Meeting of the Audit and Risk Committee

to be held on Wednesday 25 February 2026 at 1000hrs via MS Teams

1

AUDIT & RISK COMMITTEE

NOTICE
There will be a meeting of the Audit & Risk Committee on Wednesday 25 February 2026 at 10:00am via Microsoft Teams.

AGENDA		
Agenda Item		**Paper**
29-25	Apologies for Absence	
30-25	Declaration of any Potential Conflicts of Interest in relation to any Agenda Items	
31-25	Minute of Previous Meeting (26/11/25)	X
32-25	Matters Arising Report	X
	Reserved Matter for Decision	
33-25	Risk Management Policy	X
	Matters for Discussion	
34-25	Internal Audit Reports • IT Network Arrangements • Payroll • Internal Audit Progress Report	 X X X
35-25	Committee Evaluation Feedback	Late Paper
	Reserved Matters for Discussion	
36-25	Strategic Risk Register	X
37-25	ASET Strategic Risk Register	X
	Matter for Information	
38-25	Annual Audit and Risk Committee Activity Report	X
39-25	**Any Other Business**	
40-25	**Summation of Actions and Date of Next Meeting** The next meeting will take place on Wednesday 27 May 2026.	

AUDIT & RISK COMMITTEE

MINUTE OF MEETING
DRAFT Minute of the Meeting of the Audit & Risk Committee held on Wednesday 26 November at 10:00am via Microsoft Teams and directly followed by a joint Audit & Risk and Finance & Resource Committees Meeting.

Agenda Item	
	Present: Jim Gifford Bryan Hutcheson Caroline Laurenson Ellie Zemani Leona McDermid Iain Watt Gerry Lawrie **In attendance:** David Archibald, Partner, Henderson Loggie Anne MacDonald, Senior Audit Manager, Audit Scotland Stuart Thompson, Vice Principal Finance & Resources Susan Lawrance, Board Secretary Karen Fraser, Minute Secretary
13-25	**Apologies for Absence** Apologies were received in advance of the meeting from M Dugan.
14-25	**Declaration of any Potential Conflicts of Interest in relation to any Agenda Items** J Gifford declared a transparency statement by virtue of his position with Aberdeenshire Council. L McDermid declared a transparency statement by virtue of her position with Aberdeen Foyer.
15-25	**Minute of Previous Meeting (18/09/25)** The Minute was approved as a true and accurate record.
16-25	**Matters Arising Report** Members noted the update to the Matter Arising captured in the shared report.
	Reserved Matter for Discussion
17-25	**Annual Internal Audit Report 2024/25**
18-25	**Audit Certification of Student Activity & Report AY2024/25**

19-25	**Audit Certification Support Fund Year-End Returns AY2024/25**
20-25	**Strategic Risk Register**
	Matters for Discussion
21-25	**Good Governance Compliance Report (from May 2025)** Attention was drawn to Appendix 1 which captured a summation of Regional Board activities and behaviours to determine compliance with the Code of Good Governance.

	With an apology expressed for the item not featuring at the 28/05/25 meeting, S Lawrance referenced the green highlighted additions and the continuation of actions from the previous version. Assistance was requested with the accessing of KPIs by Regional Board members via COLin in relation to point 3. **Action: Board Secretary to share "how to" detail via email.** A suggestion was put forward to have NESCol's work with the Aberdeen Local Employability Partnership included in point 6. D Archibald recognised the usefulness of the content and its tie-in with the 2025/26 internal audit programme and expressed positivity for the report having been completed. S Lawrance was thanked for the work undertaken.
22-25	**University of Dundee Key Findings Report** Following the publishing of the findings of the Gillies Report, NESCol's responses were captured in a straightforward format so as to demonstrate relevance and progress. In discussion, point 18 was spotlighted and a question raised regarding how NESCol's culture is measured. The response initially itemised evaluation undertaken via the People Services' Enhancement Plan, the tracking of complaints, and attendance at Open Staff Information Sessions as sources of understanding. In elaboration, it was ventured that all indicators suggest a positive and inclusive culture has been created; senior management is ever mindful of assessing and sustaining this. It was stated that good relationships exist with the trade unions, and this position is not taken for granted. D Archibald also shared that one key feature of the effectiveness review undertaken by the auditors is the scheduling of 1:1's at which Regional Board members are encouraged to express how the College feels to each of them. A request to have NESCol's responses shared with all Regional Board members for information was noted. **Action: Board Secretary to progress.** S Lawrance was thanked for the work undertaken.
	Matters for Information
23-25	**Data Protection Report AY2024/25** Report shared to facilitate an overview of DPO activities during AY2024/25 and to provide reassurance that NESCol continues to meet its legal obligations. Discussion centered on the increased volume of SARs and data breaches associated with email sending. Individuals' desires to gather information was noted, and refresher training implementation was a suggested cause for raised awareness resulting in greater reporting. Risk 6.2 on the Strategic Risk Register was highlighted. An observation was shared regarding an increase of the same in industry also, and the need to maintain a watching brief on volume to determine whether this is a temporary rise, or a trend. S Thompson confirmed a review of associated NESCol policies and procedures, and the sourcing of legal advice. In response to a positive comment concerning mandatory GDPR training having been completed by 88% of staff during the calendar year but noting that its' undertaking should be nearer 100% if compulsory, S Thompson highlighted an ongoing review regarding what constitutes obligatory learning.
24-25	**Any Other Business**

	No items were raised.
25-25	**Summation of Actions and Date of Next Meeting** S Lawrance provided a summary of the identified actions and confirmed the next Committee Meeting as Wednesday 25 February 2026 at 10:00am.
	Meeting ended at 11:14am **Members of the A&R Committee and Audit Scotland Attendee joined the F&R Committee Meeting at 11:30am**
	Reserved Matter for Decision (in conjunction with F&R Committee)
26-25	**Financial Statements, 2024-25 Overview**
27-25	**Draft Audited Financial Statements, 2024-25**

	Reserved Matter for Discussion (in conjunction with F&R Committee)
28-25	**Audit Scotland Annual Audit Report AY2024/25**
	Members of the A&R Committee and Audit Scotland Attendee left the F&R Committee Meeting at 12:10pm

Actions from the Audit & Risk Committee Meeting – 26 November 2025			
Agenda Item	**Action**	**Responsibility of**	**Deadline**
20-25	Strategic Risk Register:		
20-25	Strategic Risk Register:		
21-25	**Good Governance Compliance Report**: PowerBi access detail to be shared with Regional Board members via email	Board Sec	ASAP
22-25	**University of Dundee Key Findings Report:** responses to the findings to be shared with Regional Board members for information	Board Sec	10/12/25

Agenda Item 32-25

AUDIT & RISK COMMITTEE

An update on matters arising from the meeting of the Audit and Risk Committee held on 26/11/25.

Agenda Item	Action
20-25	**Action: Strategic Risk Register:**
	Status:
20-25	**Action: Strategic Risk Register:**
	Status:
21-25	**Action: Good Governance Compliance Report**: PowerBi access detail to be shared with Regional Board members via email
	Status: Complete. Email sent to Board members with options to access PowerBi.
22-25	**Action: University of Dundee Key Findings Report:** responses to the findings to be shared with Regional Board members for information
	Status: Complete. Findings shared at December Board meeting.

