Audit & Assurance Committee

Date of Meeting	**2 September 2025**
Paper No.	**AAC1-H**
Agenda Item	**5.4.1**
Subject of Paper	**Internal Audit Report – Back Up Process/Digital Business Continuity**
FOISA Status	**Disclosable**
Primary Contact	**David Archibald/Stuart Inglis, Henderson Loggie**
Date of production	**18 June 2025**
Action	**For Discussion**

1. Recommendations

1.1. The Committee is asked to consider and discuss the report and the management responses to the Internal Audit Recommendations.

2. Consultation

2.1. The Lead Auditor has consulted with the Executive Owner, the College Lead, and the Compliance Auditor.

3. Key Insights

3.1. The Internal Audit for Back Up Process/Digital Business Continuity was graded overall as Satisfactory, 'System meets control objectives with some weaknesses present.'

3.2. There are three Priority 3 recommendations arising from the fieldwork, which have management responses.

4. Impact and Implications

4.1. Internal Audit provides an objective insight into the efficiency of operations, evaluation of risks, and organisational controls.

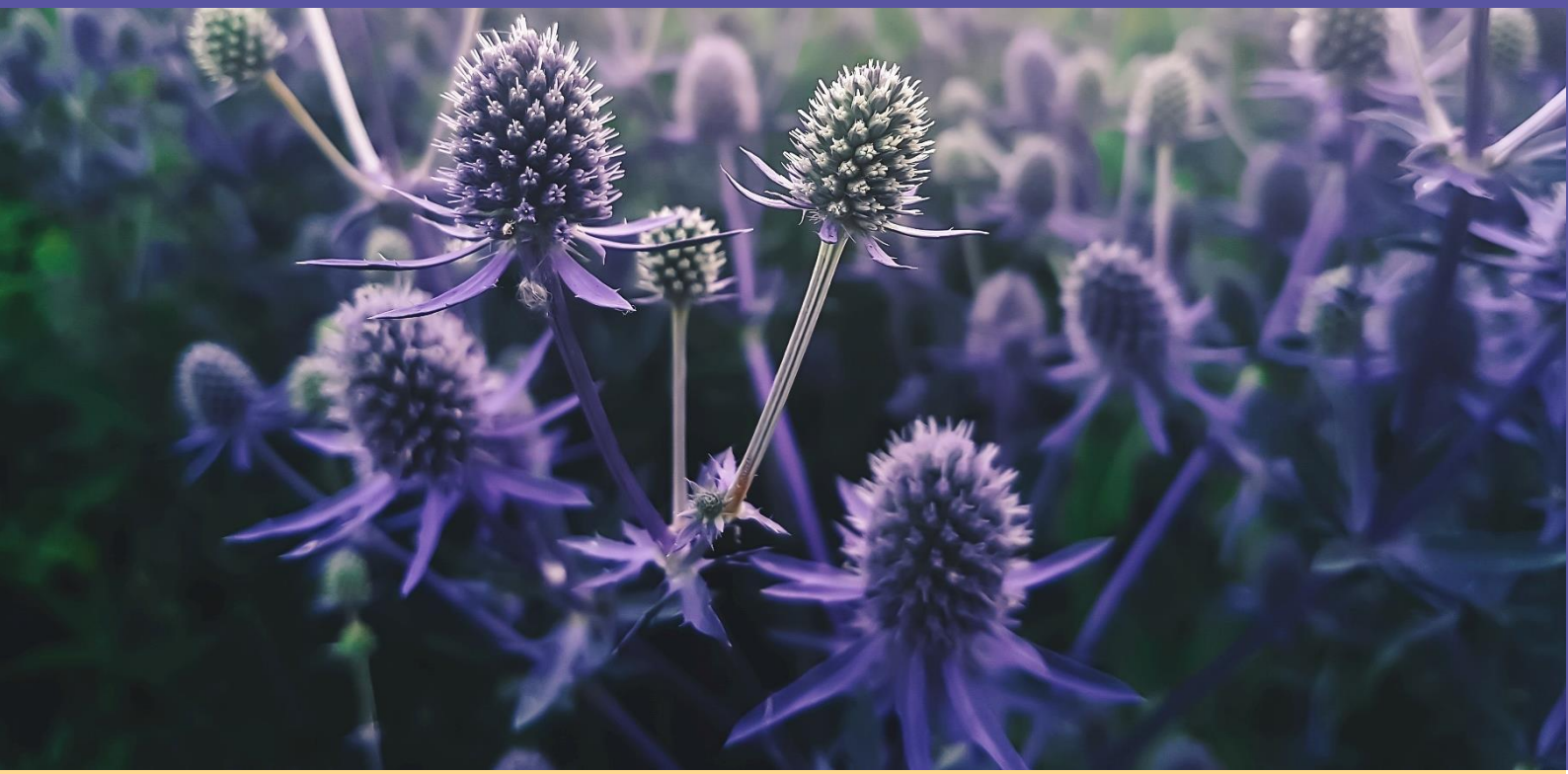
Appendix 1: Internal Audit Report – Back Up Process/Digital Business Continuity

