Centre (NCSC) is an organisation of the United Kingdom Government that provides advice and support for the public and private sector on how to avoid computer security threats. The NCSC's 10 steps to Cyber Security guidance aims to help organisations manage their cyber security risks by breaking down the tasks 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 on an organisation when incidents do occur.

The table below illustrates the College's current position in relation to the NCSC's 10 Steps to Cyber Security guidance. We have set the maximum appetite for success at 1. The closer the score is to that maximum, the stronger the performance in that area. Each of the 10 steps have been scored based on our assessment:

NCSC 10 Steps	Appetite	Score
Risk Management	1	1
Engagement & Training	1	1
Asset Management	1	1
Architecture & Configuration	1	1
Vulnerability Management	1	1
Identity & Access Management	1	1
Data Security	1	0.9
Logging & Monitoring	1	1
Incident Management	1	1
Supply Chain Security	1	1

# 1 Executive summary



We have raised 1 recommendation that would help to improve scores in a number of these areas. **Please see Section 3: Detailed Recommendations for further information.**



# 1 Executive summary

## Work Undertaken

Our work for this review included the following:

### **Objective 1: There is an appropriate risk-based approach to securing data and systems which has been adopted.**

- | We reviewed the Risk Register and the formal documentation of operational risks, including cybersecurity risks, to assess whether potential threats are identified, assessed, and managed effectively.

### **Objective 2: There is appropriate cyber-awareness training for College staff that has been mandated.**

- | We reviewed the College's new start cyber security training programmes to assess whether these are mandated and completed by all staff.
- | We reviewed the College's cyber security refresher training programme to assess whether these are mandated and completed by all staff on a frequent basis.

### **Objective 3: The architecture and configuration of key College systems is easily maintained and updated to adapt effectively to emerging cyber threats.**

- | We discussed the current network setup arrangements with the College's IT & Digital Learning Team to assess whether the IT infrastructure was robust and capable of supporting its operations securely and efficiently.
- | We reviewed the College's network security procedures, including any change management processes to assess whether these were appropriately logged and recorded.

### **Objective 4: There are appropriate solutions in place to control access to the College's information systems.**

- | We reviewed the College's controls for user creation and user permissions to assess whether proper access management practices are in place, safeguarding sensitive data and maintaining system integrity.
- | A review of the College's process for evaluating user accounts which compares users with data held by HR.
- | We reviewed the physical and environmental controls in place at the College to assess whether they are effectively safeguarding the critical network infrastructure against potential threats and vulnerabilities.
- | We reviewed the College's controls surrounding users accessing the network remotely, including the enforcement of Multi-Factor Authentication (MFA).

# 1 Executive summary

## **Objective 5: There are appropriate solutions in place to protect College data from unauthorised access, modification, and deletion.**

- | We reviewed the College's controls to safeguard sensitive data to assess compliance with data protection regulations and to mitigate the risk of data breaches.
- | We reviewed the College's backup and replication procedures to assess data integrity, availability, and resilience against data loss or system failures.

## **Objective 6: The College systems are appropriately patched to minimise the risk of vulnerabilities being successfully exploited in an attack.**

- | We reviewed the College's patching procedures and assessed the validity of the process to assess whether these are robust and in line with good practice.
- | We reviewed the College's patching levels and endpoint operating systems to assess whether the platforms are suitably protected and supported, minimising vulnerabilities and enhancing overall security posture.

## **Objective 7: There are appropriate processes and procedures in place to respond to security incidents that will help prevent further damage.**

- | We reviewed the College's Cyber Incident Response Plan for adequacy to assess whether it effectively prepares the College to respond promptly and efficiently to cyber threats, minimising potential damage and disruption.
- | We held discussions with the College to establish whether the plan had been exercised and if relevant staff are aware of their roles and responsibilities.

## **Objective 8: There are appropriate processes in place for vetting suppliers and assessing the adequacy of their cyber security controls.**

- | We held discussions with the College to establish the current arrangements in place.
- | We reviewed the College's policies and procedures to assess whether these are robust and in line with best practice.

# 1 Executive summary

## **Objective 9: There is an appropriate understanding of all assets that are part of the College's IT network and environment.**

- | We reviewed the College's Asset Management Register to assess accurate tracking and protection of assets, and to verify proper allocation and utilisation of resources.
- | We reviewed the controls in place that prevent unauthorised devices connecting to the network.