LEVEL OF ASSURANCE
Good

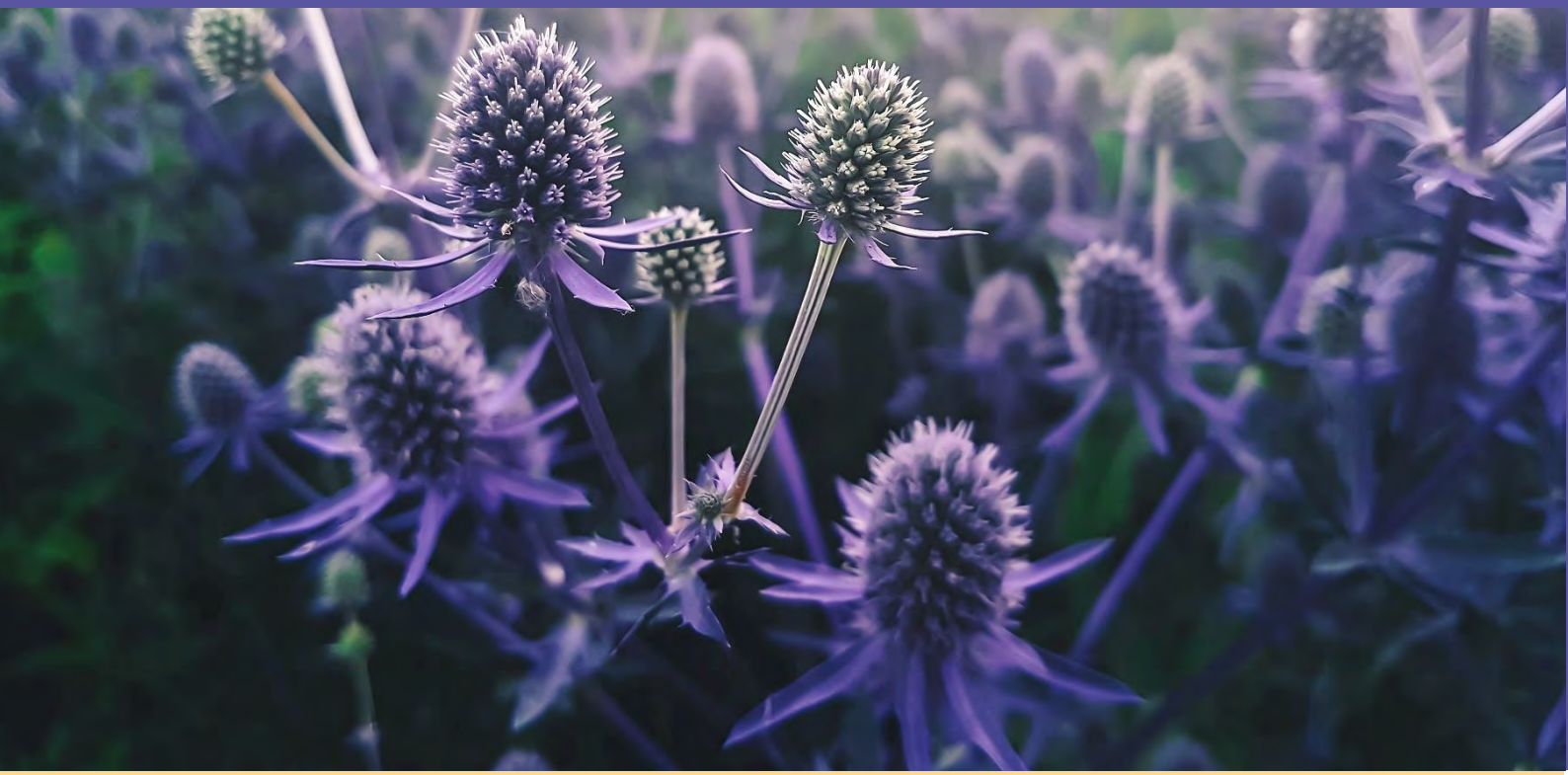
North East Scotland College

IT Network Arrangements

Internal Audit report No: 2026/03

Draft issued: 18 February 2026

Final issued: 19 February 2026



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 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 risk on the North East Scotland College ('the College') Risk Register:

- IF the College is the victim of a cyber-attack THEN the College may experience IT systems outages and/or data security breaches, both resulting in significant business disruption (current risk rating = 8, medium).

Background

As part of the Internal Audit programme at the College for 2025/26, we conducted a review of the College's IT network arrangements, including cyber security controls. Our Audit Needs Assessment, agreed with management and the Audit and Risk Committee in September 2025, identified this as an area where risk can arise and where Internal Audit can assist in providing assurances to the Principal and the Audit and 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 the College services to students and is also vital to the effective internal operation of the College. New technologies bring clear benefits, but also bring with them new obligations and areas of risk exposure.

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

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

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

Scope, Objectives and Overall Findings

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

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

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

Audit Approach

Our approach was based upon the guidance and best practice provided by NCSC; discussion with the Director of IT and Technical Services (ITTS) and members of the IT and Digital Team, review of relevant documentation; 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. We have taken cognisance of the new Topical Requirement for Cybersecurity, which was issued by the Institute of Internal Auditors in 2024 and will be enforced from 6 February 2026 onwards.

Summary of Main Findings

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

Strengths

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

- a risk management regime has been established, which includes identifying cyber security as key strategic and operational risks, and there are structures in place which act as appropriate mechanisms for evaluating and monitoring information security risks within the College;
- 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 the 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;
- multi-factor authentication (MFA) is in place for access to all corporate systems and data;
- data in transit is protected through encryption and secure communication channels;
- standard baseline security builds have been established for all College managed devices to ensure the consistency of security configurations;
- processes are in place to regularly test and monitor the effectiveness of cyber security training. Training is supported through regular communication of good practice to promote a positive cyber security culture;
- network hosts and endpoints are protected by an antivirus solution, which automatically scans for malware;
- the College has access to the HEFESTIS shared Chief Information Security Officer (CISO) service, which provides external evaluation of the College security environment and ongoing advice on compliance with applicable security standards;
- the latest HEFESTIS review of the College's compliance with the NCSC Cyber Assessment Framework (CAF), conducted in November 2025, reported that the College demonstrates a strong overall cyber maturity; and
- our review noted that the College has made significant improvements to its cyber security control environment since our last audit of this area in 2021. Our previous report was graded as 'requires improvement', and a total of 12 recommendations were raised (see internal audit report 2021/07, which was issued in May 2021).

Summary of Main Findings (Continued)

Actions Already in Progress

Our review identified several weaknesses or gaps in the College's cyber security control environment, including organisational as well as technical controls. However, these gaps had already been identified by the IT and Digital team through their own review and awareness of the control environment, and through the CAF compliance review process conducted in conjunction with HEFESTIS. We noted that actions are either in progress or are planned to address these gaps and therefore recommendations have not been raised in this report. These areas include:

- hardware and software inventories have been created along with processes and tools for asset identification, however following the migration of asset data during the implementation of UniDesk, the asset inventory is not fully up to date. Work is ongoing to ensure all asset information is complete;
- the College is aware that staff are able to, and do, extract data from College systems and share via email or store locally on their College device, rather than using the College tools and structured systems such as OneDrive, Teams and SharePoint. The need for a data classification and handling policy has been recognised by the College to strengthen data sharing controls, and this is being developed; and
- ensuring that cyber incident response training is conducted during 2026 to test and provide assurance that the College's documented incident response plan is effective.

Furthermore, a new learning management system (LMS) is scheduled to be implemented by October 2026 which will provide improved reporting and monitoring capability, and therefore improved visibility for line managers and the IT and Digital Team to follow up on instances of low or non-compliance with mandatory information security training.

Opportunities for Enhancement

We identified a small number of additional opportunities to build on existing arrangements and to further enhance the robustness of the control environment to reduce the potential for cyber-attack and data loss. These include:

- identifying potentially stale user accounts and remediating risks through disablement or deletion of staff and student accounts that are no longer required; and
- enhancing the existing procurement and supplier management processes by ensuring that suppliers provide evidence of any cyber security certifications held or standards adhered to.

Acknowledgments

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

IT Network Arrangements

Main Findings and Action Plan

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

Education and Training
People should be at the heart of any cyber security strategy. Good security considers the way people work in practice and does not 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 the organisation, but also demonstrates that you value your staff, and recognise their importance to the business.

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

We reviewed the College's approach to cyber awareness training and noted that the College issues regular communications and guidance to staff on cyber security: via the College intranet; by email; as part of the staff development days; ad hoc training for staff groups; and also tailored advice provided to individual staff members. As noted above, mandatory cyber security training is also in place for all staff.