LEVEL OF ASSURANCE
Satisfactory

City of Glasgow College

Back Up Process / Digital Business Continuity

Internal Audit report No:	**2025/07**
Draft issued:	**21 May 2025**
Final issued:	**18 June 2025**



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') Risk Register (as at November 2024):

- **SR14** - Failure of compliance with the General Data Protection Regulations (GDPR) (Net Score 8, amber);
- **SR16** - Failure of business continuity (Net Score 8, amber); and
- **SR28** – Failure to manage strategic, physical and digital assets and infrastructure effectively (Net Score 12, amber)

Background

As part of the Internal Audit programme at the College for 2024/25, we carried out a review of the College's ICT back-up and digital continuity processes. The Annual Plan, agreed with management and the Audit and Assurance Committee on 27 November 2024, identified this as an area where risk can arise and where Internal Audit can assist in providing assurances to management and the Audit and Assurance Committee that the related control environment is operating effectively, ensuring risk is maintained at an acceptable level.

The College's digital backup processes represent the safety net against data loss, cyber threats, and unexpected disasters. Without a strong backup system, critical information – such as student records, research data, financial records, and academic resources - could be compromised, leading to operational disruption and reputational damage.

Digital business continuity refers to an organisation's ability to maintain essential digital operations and recover quickly from disruptions, such as cyberattacks, system failures, or natural disasters. It ensures that critical digital assets - like databases, applications, and online services - remain available and functional, even when unexpected events occur.

Digital continuity is the ability to use your information in the way you need, for as long as you need. Managing digital continuity protects the information you need to do business. This enables you to operate accountably, legally, effectively and efficiently. It helps you to protect your reputation, make informed decisions, avoid and reduce costs, and deliver better public services. If you lose information because you have not managed your digital continuity properly, the consequences can be as serious as those of any other information loss.

The backup process is a crucial component of digital continuity because it ensures that important data remains accessible and usable even in the event of disruptions, such as system failures, cyberattacks, or accidental deletions. Regular backups create copies of data, allowing organisations to recover from unexpected events and continue operations without significant loss or downtime.

Scope, Objectives and Overall Findings

This audit focused on evaluating the effectiveness and efficiency of the College's digital back-up processes and relevant aspects of business continuity plans.

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

Objective	Findings			
The specific objectives of the audit were to gain reasonable assurance that:		1	2	3
		No. of Agreed Actions		
1. Current digital back-up and business continuity processes have been documented and assessed by the College to identify potential gaps and weaknesses, and remedial action taken as required.	**Satisfactory**	-	-	1
2. Back-up processes are robust and capable of protecting all digital systems and critical information assets.	**Satisfactory***	-	-	-
3. Back-up and recovery processes are regularly tested and validated to guarantee their effectiveness.	**Satisfactory**	-	-	2
4. The resources (personnel, technology, and budget) allocated to back-up and business continuity efforts are optimally utilised.	**Good**	-	-	-
Overall Level of Assurance	**Satisfactory**	**-**	**-**	**3**
		System meets control objectives with some weaknesses present.		

*Grading is linked to findings and recommendations covered under objective 3

Audit Approach

Through discussions with the Director of IT, and other IT staff and core business system owners, we established the digital back-up and system business continuity plans which are currently in place. These were then evaluated to establish the extent to which they follow recognised good practice. We also considered how the College obtains assurance that digital back-up and recovery processes are effective and workable.