## **Objective 10: The College systems are appropriately monitored with information logged and actively analysed.**

- | We reviewed of the College's network security appliances to assess whether they are effectively protecting the network from threats and vulnerabilities.
- | We reviewed of the College's network monitoring and logging capabilities to assess timely detection and response to security incidents.

# 1 Executive summary

## Conclusion

### Conclusion

#### Overall Conclusion: Strong

Following our review, we can provide a strong level of assurance over the College's Cyber Security and their associated policies, procedures, and controls. Although we have raised a number of good practice points, we have raised one low grade recommendation for improvement. **Please see Section 3: Detailed Recommendations for further information.**

### Summary of recommendations

#### Grading of recommendations

	High	Medium	Low	Total
Cyber Security	0	0	1	1

As can be seen from the above table there were no recommendations made which we have given a grading of high.

# 1 Executive summary

## Areas of good practice

**The following is a list of areas where the College is operating effectively and following good practice.**

- |    |   |
|----|---|
| 1. | The College has implemented a robust and integrated monitoring and alerting framework. External support through Jisc and the JANET network further enhances the College's security by providing access to national-level threat intelligence and advanced mitigation tools. Additionally, Jisc's SIEM and Cyber Security Threat Monitoring (CSTM) services provide the College with centralised log collection, real-time threat detection, and expert analysis, enabling proactive identification and response to potential security incidents.                            |
| 2. | The College has a detailed IT asset inventory, held by the IT Team. It provides a detailed database of the College's IT Estate, allowing the IT Team to manage those assets and review the register if and when required.   |
| 3. | The College demonstrates a structured approach to managing supplier and third-party risks. The College's vetting process requires relevant partners to hold Cyber Essentials Plus, ISO27001, or an equivalent accreditation. These measures reflect a robust and risk-aware strategy for maintaining supply chain security and compliance.  |
| 4. | The College's Cyber Security Incident Response Plan is a detailed document, outlining how the Cyber Security Incident Response Team would work to eliminate a cyber threat efficiently and effectively. The plan helps clarify roles and responsibilities, and includes the steps required to properly detect, triage, respond to and recover from a directed cyber-attack. The College has enhanced its Cyber Security Incident Response Plan by conducting a tabletop exercise, simulating a cyber incident scenario that could potentially impact on College operations. |

# 1 Executive summary

**The following is a list of areas where the College is operating effectively and following good practice.**

5.	The College demonstrates robust practices in vulnerability management and patching, underpinned by structured processes and independent verification. These measures are strengthened through regular network scans and complemented by annual penetration testing.
6.	Administrator access to network components is carried out over a dedicated and secure network infrastructure, managed by the IT Team. The network architecture incorporates VLAN segmentation to enhance security and is supported by business-grade anti-virus software.
7.	The College demonstrates strong user account management processes, ensuring secure and accountable access control. Structured provisioning through HR, regular audits against HR records, and role-based segregation of administrative accounts reflect a disciplined approach.
8.	Remote access for staff is restricted to the shared services offered by Microsoft 365 and to a number of services requiring VPN access, helping to limit unnecessary exposure of internal systems. All remote connections are secured with Multi-Factor Authentication (MFA), ensuring a strong layer of protection against unauthorised entry.
9.	The College's core network infrastructure is housed inside a secure server room with robust physical and environmental controls protecting the network equipment. It is secured behind locked doors and is protected by temperature controls, smoke alarms, flame suppressing equipment, and has Uninterrupted Power Supply (UPS) hardware attached.

# 1 Executive summary

**The following is a list of areas where the College is operating effectively and following good practice.**

10.	Wireless access is appropriately separated for different users on the network, with unmanaged devices restricted to external resources only i.e., hosted on the Internet. Access to College network resources is secured using domain credentials for both staff and students. Security is again enhanced by security rules set on the College firewalls and internet filtering. Further external protection is provided by the College's Internet Service Provider, Jisc Services Limited.
11.	The College has appropriate controls in place to prevent deliberate or accidental data leakage from their network. Data cannot be transferred onto unmanaged USB storage devices. This is underpinned by effective staff access permissions.
12.	The College has robust IT architecture. Network segmentation is in place to help improve network security. The network is protected from external threats by dedicated firewalls, denying direct connections to untrusted external services and protecting internal IP addresses. Endpoints are protected by an anti-virus solution that will automatically detect and respond to cyber security threats.
13.	The College mandates cyber security training for all staff during onboarding and delivers continuous refresher training. Regular phishing simulations are conducted to assess staff awareness of phishing threats and to reinforce good cyber security practices.
14.	At a corporate level, a risk management regime has been established with a Risk Register. This identifies cyber security as a key risk to the College and is monitored by the Audit & Risk Committee in line with the College's risk management framework. Emerging cyber security risks, along with related controls and mitigations, can be captured within the IT Team's own Digital Services Risk Register.