Completion of mandatory cyber security training is monitored by the Learning & Development team, with reports then passed to line managers to follow-up with staff. The IT and Digital team are also notified of completion rates.

We obtained confirmation from the College's Learning & Development team, of the completion rates for the information security e-learning module, which noted that 79% of all staff had completed the training within the last three years, rising to 94% having completed at any time, i.e. in a period greater than the last three years. This indicates that either not all staff are completing the mandatory training; that results are not being accurately recorded when staff are completing the training; and / or there are weaknesses in the process for reviewing completion data and following up with staff to ensure that mandatory training is being completed in line with the College policy. The College has recognised that training completion rates could be improved, and a new learning management system (LMS) is scheduled to be implemented by October 2026 which will provide improved reporting and monitoring capability, and therefore improved visibility for line managers and the IT and Digital Team to follow up on instances of low or non-compliance with mandatory training.

The College currently requires staff to complete cybersecurity refresher training every three years, which is significantly less frequent than current good practice. Modern guidance indicates that awareness declines quickly, and more regular reinforcement is essential to reduce human-error-related breaches. Current industry recommendations point to training every 6 - 12 months, with additional shorter, periodic refreshers delivered throughout the year. The implementation of the new LMS will be accompanied by a mandatory requirement to complete the information security e-learning module. Thereafter, refresher training will be delivered annually supplemented by quiz-based learning exercises. Therefore, we have not raised a separate recommendation on this point.

IT Network Arrangements

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

Mandatory cyber security training forms part of induction training for new staff. All staff receive mandatory baseline and refresher cyber security training. New staff have one month to complete the full induction training pack, including mandatory training. Cyber security training can be completed up to one month after a user is issued with a College owned device and has access to the College's systems and data. Whilst not a significant risk for some roles, such as facilities staff, it is an elevated risk for users in high volume processing roles and / or those with access to personal and sensitive data (for example Finance and Student Records). Delays in completing cyber security training and implementing that learning into working practices creates security vulnerabilities through gaps in staff knowledge and awareness of cyber risks. Better practice would be for staff to compete cyber security training within 48 hours of employment commencing. This weakness and potential vulnerability were accepted by the College during the audit, and the induction process for new staff has since been updated to now require mandatory information security training to be completed within the first 48 hours of employment.

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.

Active Directory contains an account for every staff and student user. Over time, users leave the organisation, and those user accounts may not get removed from Active Directory. Stale accounts are user accounts that are inactive or no longer needed (e.g., belonging to former employees or students, or unused service accounts) and are a significant security issue, as potentially, former employees, students, suppliers, contractors or external attackers could use those accounts to gain unauthorised access or attack the organisation.

IT Network Arrangements

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

Observation	Risk	Recommendation	Management Response
As part of our testing, we obtained a report showing the status of staff and student user accounts listed in Active Directory and identified: • 33 staff user accounts (out of 727 accounts) listed as 'live' which had not been accessed for more than six months, with 18 of those accounts not accessed in the last 24 months. • 1,026 student user accounts (out of 9,303 accounts) listed as 'live' which had not been accessed for more than six months, with 61 of those accounts not accessed in the last 24 months. Although these accounts were still 'live,' we noted that access controls were in place, such as automated password expiry and Multi-factor authentication (MFA).	If unused accounts remain active, attackers or malicious insiders can exploit them to gain access without detection. Stale accounts often retain privileges they no longer need, increasing the impact if compromised. Security teams may overlook these accounts during monitoring, creating blind spots in access control.	**R1** The account lifecycle management process should be updated to ensure that: • existing automated reporting of data on stale student accounts is reported to curriculum and student records teams to review and confirm if students are still current and require access to their user accounts. Results should be communicated to the IT and Digital team so that user accounts that are no longer required can be disabled, and then deleted in time; • there is immediate deprovisioning of accounts for terminated employees; and • there is integration with HR systems to ensure timely updates.	**ACTION:** IT will implement a monthly report on stale student accounts and share with student records team for attention and action. If a user account is found to be no longer required, student records / curriculum team will update user status in student records system, triggering automated account deprovisioning. Review manual process for terminated accounts, working closely with HR to ensure process is followed. Automated integration with the HR is not possible and will be addressed with upcoming tender of HR solution. **To be actioned by:** IT Service Delivery Manager **No later than:** 31st March 2026
			Grade **3**

IT Network Arrangements

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

Incident Management
Incidents can have a huge impact on an organisation in terms of cost, productivity, and reputation. However, good incident management will reduce the impact when incidents 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 have 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 connected to the main domain, and multiple copies are retained across several sites, including cloud backups. Whilst back-ups have been partially tested in the past, through recovery of files, a full system and data restore has not been undertaken to provide assurance that a full restore would work as per the College's Business Continuity and Incident Response plans and can be restored in line with the expected recovery time objectives (RTOs). Scheduling a real time test of the back-up capability is difficult without disrupting College operations, however the College recognises the importance of testing back-ups and we noted that the College is committed to undertaking testing in the future. As a mitigation, incremental back-ups are reviewed and tested by the College to ensure that they are readable, and cloud copies of back-ups would allow a prompt restore of systems and data and remotely if College buildings could not be accessed.

Best practice guidance from the NCSC, and recognised cyber security standards such as ISO 27001, recommends that organisations maintain a documented and tested Cyber Incident Response Plan (CIRP) to ensure timely and coordinated action during cyber incidents. We noted that the College does have a documented response plan in place. Whilst we obtained evidence during our audit fieldwork that the College has technical and organisational controls for detecting and responding to cyber security incidents, there are no formal procedures for testing the effectiveness of its cyber incident response plan, with no testing of the plan conducted in recent years. However, the College has recognised the gaps in its response planning arrangements and management and the Board have committed to undertaking scenario-based desktop testing of the plan in 2026.

IT Network Arrangements

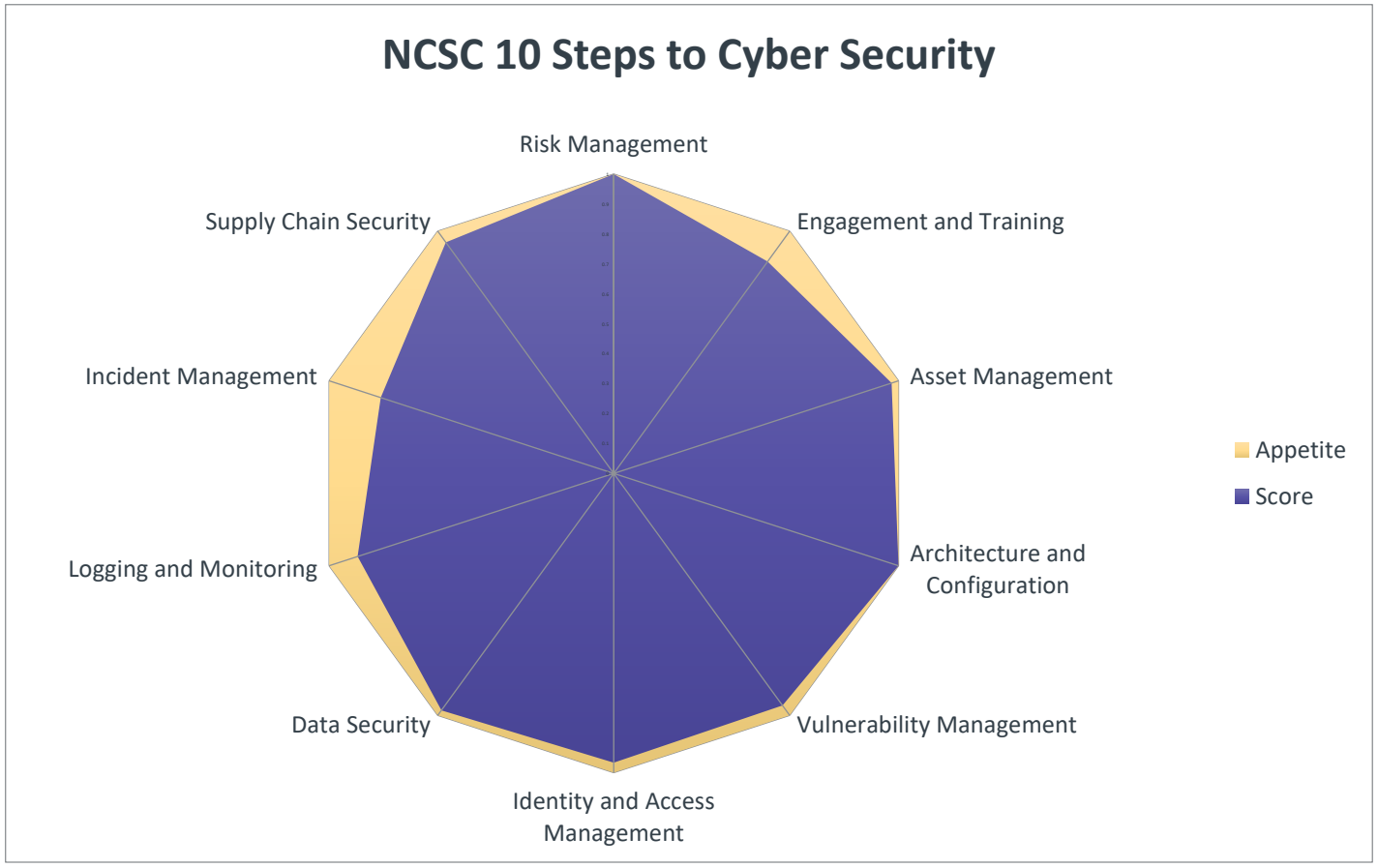
Objective 1: The internal controls in place which ensure that the security of the IT network, the configuration of key elements of IT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT and Digital department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