Summary of Main Findings

Strengths

- The College has a documented overarching Business Recovery Plan (BRP), which is supported by departmental BRPs for key operational areas.
- We compared the back-up requirements, and process prioritisation in the BRPs, with the back-up processes for the centrally managed IT infrastructure and the back-up frequency, retention periods for daily, weekly and monthly back-ups, and recovery capability documented in third-party contracts and agreements. We confirmed that the frequency of back-ups and back-up retentions that are taken in practice – both by the IT team and third parties - are in line with the College's requirements, as described in the BRPs.
- Standardised backup schedules are in place for the infrastructure managed by the College, to reduce data inconsistency risks.
- Back-ups are held separately from live data, encrypted, access restricted to specific members of the College IT team, and protected by multi-factor authentication (MFA).
- The College systems and processes are supported by a multi-layered back-up strategy, incorporating full, incremental, and differential backups to optimise storage and recovery speed. Automated scheduling ensures frequent back-ups, minimising data loss risks.
- Specific members of the IT team responsible for managing the infrastructure have been assigned roles to for overseeing backup processes, cybersecurity, and disaster recovery.

Weaknesses

The College's digital backup and business continuity processes demonstrate a commitment to resilience, although we noted that improvements in obtaining positive assurance that the College's and third-party supplier / vendor back-up and recovery capability is robust, are necessary. Implementing the recommendations outlined in this audit will enhance the institution's capability to protect and recover critical digital assets efficiently.

Acknowledgments

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

Main Findings and Action Plan

Objective 1 – Current digital back-up and business continuity processes have been documented and assessed by the College to identify potential gaps and weaknesses, and remedial action taken as required.

Backup processes are fundamental to digital continuity, ensuring that data remains accessible and intact despite disruptions. They protect against data loss from cyberattacks, hardware failures, or accidental deletions. A well-structured backup strategy allows organisations to recover quickly, minimising downtime and preserving operations. By maintaining multiple copies of back-ups across different locations, the College can safeguard information and ensure seamless transitions across technological changes. Digital continuity relies on back-ups to uphold integrity, security, and reliability, supporting compliance and historical access. Without effective backups, data vulnerabilities could jeopardise continuity, making resilience strategies essential for long-term sustainability and operational stability.

The College has a documented overarching Business Recovery Plan (BRP), which is supported by departmental BRPs for key operational areas, including IT, Estates, People & Culture, Finance (including procurement and Student Records) and Student Experience. A sample of BRPs were reviewed as part of our audit and we noted that these had recently been updated as part of the College's cyclical review process within the last 12 months. The BRPs identify process priorities, key dependencies, including systems, and IT service recovery capability.

- Process Priorities – key processes and the Recovery Time Objective (RTO), i.e. the maximum desired time taken to recover a process to a minimum operating level are identified.
- Resource recovery – identifies the estates, IT device, and other equipment or services that are required to support recovery of data.
- Dependencies – identifies other College departments or external third parties which are required to perform key processes, and how quickly those services are required to restore services.
- IT Service Recovery Capability – identifies the RTO and Maximum Data Loss (MDL), i.e. the maximum amount of IT data (measured in time) which may be lost between the last backup and the point of IT service failure.

As well as considering the processes for managing back-ups and digital continuity for data held on the College's main servers and other parts of the infrastructure, we also considered the key College systems which are not fully managed or supported by the IT team. These included the:

- College VLE – Canvas
- Finance system
- procurement system – PECOS
- HR system
- library catalogue system
- Estates systems, including the door access system
- Student records system
- Student funding system

Objective 1 – Current digital back-up and business continuity processes have been documented and assessed by the College to identify potential gaps and weaknesses, and remedial action taken as required (continued).

We compared the back-up requirements and process prioritisation in the BRPs with the back-up processes for the centrally managed IT infrastructure and the back-up frequency, retention periods for daily, weekly and monthly back-ups, and recovery capability documented in third-party contracts and agreements. We confirmed that the frequency of back-ups and back-up retentions that are taken in practice – both by the IT team and third parties - are in line with the College's RTO and MDL requirements. We also confirmed that the back-up strategy adopted by the IT team accords with good practice, in that it follows a 3-2-1 rule, with three copies of data, stored on two different media types, with one offsite, which is essential for ensuring digital continuity. Back-ups are held for the Active Directory environment on separate domain controllers, emails, firewall configuration and network switch configuration. From the information included in third-party contracts and agreements we also confirmed that suppliers and vendors demonstrated resilience through use of primary and secondary data centres for replicating data processing activity and for disaster recovery capabilities.

