

Glasgow Kelvin College

Cyber Security

Internal Audit report No: 2023/03

Draft issued: 3 February 2023

Final issued: 6 February 2023



Contents

	Page
Section 1	Management Summary
	• Overall Level of Assurance 1 • Risk Assessment 1 • Background 1 • Scope, Objectives and Overall Findings 2 • Audit Approach 2 • Summary of Main Findings 3 • Acknowledgements 3
Section 2	Main Findings and Action Plan 4 - 7
Appendix I	NCSC 10 Steps to Cyber Security 8
Appendix II	Updated Action Plan - Internal Audit Report 2021/05 – IT Network Arrangements 9 - 10

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 & Risk 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

Good	System meets control objectives.
-------------	----------------------------------

Risk Assessment

This review focused on the controls in place to mitigate the following risks on the Glasgow Kelvin College ('the College') Strategic Risk Register:

- Risk number 11 – A widespread cyber-attack breaches college defence (risk rating: high).

Background

As part of the Internal Audit programme at the College for 2022/23 we carried out a review of the organisation's 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 management and the Audit & Risk 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 College services to students and external stakeholders and is also vital to the effective internal operation of the organisation. 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 therefore 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

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 National Cyber Security Centre (NCSC), the UK Government's national technical authority for information assurance.

The table below notes each separate 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 ICT department and users is in line with the NCSC 10 Steps to Cyber Security guidance.	Good	0	0	4
Overall Level of Assurance	Good	0	0	4
		System meets control objectives.		

Audit Approach

Our approach was based upon the guidance and best practice provided by NCSC; discussion with the Director of Digital Services and members of the ICT Team, supplemented by review of information provided by members of the IT Team and policies and procedures; and observation. This 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.

We specifically considered the way in which risks associated with cyber security, and the associated impact on delivery of College business, are being managed.

Summary of Main Findings

Strengths

Throughout our review we observed examples of good practice, and we welcomed the willingness of staff to assist our review and to seek ways to improve security within the organisation. We have concluded that, overall, the College exhibits a strong awareness of 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 information / cyber security as key strategic risks, and there are structures in place which act as appropriate bodies for evaluating and monitoring information security risks within the College.
- regular security reviews are conducted of the College ICT environment which includes vulnerability scans of the firewall and internal network to identify vulnerabilities and exploits.
- a baseline security build for workstations, servers, firewalls, and routers is in place.
- hardware and software inventories have been created.
- processes are in place for applying updates and patches to all devices connected to the network.
- the ICT architecture protects the network through use of firewalls and segregation prevents direct connections to untrusted external services and protects internal IP addresses.
- management of user accounts is linked to the organisation'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.
- network hardware/endpoints are protected by an antivirus solution, which automatically scans for malware.
- good practice controls in user authentication are being maintained which support remote working for users whilst maintaining the security of the ICT infrastructure.
- The College subscribes to HE/FE Shared Technology & Information Services (HEFESTIS) which provides the College with access to information security expertise and advice and guidance on the latest cyber threats and development of policies and procedures.

Opportunities for Improvement

Using the latest guidance available from the NCSC we identified opportunities where controls could be strengthened, which are discussed with the main text of this report. Implementation of the recommendations raised in this report will reduce the organisation's current risk position and will enhance the organisation's ability to manage cyber 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.

Follow-up of Previous Audits

An internal audit review of the College's cyber security control environment was last undertaken in 2020/21. The overall assurance reported in internal audit report *2021/05 IT Network Arrangements*, issued in June 2021, was graded as 'Good'. The report included three recommendations which were subject to follow-up by internal audit in 2021/22, as reported in internal audit report *2022/08 Follow-up*, issued in August 2022. The report identified that one recommendation had been fully implemented, and the remaining two recommendations were assessed as partially implemented and these have been followed-up as part of this report at Appendix II.

Acknowledgments

We would like to take this opportunity to thank the staff 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 ICT department and users is in line with the NCSC 10 Steps to Cyber Security guidance.

Engagement 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 organisation.