Supply Chain Security
The College relies on many third parties (system vendors, software suppliers, maintenance contractors). Weak security at a supplier can become the College's vulnerability. It is vital to vet suppliers' security practices and include cyber requirements in contracts.

Observation	Risk	Recommendation	Management Response
Best practice guidance (e.g. NCSC Supply Chain Security Principles, ISO 27001, and UK GDPR) recommends that organisations implement supplier due diligence and ongoing monitoring to ensure third parties meet minimum cyber security requirements. 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.	There is a risk that vulnerabilities within the supply chain could be exploited, leading to unauthorised access to sensitive data, disruption of critical services, and potential regulatory penalties.	**R2** Mandatory requirements should be introduced within existing procurement procedures for relevant suppliers to provide evidence of their current cyber security certifications. Steps should be taken to ensure that relevant suppliers provide copies of recertifications when these are due.	NESCol primarily uses approved, certified suppliers, with standards such as Cyber Essentials or ISO 27001 providing core assurance, these suppliers are engaged through approved frameworks (APUC etc). For smaller procurements without formal certification, NESCol applies proportionate, risk-based cybersecurity questionnaires. **ACTION:** Supplier questionnaires will be updated to record and annually review certification status. **To be actioned by:** InfoSec / Data Protection Manager **No later than:** 31st March 2026
			Grade **3**

Appendix I – NCSC 10 Steps to Cyber Security

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



Henderson Loggie

Aberdeen: 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 226 0200
Glasgow: Suite 5.3, Kirkstane House, 139 St Vincent Street, G2 5JF **T:** 0141 471 9870

LEVEL OF ASSURANCE
Good

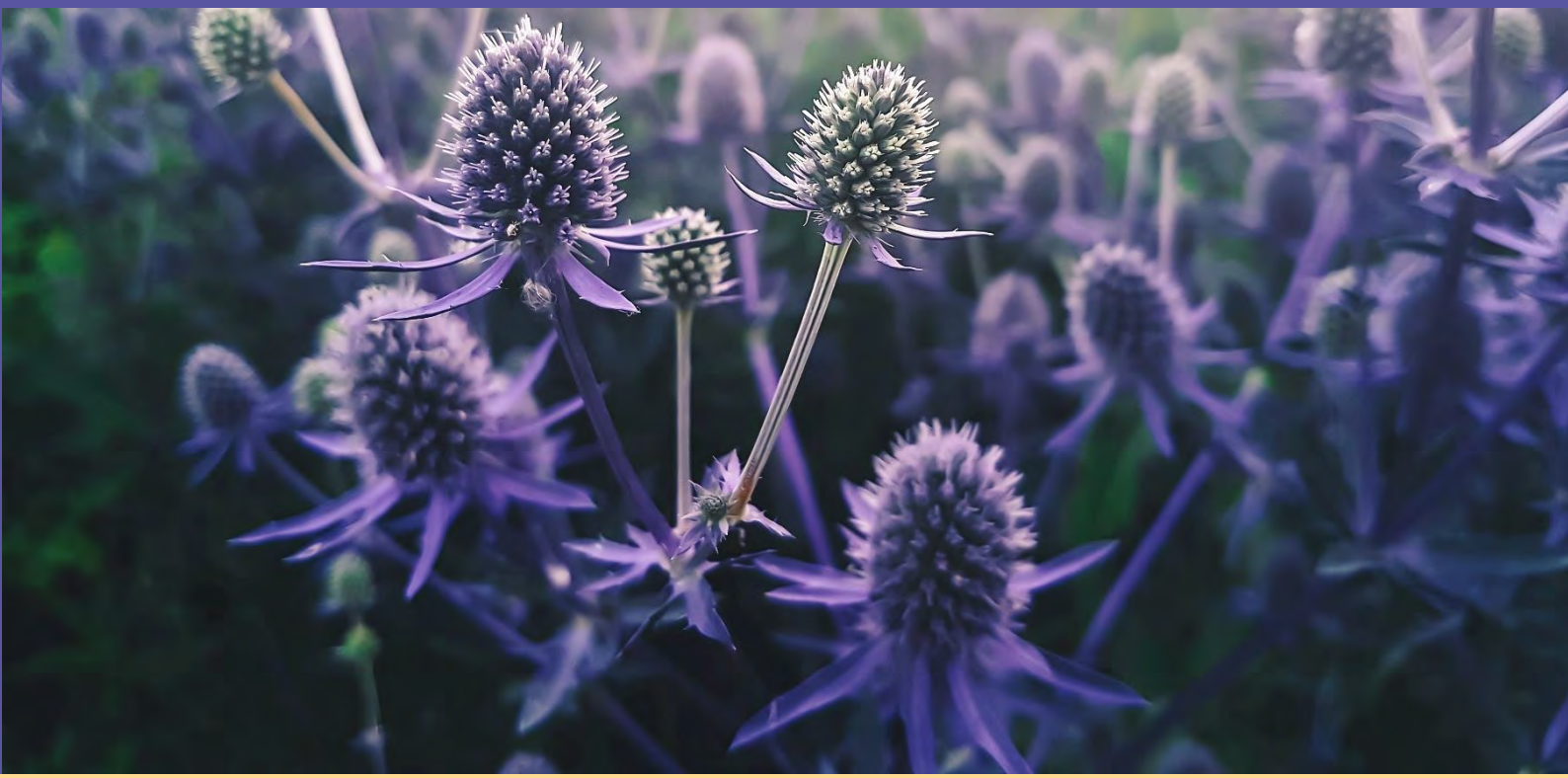
North East Scotland College

Payroll

Internal Audit report No: 2026/02

Draft issued: 4 February 2026

Final issued: 9 February 2026



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 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.

Payroll

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 North East Scotland College Risk Register (as at September 2025):

- Risk 6.1 - If staff do not adhere to key statutory obligations and legislative requirements then the College may face significant financial penalties and/or reputational damage may occur (Risk rating = 16)

Background

As part of the Internal Audit programme at North East Scotland College for 2025/2026, we carried out a review of the systems in place for Payroll. Our Audit Needs Assessment identified this as an area where risk can arise and where Internal Audit can assist in providing assurances to the Audit and Risk Committee and management that the related control environment is operating effectively, ensuring risk is maintained at an acceptable level.