Through discussion with members of the IT team, and review of back-up and storage (and back-up and recovery logs), we noted that standardised backup schedules are in place for the infrastructure managed by the College to reduce data inconsistency risks.

Back-ups are held separately from live data, encrypted, access restricted to specific members of the College IT team, and protected by multi-factor authentication (MFA).

Objective 1 – Current digital back-up and business continuity processes have been documented and assessed by the College to identify potential gaps and weaknesses, and remedial action taken as required (continued).

Observation	Risk	Recommendation	Management Response	
Centralised backup policies and procedures, i.e. for the systems and applications, and the infrastructure which supports them, managed by the IT team, are well documented, including details of data storage locations. For decentralised locations, including third-party cloud systems and applications, back-up arrangements including back-up frequencies are contained in contacts and service agreements. however, these are held locally at a departmental level and IT do not have visibility of all third-party agreements. Whilst IT do not own or manage third party systems, particularly cloud applications and services, IT would be expected to support departments with the recovery of those systems and databases, working with vendors and suppliers as documented in the BRPs. We noted that whilst IT have a record of all systems, services and applications which are running on the College IT network, there is no formal record of third-party systems, services and applications which are utilised by College staff that are not accessible from the College network - particularly cloud applications.	The IT team has no knowledge of third-party systems and applications used to process College data, security arrangements for protecting data held on those systems, and how the College manages back-ups.	**R1** A full discovery exercise should be conducted to identify all third-party systems and applications in use across the College. Copies of all contracts and agreements for third-party systems, services and applications, which hold and process College data, should be shared with and retained by the IT team, so that the IT team has complete visibility of third-party systems and databases, and understand their role in supporting the recovery and restore processes.	A full discovery exercise will be completed. A new Policy and / or Procedure will be implemented to clarify the use of third-party systems and applications within the College. **To be actioned by:** Director of IT **No later than:** 31 May 2026	
			Grade	**3**

Objective 2 – Back-up processes are robust and capable of protecting all digital systems and critical information assets.

The College's back-up processes should be designed to be robust and highly capable of safeguarding digital systems and critical information assets. These processes should adhere to industry best practices and regulatory standards, ensuring comprehensive data protection, resilience against cyber threats, and seamless recovery in case of disruptions.

We noted through review of back-up and storage polices, and discussions with IT staff, that the College systems and processes are supported by a multi-layered back-up strategy, incorporating full, incremental, and differential backups to optimise storage and recovery speed. Automated scheduling ensures frequent back-ups, minimising data loss risks. Moreover, back-ups are securely stored across multiple locations, including on-premise servers, encrypted cloud storage, and offline archives, following the 3-2-1 backup rule as noted earlier in this report - three copies, stored on two different media types, with one copy offsite.

To counter cybersecurity threats, such as ransomware attacks, the College implements air-gapped (i.e. off network) and immutable backups, preventing unauthorised modifications. End-to-end encryption ensures that sensitive academic records, financial data, and student information remain protected, both in transit and at rest. Access controls, including restricted admin accounts and MFA, further reinforce security, restricting backup operations to authorised IT staff only.

Objective 3 – Back-up and recovery processes are regularly tested and validated to guarantee their effectiveness.

Observation	Risk	Recommendation	Management Response	
Beyond security, digital continuity is prioritised through rapid recovery mechanisms, including snapshot-based rollbacks and disaster recovery plans that enable the College to restore operations swiftly. Regular recovery of accidently deleted files to an extent validates the backup integrity, ensuring reliability when critical information is needed, however this is limited to files / documents only. A full restore and recovery of systems and data at a server level has not been performed for several years. Industry best practices recommend performing a full restoration at least once a year, but in high-risk and high-user demand environments like education, quarterly or semi-annual testing would be optimal if practicable to do so, and permitted by the available resource and operational requirements. Whilst we recognise that a full restore can be disruptive, if not well planned, it is essential that the College is able to demonstrate that its recovery capability is robust and effective.	Not regularly performing full server restores may result in significant risks that could compromise operations, data integrity, and institutional security, including data corruption and integrity issues; extended downtime; loss of digital continuity; and cyber security vulnerabilities.	**R2** To mitigate the risks associated with not performing regular full server restores, the College should perform full server restores at least once a year, with additional partial recovery tests conducted quarterly.	The IT Team currently perform VMware server restores on a regular basis. An annual exercise with HEFESTIS has been agreed and will be completed in line with the requirements in the IT Network Arrangements / Security Audit. To be tracked through the IT Network Arrangements / Security Audit. **To be actioned by:** N/A **No later than:** N/A **Auditor comment:** Accepted. Action will be tracked through follow-up of recommendation **R3** raised in Internal Audit Report 2024/08, IT Network Arrangements / Security, issued in April 2024.	
			Grade	**3**

Objective 3 – Back-up and recovery processes are regularly tested and validated to guarantee their effectiveness (continued).