Observation	Risk	Recommendation	Management Response
Our review noted that mandatory e-learning cyber security training is in place for all staff, and which forms part of the new staff induction process. To maintain user awareness of the cyber risks faced by the College, without exception, all users should receive regular refresher training on the cyber risks to the organisation and to them as employees or students, and as individuals. Whilst we noted that regular cyber awareness guidance and updates are issued to staff in response to cyber threats identified by ICT staff, e.g., increased occurrences of phishing emails reported, there is no formal programme of refresher training for staff users.	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; and - external attacks due to email phishing and social engineering.	R1 Ensure that a formal programme of refresher training is established for staff users with a risk-based approach adopted in identifying the frequency of refresher training requirements.	Agreed. Our current cyber security training module is available for all staff but is not required to be repeated periodically. This will be reviewed. Training workshops will be considered along with simulated cyber-attack exercises and follow-up training, to ensure staff have every opportunity to refresh their knowledge. To be actioned by: Director of Digital Services No later than: 31 July 2023
			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 ICT department and users is in line with the NCSC 10 Steps to Cyber Security guidance (Continued).

Observation	Risk	Recommendation	Management Response
Engagement and Training (Continued) We reviewed the training compliance data for staff users and noted that at the time of our audit, 71% of staff had completed the training. Whilst a compliance rate of 100% may be difficult to achieve, due to new staff onboarding and completion of induction training as well as staff absences and annual leave, a compliance rate of 90+% should be achievable. Reasons for not achieving a higher rate of compliance may include staff that do not require regular access to computer systems, e.g. janitorial or cleaning staff. However, all staff that do have access to College systems, albeit limited access, represent a potential vulnerability and it is therefore important that all staff complete the training.	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; and • external attacks due to email phishing and social engineering.	R2 Ensure that departmental compliance rates for completion of the cyber security training are communicated to departmental line managers and instances of non-compliance are followed up. Potential barriers to completion of the training should be investigated and remediated.	Agreed. An initial drive to increase the cyber security training completion rate will be undertaken. Thereafter, ongoing monitoring of compliance will be linked in with recommendation R1 of this report, to ensure departments are aware of non-compliance. To be actioned by: Director of Digital Services No later than: 31 July 2023
			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 ICT department and users is in line with the NCSC 10 Steps to Cyber Security guidance (Continued).

Data Security / Incident Management

Incidents can have a huge impact on the College 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 any lessons learned in the aftermath of an incident will mean the College is better prepared for any future incidents.

Observation	Risks	Recommendation	Management Response		
The College Business Continuity Plan (BCP) contains several scenarios for the most likely types of incidents which could occur, including those which could affect the College’s ICT infrastructure. The BCP contains detailed guidance on the key stages in the management of relevant scenarios, including, data / ICT systems loss; cybercrime; and data breach. The guidance is supported by a Business Impact Analysis (BIA) which is designed to enable the prioritisation of recovery activities. A more specific approach to recovery from a loss of ICT services or data from a cyber-attack is contained with the College’s Incident Response Procedure, which is supported by a range of playbooks which detail the College’s response protocols for specific types of threats such as malware, data breaches, user account compromise, denial of service attacks, ransomware and phishing. At the time of our audit, the Incident Response Procedure had yet to be formally tested. Whilst recovery of files is undertaken regularly, there has been no full restore of back-ups. The College back-up strategy includes a server back-up plus a cloud copy. The back-up solution provides reports confirming back-ups were taken successfully, however a full server based recovery has not been performed to provide assurance that back-ups are readable. It is good practice to perform back-up recovery tests at annually and should form part of regular incident management / disaster recovery tests.	Ineffective incident management can increase the impact of a cyber incident. An unpractised plan results in poor decisions being made under the pressure of a real incident.	R3 A Cyber Incident Response Procedure should be communicated to all relevant staff and stakeholders to ensure that everyone’s roles and responsibilities are defined and understood. This should then be supported through appropriate training. The response procedure should then be practised to ensure staff know how to respond during a cyber security incident, and to also highlight any potential weaknesses or gaps in the planned response. Practises should also include restoring systems and files from backups to ensure that recovery times and recovery points can be achieved.	Agreed. A simulated large scale cyber incident exercise will be challenging and will affect day-to-day operations. However, a plan for both paper-based practice and live scenarios will be prepared on a sufficient scale to test our incident response, including data recovery from backup systems. To be actioned by: Director of Digital Services No later than: 31 July 2024		
			<table><tr><td>Grade</td><td>3</td></tr></table>	Grade	3
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 ICT department and users is in line with the NCSC 10 Steps to Cyber Security guidance (Continued).