The Payroll team provides payroll services for College employees, including ASET. All staff salaries and expenses payments are made through the Zellis payroll system. Where additional hours payments are due these are approved in line with the College's payroll procedures before payment is made. All data relating to new employees, leavers, additional hours, and changes to employees standing data is entered by the payroll team on to the Zellis payroll system.

Once the payroll amendments are completed the payroll is run with the output subject to a number of validation checks. Amendments are made, where required, before the final payroll is calculated and is submitted for payment. The total payroll cost to the College is circa £2.5m per month, with an additional £0.1m relating specifically to ASET.

Payroll

Scope, Objectives and Overall Findings

This audit considered the key internal controls in place over the College's spend on staff costs of approximately £34m per annum (including ASET). Our audit covered the procedures in place within both Human Resources (HR) and Finance

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

Objective	Findings			
To obtain reasonable assurance that systems are sufficient to ensure:	**Level of Assurance**	**1**	**2**	**3**
		No. of Agreed Actions		
1. Correct calculation of gross pay and deductions	**Good**	0	0	0
2. Correct calculation of employer national insurance and superannuation contributions.	**Good**	0	0	0
3. Part-time lecturers, overtime and staff expenses payments are properly authorised	**Good**	0	0	0
4. Appropriate approval and checking of changes to employee standing data.	**Good**	0	0	0
5. Starters and leavers are properly treated and enter and leave the system at the correct dates.	**Good**	0	0	0
6. There is proper authorisation, processing and recording of payments.	**Good**	0	0	0
Overall Level of Assurance	**Good**	**0**	**0**	**0**
		System meets control objectives.		

Audit Approach

Through our discussion with HR and Payroll staff, and review of procedures documentation, we identified the key internal controls in place within the College's HR / Payroll system and compared these with expected controls. We reported on any areas where expected controls were found to be absent or where controls could be further strengthened.

Compliance testing was then carried out to ensure that the controls in place are operating effectively, concentrating on starters, leavers and variations to pay.

Payroll

Summary of Main Findings

Strengths

- From our sample testing we confirmed that gross pay and deductions had been correctly calculated; and salaries, hourly rates and rates for non-statutory deductions were agreed to the standing data held in the HR / Payroll system.
- From our sample testing we confirmed that employer national insurance and employer superannuation contributions had been correctly calculated;
- All part-time lecturers, overtime and travel payments tested had been correctly input into the HR / Payroll system and were appropriately authorised, in line with the College's procedures;
- All changes to employee standing data selected for testing had been appropriately made to the HR / Payroll system and were independently checked and verified;
- Our sample of starters and leavers tested had entered and left the HR / Payroll system at the correct date with all details entered correctly; and
- There was proper authorisation, processing and recording of payments.

Weaknesses

- Due to the way the workflow process operates on MyView, once a change has been authorised by Payroll staff, this change is archived into the individual staff members portal and can no longer be reviewed by Payroll staff. As a result, for testing of processes that utilise the MyView portal, including the submission of timesheets, expenses and changes to standing data, we were unable to review source documentation to verify the authorisation by line management and Payroll staff.
- Supporting documentation was not available for one of the non-statutory deductions selected as part of our sample testing. Through discussion with Payroll staff it was identified that the deduction related to a club which was set up many years before the College merger which created NESCol. As such, the original supporting paperwork is not available or held on file for relevant employees. However, through discussion with the Assistant Principal People Services, it was established that during academic year 2025/26 the club had been disbanded and therefore no further deductions will be taken. The amounts relating to the social club were not significant and therefore no further action is proposed.

Acknowledgments

We would like to take this opportunity to thank the staff at North East Scotland College who helped us during the course of our review.

Main Findings and Action Plan

Objectives 1 and 2 - Correct calculation of gross pay and deductions, and correct calculation of employer national insurance and superannuation contributions.

We reviewed the systems and procedures in place to ensure that staff on the payroll are paid the correct amounts, including controls over increases in pay grades, and checked whether deductions had been made at the correct rates, and confirmed that these were appropriate.

A sample of 20 employees was selected at random, 15 from the College payroll (including both academic and support staff), and 5 from ASET, and the calculation of statutory deductions (PAYE and national insurance) were re-performed and checked for accuracy. As part of our audit testing, we were able to agree gross pay to salary records held on the combined HR and payroll system, Zellis, and confirmed these as accurate. Through re-calculation we were able to confirm accuracy of statutory PAYE and National insurance deductions.

The College operates two pension schemes – LGPS and SPPA. Our sample covered employees across both pension schemes and both employee and employer pension contributions were recalculated. There were no issues arising from our testing in this area.

In addition, a sample of non-statutory deductions, such as cycle to work payments and union subscriptions, were checked back to source documentation to ensure accuracy. One employee tested as part of the sample was a member of the College social club. No supporting source documentation was available for review. Through discussion with Payroll staff, it was identified that the social club was a group formed at Banff & Buchan College several years before the College merger which created NESCOL. None of the current payroll staff were employed in the College when the social group was formed and as a result no source documentation could be found. As the monthly contribution is negligible (at £3 per month), with few current members and the social club is no longer accepting new members, the impact is deemed to be negligible.

One sampled individual was subject to an arrestment payment, which had a minor discrepancy between the system calculation and our calculation. However, upon discussion, it was noted that due to the way the payroll system operates, there are rounding differences when compared to manual calculations. There were no other issues identified and the results of our testing in this area proved satisfactory.

Payroll

Objective 3 - Part-time lecturers, overtime and staff expenses payments are properly authorised

Additional Hours (part-time and overtime) payments:
Through discussion with payroll staff, it was confirmed that online submission of time is completed through My View. Employees record their hours worked through My View, which is then then sent to their line manager for approval. Following manager approval, the claim goes to payroll for input. Each month, a report is produced showing all time submitted through MyView and this is reviewed by Payroll and HR before being forwarded to SMT for review.

A sample of 20 additional hour payments were selected. For the 20 MyView time records, it was not possible to review the submission of individual time records by the employee or the relevant authorisation by the line manager. This was discussed with the Payroll Manager who highlighted that due to the way the system retains records, once a submission has been approved by the manager or by payroll, it is no longer visible on the system except to the employee. We were walked through the process that would be carried out, and shown an Excel spreadsheet showing authorisation of each payment.

For the sample of 20 selected, hourly rates from HR records were provided. These were then checked to payroll records to ensure that the correct hourly rate had been applied. These were all agreed with no issues noted.

Travel & subsistence:
Travel and subsistence claims are processed through Payroll. Employees complete expenses applications through the online portal, MyView, detailing the type of expense, the purpose of the expenditure, and the value. Once submitted, it is sent to the Payroll team who then consider the claim against the criteria set out in the Expenses Policy. If it meets the criteria set out in the Expenses Policy, then the expense will be authorised. If it does not, a notification is sent to the employee explaining any issues that have arisen, and they then have the opportunity to amend the claim for resubmission.

A sample of 20 employee expenses, which were processed through MyView, were reviewed. We were able to see evidence of the claims made, such as mileage, and non-travel expenses, such as payments for student Visas. Evidence was provided for these claims, including receipts and bank statements as appropriate with no issues noted. During testing it was noted that, similar to overtime payments, once a claim has been authorised and paid, specific records of authorisation are no longer viewable, although the claim is flagged as ‘approved’ on the system. Although we were unable to individual evidence of authorisation for the sampled claimed, assurance was provided that claims can only progress through workflows when appropriate authorisation is granted.

Payroll

Objective 4 - Appropriate approval and checking of changes to employee standing data.

The majority of changes to employee standing data are completed through the self-service portal, MyView. Through this system, staff can make changes to key standing data, which will impact on the standing information held on the payroll system, such as name, address or bank details. Any changes made through this method are notified to Payroll staff, who are then required to authorise any changes made. If a member of staff is unable to make a change through MyView, for whatever reason, then staff members can contact a member of the Payroll department directly to request a change, although we were advised that this service is rarely required. If the change is requested via email or through MS Teams, then the Payroll team contact the staff member directly by an alternative method of communication to verify the change requested, before amending the standing information on the payroll system.