Observation	Risk	Recommendation	Management Response	
Supplier / vendor management for third-party systems and applications is the responsibility of the relevant head of department that uses each system, and not the IT team. For key business systems, including the Finance, procurement, HR, and student funding systems, the supplier / vendor is responsible for ensuring that robust data back-up and disaster recovery strategies are provided as part of the service delivery contract / agreement. Whilst we noted that information of data back-up frequency, back-up retention periods, and data centre resilience are included in contracts / agreements, confirmation that the College's data is being backed up in line with the terms of the contracts / agreements is not currently obtained from system suppliers / vendors.	If the College does not actively obtain confirmation from system suppliers / vendors regarding backup frequency, retention periods, and data centre resilience, several critical risks may arise: • unverified compliance – without confirmation, there is no assurance that the suppliers adhere to the agreed backup protocols, potentially leading to non-compliance with regulatory frameworks such as GDPR and Cyber Essentials; • data loss & integrity issues – if backups are not performed as specified, critical College data may not be recoverable after failures or cyber incidents; • extended recovery times – without verification, backup systems may be inadequate, causing prolonged downtime in the event of a disaster, impacting academic and administrative functions; • security vulnerabilities – weak backup retention or inadequate resilience measures could leave the institution exposed to ransomware, malware, and data corruption risks.	**R3** The College should request regular compliance reports and documented confirmations from suppliers / vendors. Where confirmations cannot be obtained for high risk or critical third-party systems, the College should consider commissioning independent audits to verify backup processes.	The College will start to request regular compliance reports and documented confirmation from all new and renewed suppliers / vendors. The tender document will be updated with a clause and a technical section to ensure all new suppliers / vendors understand our expectations and their obligations. A new guidance document will be developed by IT to outline expectations for supplier / vendor data back up and disaster recovery strategies. This will also cover direct awards where no tender document is utilised. A record of all will also be maintained by IT. **To be actioned by:** Director of IT / Associate Director of Procurement **No later than:** 30 December 2025	
			Grade	**3**

Objective 4 – The resources (personnel, technology, and budget) allocated to back-up and business continuity efforts are optimally utilised.

To ensure optimal utilisation of resources in back-up and business continuity efforts, the College must implement robust strategic planning and efficient resource management, which includes deployment of IT staff, investment in IT infrastructure which fulfils the existing operational requirements but also has capacity scalability to meet future needs.

Through discussion with the IT team, we noted that specific members of the IT team responsible for managing the infrastructure have been assigned roles to for overseeing backup processes, cybersecurity, and disaster recovery. Arrangements are in place to ensure that IT staff are able to access opportunities for training and keeping updated on industry best practices. Several members of IT staff are familiar with the College's backup and recovery procedures ensuring resilience and coverage is available during emergencies.

The College has invested in a scalable, secure backup solution based on risk, compatibility with systems and infrastructure, and cost. This includes utilising an appropriate mix of cloud storage and on-premise infrastructure that aligns with the College's needs. Back-up processes have been automated to reduce manual workload. IT staff review back-up logs regularly to confirm that back-ups have been successfully taken in line with scheduled frequencies.

Restore tests are conducted, evidenced through frequent file recoveries, to verify backup reliability, though as recommended at **R2** regular server restores are required to provide further assurance on the College's digital business continuity capability.

Henderson Loggie

Aberdeen: 1 Marischal Square, Broad Street, AB10 1BL **T:** 01224 322 100
Dundee: The Vision Building, 20 Greenmarket, DD1 4QB **T:** 01382 200 055
Edinburgh: Level 5, Stamp Office, 10-14 Waterloo Place, EH1 3EG **T:** 0131 225 0200
Glasgow: 100 West George Street, G2 1PP **T:** 0141 471 9870