Supply Chain Security

Most organisations rely upon suppliers to deliver products, systems, and services. An attack on your suppliers can be just as damaging to you as one that directly targets your own organisation. Supply chains are often large and complex, and effectively securing the supply chain can be hard because vulnerabilities can be inherent, introduced or exploited at any point within it. The first step is to understand your supply chain, including commodity suppliers such cloud service providers and those suppliers you hold a bespoke contract with. Exercising influence where you can, and encouraging continuous improvement, will help improve security across your supply chain.

Observation	Risk	Recommendation	Management Response	
Processes are in place for vetting suppliers and assessing the adequacy of their cyber security controls as part of procurement procedures. However, we noted that current procurement procedures do not include a mandatory requirement for suppliers to provide copies of current certifications they might hold that could demonstrate how they meet the minimum-security requirements for the College. Additionally, there is no requirement for suppliers to submit evidence of recertifications when these are due, which is normally annually.	Suppliers' cyber security arrangements do not meet the minimum standard required by the College. Weaknesses in supplier security are exploited resulting in a cyber security incident impacting the College systems and data.	R4 Establish mandatory requirements within procurement procedures for relevant suppliers to provide evidence of current cyber security certifications. Also ensure that relevant suppliers provide copies of recertifications when these are due.	Agreed. Director of Digital Services to work with Procurement Manager to establish best method of including cyber security arrangements within the procurement procedures. To be actioned by: Director of Digital Services / Procurement Manager No later than: 31 January 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.



Appendix II - Updated Action Plan

Internal Audit Report 2021/05 – IT Network Arrangements

Original Recommendation	Priority	Management Response	Agreed	To Be Actioned By	No Later Than	Progress at August 2022	Progress at February 2023
R2 Mechanisms, such as the use of ethical phishing campaigns, should be established to test the effectiveness of the range of security training provided to staff. The areas of the organisation that regularly feature in security incident reports or achieve the lowest feedback from information security questionnaires or training modules, should be the focus for further support and tailored training.	3	The College accepts this recommendation and will seek to implement methods to evaluate the effectiveness of the User Education & Awareness program.	Yes	Director of Digital Services	31 March 2022	Cyber Security training is now a mandatory feature of staff training and is provided, and monitored, through the WorkRite system. A recent table-top exercise has been undertaken by the ICT team, which focused on the College's response to a phishing attack. Two staff from ICT services are currently undertaking a course relating to cyber-penetration testing, view a view to utilising the skills to implement a programme of simulated cyber-attacks. Revised completion date: 31 January 2023 <i>Partially Implemented</i>	Ethical phishing solution identified, and campaigns planned for February 2023 as part of the College's 'Digital Month' awareness campaign. Further ethical phishing tests will be conducted later in the year. Revised completion date: 28 February 2023 <i>Partially Implemented</i>



Original Recommendation	Priority	Management Response	Agreed	To Be Actioned By	No Later Than	Progress at August 2022	Progress at February 2023
R3 Tools such as network IDS / IPS of SIEM should be placed on the network and configured to monitor traffic for unusual or malicious incoming and outgoing activity that could be indicative of an attack or an attempted attack. Alerts generated by the system should be promptly managed by the Digital Services team.	3	The College acknowledges this recommendation. The College will explore the feasibility of the implementation of SIEM and IDS solutions.	Yes	Director of Digital Services	30 April 2022	The ICT team has implemented a Zero Trust methodology to provide the network with intrusion detection (IDS) and intrusion prevention (IPS). This will mitigate unwanted lateral movement between systems and detection malicious code. Implementation of a full SIEM solution is still being explored to assess the feasibility in relation to cost and benefit. Revised completion date: 31 January 2023 <i>Partially Implemented</i>	Potential SIEM solutions have been identified, and suitability of those solutions was being considered by the ICT team at the time of our audit in January 2023. A solution is expected to be procured and implemented by 31 July 2023. Revised completion date: 31 July 2023 <i>Partially Implemented</i>

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 **F:** 01224 327 911
T: 01382 200 055 **F:** 01382 221 240
T: 0131 226 0200 **F:** 0131 220 3269
T: 0141 471 9870

Henderson Loggie LLP is a limited liability partnership registered in Scotland with registered number SO301630 and is a member of PrimeGlobal, a global association of independent accounting firms, the members of which are separate and independent legal entities. Registered office is: The Vision Building, 20 Greenmarket, Dundee, DD1 4QB. All correspondence signed by an individual is signed for and on behalf of Henderson Loggie LLP. Reference to a 'partner' is to a member of Henderson Loggie LLP. A list of members' names is available for inspection at each of these addresses.