As mentioned above at Objective 3, due to the workflow process on MyView, once a change has been authorised by Payroll staff, it is no longer possible for Payroll to view this change as is it archived into the staff members portal. Due to reporting limitations on the system it was not possible to review a report of changes made through the portal in the testing period to perform sample testing. As a result, we undertook walkthrough testing with the payroll team to demonstrate how a change would be made on the system by an employee, considering each stage up to authorisation. We are comfortable that the process as demonstrated is reasonable.

Payroll

Objective 5 - Starters and leavers are properly treated and enter and leave the system at the correct dates.

Starters
A sample of five new starts was selected at random from a new starts report generated from the HR / Payroll system. Each starter was successfully traced to all required documentation, including the appointment letter, contract of employment, HR starter form, and Payroll checklist. We noted that HMRC starter checklist were completed by four of the sampled new starts. For the one new start where there was no starter checklist, the employee was placed on an emergency tax code until the necessary information was made available for processing. We found that each new start had been entered on to the HR / payroll system at the appropriate date and in line with the contract start date. We re-calculated the first pay for each new start and agreed this to the relevant payslip. We did not note any issues from this testing.

Leavers
A sample of five leavers was selected at random from a leavers report generated from the HR / Payroll system. Each leaver was successful traced to the leavers form (and a letter of resignation where the leaver had resigned). We ensured that the leavers notification operated in each case and that the leavers form was signed by both payroll and HR. It was found that the leavers had been appropriately removed from the HR / payroll system in line with the last day of employment. We re-calculated the final pay for each leaver, ensuring that pay ceased on the final day of service and any outstanding financial sums were deducted. No issues were noted during our testing.

It should be noted that one of the sampled leavers left the College due to a dismissal. This instance was discussed with the Assistant Principal People Services, and it was noted that due to the circumstances of the individual leaving the College, a different leavers process was deployed. The employee was initially suspended for a period of time, before being dismissed following due process. As such, the standard leavers checklist was not utilised. However, we received adequate assurances that relevant steps (such as removal of the employee from relevant systems and retrieval of equipment) were still completed and the rest of the leavers process, including calculation of final pay, operated effectively with no issues noted.

Payroll

Objective 6 - There is proper authorisation, processing and recording of payments.

Prior to processing monthly payroll payments, a variance analysis is carried out between the current month and prior month's payroll figures. Any differences identified on the report are agreed back to source documentation (for example contractual changes or overtime / additional hours worked per authorised timesheets), to confirm that they are valid. The payroll is then reviewed and authorised by the Vice Principal Finance and Resources.

We reviewed a sample of three payroll runs in the period from January 2025 to December 2025 for both NESCol and ASET, and for each month we confirmed that there was evidence to confirm that the above checks had been completed.

We reviewed the monthly payroll BACS runs for the same period and noted that in all instances these had been appropriately authorised by the Financial Controller (External Affairs) or by the Vice Principal Finance and Resources.

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 226 0200
Glasgow: Suite 5.3, Kirkstane House, 139 St Vincent Street, G2 5JF **T:** 0141 471 9870

North East Scotland College

Internal Audit Progress Report

Audit and Risk Committee: 25 February 2026

Issued: 19 February 2026

Henderson Loggie

Internal Audit Progress Report
February 2026

Progress with the annual plan for 2025/26 is shown below.

Audit Area	Planned reporting date	Report status	Report Number	Overall Conclusion	Audit & Risk Committee	Comments
Internal Audit Annual Plan 2025/26	February 2025	Draft: 07/02/25 2nd Draft: 18/02/25 Final: 01/09/25	2026/01	N/A	26 February 2025	
Payroll	February 2026	Draft: 04/02/26 Final: 09/02/26	2026/02	**Good**	25 February 2026	
Estates Strategy / Capital Projects	September 2026					Agreed start date for fieldwork 04/05/26.
Budgetary Control	May 2026					Agreed start date for fieldwork 06/04/26.
Corporate Governance	May 2026					Fieldwork started w/c 16/02/26. Findings to be discussed at Board meeting on 18/03/26.
IT Network Arrangements	February 2026	Draft: 18/02/26 Final: 19/02/26	2026/03	**Good**	25 February 2026	
Credits Audit	November 2026					Agreed start date for fieldwork 10/08/26.

Audit Area	Planned reporting date	Report status	Report Number	Overall Conclusion	Audit & Risk Committee	Comments
Student Support Funds	November 2026					Agreed start date for fieldwork 01/09/26.
Follow-Up Reviews	May 2026					Agreed start date for fieldwork 06/04/26.

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.

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 226 0200
Glasgow: Suite 5.3, Kirkstane House, 139 St Vincent Street, G2 5JF **T:** 0141 471 9870

Agenda Item 35-25

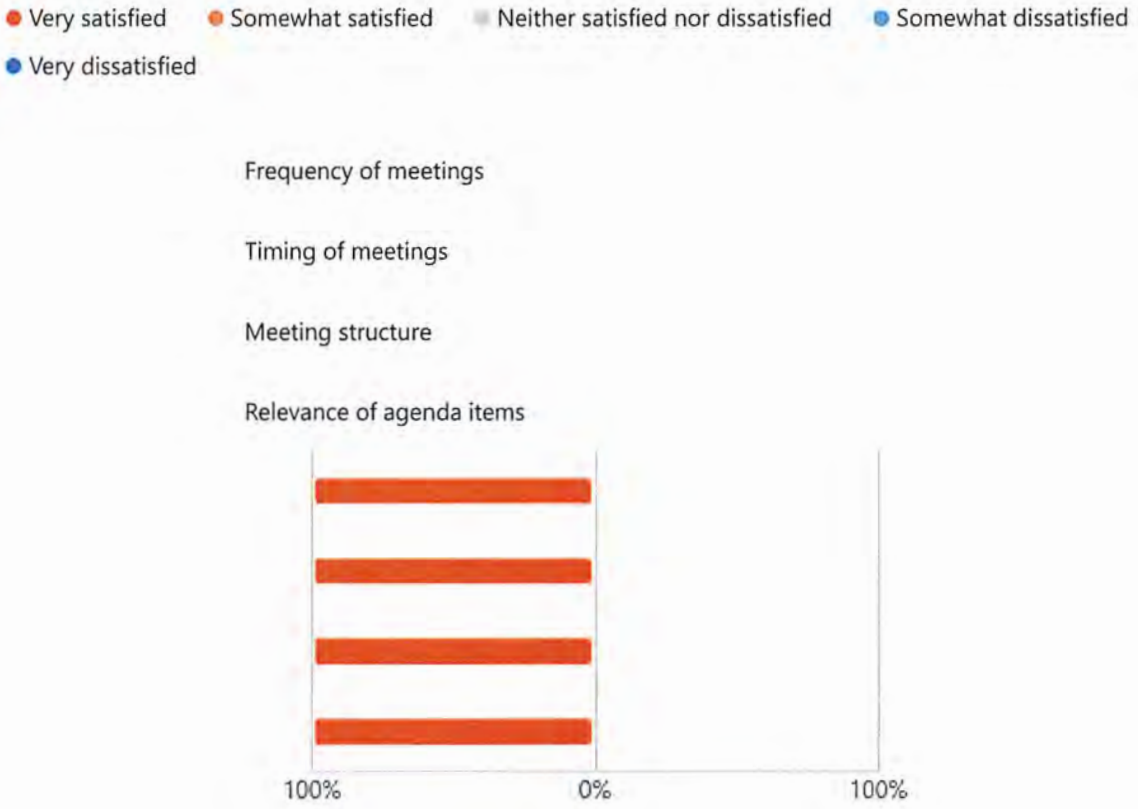
AUDIT AND RISK COMMITTEE Meeting of 25 February 2026	
Title: Committee Evaluation Feedback	
Author: Susan Lawrance, Secretary to the Board	**Contributor(s):**
Type of Agenda Item: **For Decision** ☐ **For Discussion** ☒ **For Information** ☐ **Reserved Item of Business** ☐	
Purpose: To provide the Committee with an opportunity to consider Members' feedback relating to the Committee's performance.	
Linked to Strategic Goal:	
Linked to Annual Priority:	
Executive Summary: Attached as Appendix 1 is feedback submitted by Committee Members on the performance of the Committee. The feedback was gathered through the use of an online anonymous questionnaire.	
Recommendation: It is recommended that the Committee discuss the information provided and agree if any actions are required to strengthen the performance of the Committee.	
Previous Committee Recommendation/Approval (if applicable)**:** None	
Equality Impact Assessment: **Positive Impact** ☐ **Negative Impact** ☐ **No Impact** ☒ **Evidence:**	