# 1 Executive summary

**The following is a list of areas where the College is operating effectively and following good practice.**

- |     |   |
|-----|---|
| 15. | The College's ICT policies establish a clear framework that underpins a risk-based approach to IT management, ensuring systems are secure, changes are controlled, and recovery processes are reliable. This is evidenced through regular Disaster Recovery testing, effective Change Management to minimise service impact, and defined security policies that set essential technical safeguards. |
|-----|---|



## 2 Benchmarking

We include for your reference comparative benchmarking data of the number and ranking of recommendations made for audits of a similar nature in the most recently finished internal audit year.

### Cyber Security

Benchmarking				
	High	Medium	Low	Total
Average number of recommendations in similar audits	0	3	1	4
Number of recommendations at Glasgow Kelvin College	0	0	1	1

From the table above it can be seen that the College has a lower number of recommendations compared to those colleges it has been benchmarked against.

### 3 Detailed recommendations

Backup Data Encryption			
Ref.	Finding and Risk	Grade	Recommendation
1.	<p>Data stored on backup systems should be fully protected to ensure that personal, sensitive, or organisational data remains secured against unauthorised access. Industry standards and good practice recommend that organisations implement encryption controls to safeguard backup media in the event of physical compromise.</p> <p>Backup data is encrypted in transit when transferred across the College's network. However, once stored on the backup devices, the data is not encrypted at rest. Physical access controls are in place, and the backup units are kept in a secured location. Access is restricted to authorised ICT and Estates personnel only.</p> <p>This position appears to have arisen due to the current configuration and licensing of the backup solution, which does not include encryption of data at rest as standard. While the existing setup appropriately secures data in</p>	<b>Low</b>	<p>The College should continue to prioritise and expedite the ongoing infrastructure project, including the migration of servers to Azure and the transfer of backup storage to AWS. Once complete, this will provide encryption of backup data at rest, further strengthening the protection of sensitive and personal information and aligning the College's backup environment with industry best practice.</p>

### 3 Detailed recommendations

	<p>transit, the additional controls required to enable encryption at rest have not been implemented, reflecting a combination of licensing considerations and the College's current infrastructure arrangements. Furthermore, with planned changes to the backup environment as part of an ongoing infrastructure project, including the anticipated transition to cloud-based storage, enhancements in this area have not yet been prioritised within the existing on-premise solution.</p> <p>If an unauthorised individual were to bypass physical security controls, they could gain access to unencrypted backup data. This could lead to exposure of the College's sensitive or personal information, resulting in potential data breaches, regulatory non-compliance, and reputational damage.</p>		
--	---	--	--

### 3 Detailed recommendations

Management response	Responsibility and implementation date
<p>Management agrees with the recommendation.</p> <p>The College is progressing a planned cloud migration programme which includes the move of backup services to platforms that provide encryption at rest as standard. This will fully address the risk identified and align backup arrangements with recognised good practice.</p> <p>In the interim, existing physical security and access controls continue to mitigate risk. Implementation will be completed as part of the cloud migration programme.</p>	<p><i>Responsible Officer:</i></p> <p>Michelle Harding, Head of Digital and IT Operations</p> <p><i>Implementation Date:</i></p> <p>1 December 2026</p>

## 4 Audit arrangements

The table below details the actual dates for our fieldwork and the reporting on the audit area under review. The timescales set out below will enable us to present our final report at the next Audit & Risk Committee meeting.

Audit stage	Date
Fieldwork start	30 March 2026
Closing meeting	7 April 2026
Draft report issued	14 April 2026
Receipt of management responses	15 April 2026
Final report issued	15 April 2026
Audit & Risk Committee	12 May 2026
Number of audit days	8

## 5 Key personnel

We detail below our staff who undertook the review together with the College staff we spoke to during our review.

Wbg			
Partner	Graham Gillespie	Partner and Head of Internal Audit	gg@wbg.co.uk
Director	Stephen Pringle	Director of Internal Audit	sp@wbg.co.uk
Senior Manager	Scott McCready	Senior Internal Audit Manager	smc@wbg.co.uk
Auditor	Kevin McDermott	Senior IT Auditor	kmd@wbg.co.uk

Glasgow Kelvin College			
Key Contacts	Jason Quinn	Assistant Principal: Digital and Information Services	jquinn@glasgowkelvin.ac.uk
	Michelle Harding	Head of Digital and IT Operations	mharding@glasgowkelvin.ac.uk
Wbg appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and co-operation.			