Responses Overview

Active

Responses	Average Time	Duration
6	43:09	78 Days

1. How satisfied are you with the meeting arrangements and their support for the Committee's effectiveness and remit?



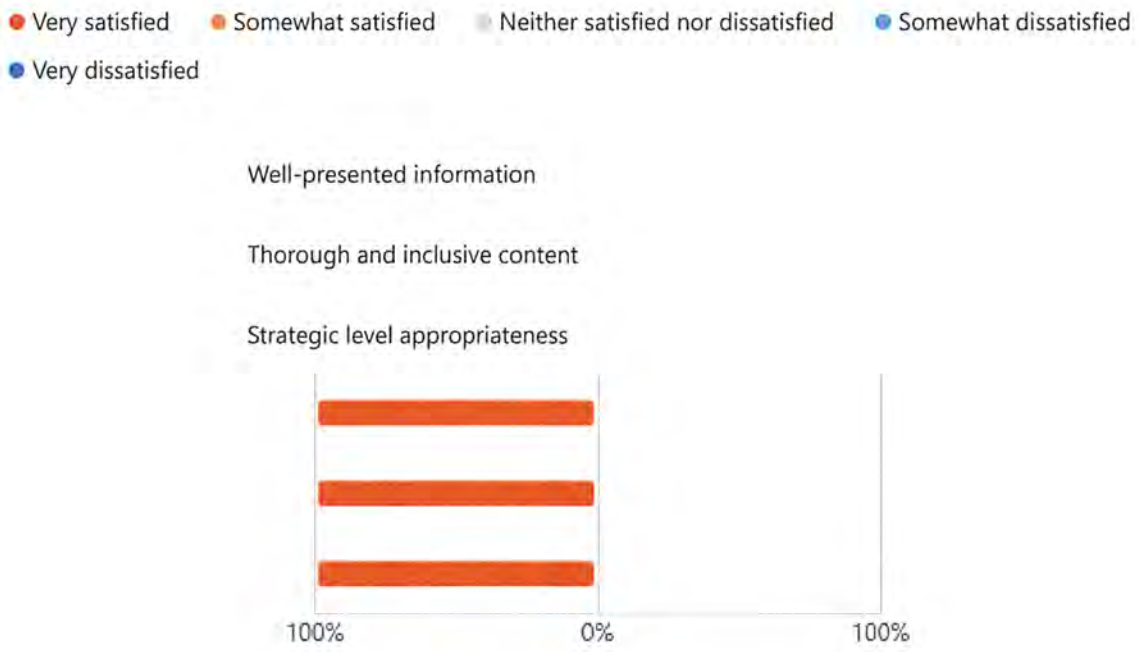
2. Please share any suggestions or comments regarding meeting arrangements or potential agenda items.

4
Responses

Latest Responses

"Meeting arrangements are well structured and support ef..."
"As much as possible have full agendas available to memb..."
"Items are always well researched"
...

3. How satisfied are you with the support and information provided by the Executive and Leadership team?



4. Do you have any suggestions to improve the support or information provided to the Committee?

3
Responses

Latest Responses
"The Executive and Leadership Team, together with our ext..."
"Not rea;;y - happy with what we currentl;y receive"
"None"

5. Do you agree that Committee Members are fully engaged, ensuring thorough discussion and con structive challenge of agenda items?

6. What could be done to further encourage engagement among Committee Members?

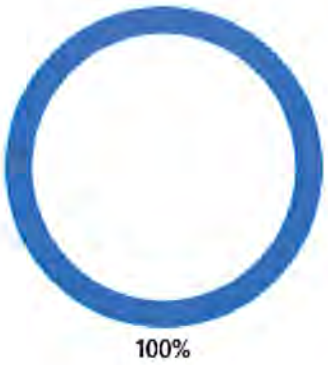
4
Responses

Latest Responses

"Engagement among Committee Members is strong, with ... "
"The early availability of papers would give people more ti... "
"Members are very engaged and there is a good mix of in... "
• • •

7. Do you agree that the collective skills, knowledge, and experience of Committee Members enable the Committee to fulfill its governance role?

Strongly Agree	6
Agree	0
Disagree	0



8. Please provide comments on the Committee Members' collective skills, knowledge, and experienc e.

4
Responses

Latest Responses

"The Committee benefits from a well-balanced mix of fina... "
"Think the mix is pretty good"
"There is a good mix of personalities as well as skills and e... "
• • •

9. Reflecting on your own skills and experience, how do you contribute to the Committee's work? H ow could your contribution be enhanced?

4
Responses

Latest Responses

"I bring experience in project governance, risk, commercial..."

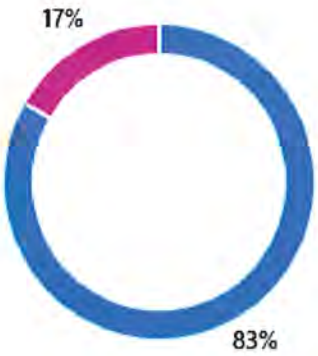
"Think the development/strategy days help widedm our k... "

"I believe you get the best out of me"

• • •

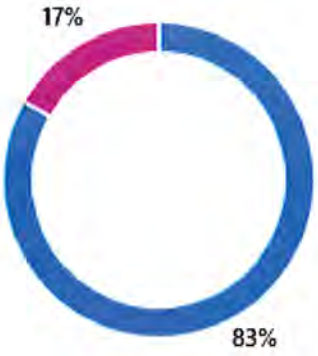
10. Do you agree that the Chair provides strong leadership, ensuring the Committee supports the C ollege's strategic ambitions?

Strongly Agree	5
Agree	1
Disagree	0



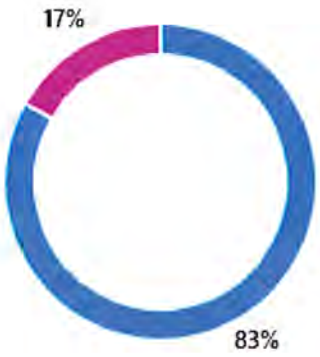
11. Do you agree the Chair communicates effectively with attendees, encouraging equal participatio n, listening, explaining, questioning, influencing, and constructive challenge?

Strongly Agree	5
Agree	1
Disagree	0



12. Do you agree the Chair allows sufficient time for informed and rigorous debate, ensuring issues are properly discussed and decisions are clear?

Strongly Agree	5
Agree	1
Disagree	0



13. Please share any additional comments regarding the Committee Chair's performance.

4
Responses

Latest Responses

"The Committee Chair runs meetings effectively, encourag... "

"They keep meetings on track whilst allowing for balanced... "

• • •

14. Do you have any additional feedback or suggestions to help improve the Committee's effectiveness?

3
Responses

Latest Responses

"The Committee is effective. Allocating more structured ti... "

"Only as mentioned above"

"Improvements to the Strategi Risk Register have streamli... "

Audit and Risk Committee Evaluation Feedback

Additional Comments

Qstn 2. Please share any suggestions or comments regarding meeting arrangements or potential agenda items:

- It's a very well run meeting helped by a narrow remit and focus
- Items are always well researched
- As much as possible have full agendas available to members a full week in advance of the meeting to allow time for reading and assessing
- Meeting arrangements are well structured and support effective oversight. Agendas are clear, relevant and appropriately focused on strategic and priority matters.