# A Grading structure

For each area of review, we assign a level of assurance in accordance with the following classification:

Assurance Classification	
Strong	Controls satisfactory, no major weaknesses found, no or only minor recommendations identified.
Substantial	Controls largely satisfactory although some weaknesses identified, recommendations for improvement made.
Weak	Controls unsatisfactory and major systems weaknesses identified that require to be addressed immediately.
No	No or very limited controls in place leaving the system open to significant error or abuse, recommendations made require to be implemented immediately.



# A Grading structure

For each recommendation, we assign a grading either as High, Medium, or Low priority depending on the degree of risk assessed as outlined below:

Grading	Classification
High	Major weakness that we consider needs to be brought to the attention of the Audit & Risk Committee and addressed by Senior Management of the College as a matter of urgency.
Medium	Significant issue or weakness which should be addressed by the College as soon as possible.
Low	Minor issue or weakness reported where management may wish to consider our recommendation.

## Purpose of review

We will undertake a review of the cyber security arrangements in place at Glasgow Kelvin College (the College) to assess whether there are appropriate controls in place to mitigate the loss of business-critical information due to a cyber-attack or failure of key systems or suppliers.

We will test these arrangements against the National Cyber Security Centre's (NCSC) 10 Steps to Cyber Security guidance.

In line with the Institute of Internal Auditors' (IIA) Topical Requirements on Cybersecurity, this work will also contribute to the internal audit function's obligation to assess and provide assurance over cyber risk management, including areas such as governance structures, incident response readiness, and supplier assurance processes.

This review will form part of our 2025/26 Internal Audit Plan.

## Scope of review

Our objectives for this review are to assess whether:

- | There is an appropriate risk-based approach to securing data and systems which has been adopted.
- | There is appropriate cyber-awareness training for College staff that has been mandated.
- | The architecture and configuration of key College systems is easily maintained and updated to adapt effectively to emerging cyber threats.
- | There are appropriate solutions in place to control access to the College's information systems.
- | There are appropriate solutions in place to protect College data from unauthorised access, modification, and deletion.

## B Assignment plan

- | The College systems are appropriately patched to minimise the risk of vulnerabilities being successfully exploited in an attack.
- | There are appropriate processes and procedures in place to respond to security incidents that will help prevent further damage.
- | There are appropriate processes in place for vetting suppliers and assessing the adequacy of their cyber security controls.
- | There is an appropriate understanding of all assets that are part of the College's IT network and environment.
- | The College systems are appropriately monitored with information logged and actively analysed.

Our approach to this assignment took the form of discussion with relevant staff, review of documentation and where appropriate sample testing.

### Limitation of scope

There is no limitation of scope.

## Audit approach

Our approach to the review will be:

- | Discussion with relevant staff involved to establish the current arrangements in place.
- | Review of IT security, access control and user policies for adequacy.
- | Review of the College's strategy for identifying and addressing system vulnerabilities in a secure and timely manner.
- | Review of the College's anti-malware/virus software including web protection.
- | Review of the College's network security appliances and monitoring.
- | Review of the College's data leakage prevention controls and monitoring.
- | Review of the College's network access controls including user account controls, remote access, third party access.
- | Discussion with staff involved to establish the current arrangements in place at the College for Backup and Disaster Recovery.
- | Review of the College's cyber awareness training for staff.
- | Review the College's vetting processes for suppliers in relation to their cyber awareness.
- | Review of the College's IT asset management.

## Potential key risks

The potential key risks associated with the area under review are:

- | There is no risk-based approach to securing data and systems.
- | Appropriate cyber-awareness training for staff has not been mandated.
- | The architecture and configuration of key IT systems are not easily maintained and updated, meaning they cannot adapt effectively to emerging cyber threats.
- | There is a lack of/inadequate controls in place to control access to the College's information systems.
- | The College's network is not protected from misuse, which would include unauthorised access, modification, and deletion.
- | If systems of defence for College IT systems are not robust and effective, then the College could be subject to system failure and loss.
- | There are insufficient processes and procedures in place to respond to security incidents to help prevent further damage.
- | There are no processes in place for vetting suppliers and assessing the adequacy of their cyber security controls.
- | There is a lack of understanding around the assets that form part of the College's IT network and environment.
- | The College systems are not monitored meaning relevant information remains unknown and will not be acted upon.