Qstn 4: Do you have any suggestions to improve the support or information provided to the Committee?

- Not really - happy with what we currently receive
- The Executive and Leadership Team, together with our external Audit partners, provide information that is clear, thorough and well presented. Papers are strategically relevant and support informed discussion and effective decision-making.

Qstn 6: What could be done to further encourage engagement among Committee Members?

- Perhaps a clearer look ahead of what is to be covered in each meeting across the year would be helpful.
- Members are very engaged and there is a good mix of input
- The early availability of papers would give people more time to think about what is presented and maybe formulate questions that would otherwise be missed.
- Engagement among Committee Members is strong, with regular and constructive challenge focused at the appropriate strategic level. Members are well prepared, papers are of high quality and discussions remain focused. The Committee benefits from an effective Chair who facilitates balanced participation and maintains a strong rhythm to meetings.

Qstn 8: Please provide comments on the Committee Members' collective skills, knowledge, and experience.

- It is good that the committee members have a range of professional backgrounds and skills from business and corporate organisations. This brings different perspectives and good practices around risk management, auditing and continuous improvement.
- There is a good mix of personalities as well as skills and experience that supports input from different perspectives
- Think the mix is pretty good
- The Committee benefits from a well-balanced mix of finance, audit, risk and sector expertise that enables it to fulfil its governance responsibilities effectively.

Qstn 9: Reflecting on your own skills and experience, how do you contribute to the Committee's work? How could your contribution be enhanced?

- I have experience of managing operational risk for offshore oil and gas facilities, this requires attention to detail and a very structured approach. These skills are very beneficial for reviewing documentation and asking questions to improve collective understanding of the risks.
- I believe you get the best out of me
- Think the development/strategy days help widened our knowledge of the work of the college. Being made aware of relevant on-line learning resources might be a benefit.
- I bring experience in project governance, risk, commercial oversight and strategy from the energy sector. I contribute mainly through questioning and testing assumptions, particularly around risk and governance. To enhance my contribution, I will continue to deepen my understanding of the education context and engage more in forward-looking discussions.

Qstn 13: Please share any additional comments regarding the Committee Chair's performance.

- Jim chairs the meeting very competently
- The meetings are well led and never feel rushed. Everyone is given the opportunity to ask questions. Actions are well recorded, giving clarity on what the outcomes are from the meeting.
- They keep meetings on track whilst allowing for balanced debate and questions
- The Committee Chair runs meetings effectively, encourages balanced participation and supports constructive challenge. Discussions stay focused and well structured, which helps the Committee work efficiently.

Qstn 14: Do you have any additional feedback or suggestions to help improve the Committee's effectiveness?

- Your insights are valuable and can help shape future Committee practices.
- Improvements to the Strategi Risk Register have streamlined the Board's ability to hone in on priority risks - very helpful changes.
- The Committee is effective. Allocating more structured time to forward-looking discussion on emerging risks and strategic priorities could further strengthen its impact.

Thank you to all committee members who took part in this evaluation.

Agenda Item 38-25/26

Audit & Risk Committee	
Title: Annual Report of the Audit and Risk Committee 2024-25	
Author: S Thompson Vice Principal Finance & Resources	**Contributor(s):** S Lawrance, Secretary to the Regional Board
Type of Agenda Item: **For Decision** ☐ **For Discussion** ☒ **For Information** ☐ **Reserved Item of Business** ☐	
Purpose: To enable the Committee to consider the Annual Report of the Committee 2024-25.	
Linked to Strategic Goal: **4 Building a stronger and more sustainable College**	
Linked to Strategic Risk(s): All	
Executive Summary: It is a requirement of the Financial Memorandum that the Audit and Risk Committee prepares an annual report on its activities for approval by the governing body. The report should include the Audit and Risk Committee's assessment of the adequacy and effectiveness of the College's internal control systems. This assessment should be based on the results of the work of the internal audit service (IAS) as reported in the IAS annual report, and the external auditor's opinion on the financial statements as well as the management letter and report issued to those charged with governance of the College. The 2024-25 Report is attached for consideration.	
Recommendation: Committee discuss the contents of the report**.**	
Previous Committee Recommendation/Approval (if applicable)**:** n/a	
Equality Impact Assessment: **Positive Impact** ☐ **Negative Impact** ☐ **No Impact** ☒ **Evidence:**	

NORTH EAST SCOTLAND COLLEGE

Annual Report of the Audit and Risk Committee to the Regional Board – Activities Undertaken for the year ended 31 July 2025

1. Introduction

1.1. Effective from 14 October 2008, current arrangements for Audit and Accounting are incorporated in the Financial Memorandum issued by the Scottish Funding Council (SFC).

1.2. The current Financial Memorandum was issued, effective 01 December 2014. This requires the preparation of an Annual Report from an institution's audit committee (or equivalent) to the Regional Board.

1.3. This report details the activities of the Audit and Risk Committee for the year ended 31 July 2025.

2. Committee Constitution and Terms of Reference

2.1. The following Committee members served during the year, together with possible and actual number of meetings attended: -

Name	Possible Attendance	Actual Attendance	Percentage Attendance
Jim Gifford (Chair)	4	4	100%
Iain Watt (Vice Chair)	4	1	25%
Bryan Hutcheson	4	3	75%
Caroline Laurenson	4	4	100%
Leona McDermid	4	4	100%
Ellie Zemani	4	2	50%
Susan Elston (Regional Board Chair)	4	4	100%
David Anderson (Co-opted until March 2025)	3	1	33%

2.2. The following Members of the Regional Board may attend and participate in meetings, but may not vote: -

- Chair of the Regional Board;
- Chair of the Finance and Resources Committee; and
- Principal and Chief Executive.

2.3. The Terms of Reference for the Audit and Risk Committee were reviewed at its meeting on 11 September 2024, having due regard to the provisions of the Code of Good Governance for Scotland's Colleges.

3. Internal Audit Service

3.1. The Regional Board appointed Henderson Loggie as internal audit service provider, for an initial four year period with effect from 01 August 2024.

3.2. The internal audit work carried out during the year was based on the Audit Needs Assessment, drawing on the College's Strategic Plan, Enhancement Plan and Strategic Risk Register, and approved at Audit and Risk Committee in February 2025. The Plan was systematically followed and the areas addressed during the year were: -

- Marketing and Communications (requested audit);
- Student Engagement (requested audit);
- Student Fees (requested audit);
- Workforce Planning (requested audit);
- Systems Development / Implementation (requested audit);
- Follow-up reviews (standard audit requirement);
- Credits Audit (required audit); and
- Student Support Funds (required audit).

3.3. Summaries of the issues arising in relation to each system or activity examined by the internal audit work in 2024-25 have been reported separately to the Audit and Risk Committee. All reports contained action plans detailing responsible officers and implementation dates. The reports were discussed and agreed with management prior to submission to the Audit and Risk Committee.

3.4. The internal auditor grades the areas reviewed as: -

- 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; and
- Unacceptable – System cannot meet control objectives.

3.5. In 2024-25, of the five requested audits, the internal auditor graded four areas reviewed as Good and one as Satisfactory.

3.6. The Committee and the internal audit service provider have established arrangements for grading recommendations arising from the Programme of internal audit review. Recommendations are graded as 'Priority 1', 'Priority 2' and 'Priority 3' (with 'Priority 1' representing matters requiring urgent attention).

3.7. In 2024-25, the internal auditor made 7 audit recommendations across the five requested reviews and two required reviews, with all the recommendations being Priority 3.

3.8. In addition, the internal audit service highlighted the existence of significant strengths and good practice across all areas reviewed.

3.9. Overall input to the audit assignments was 48 days, including those for Audit Management. The auditors presented their Annual Report 2024- 25 to the Audit and Risk Committee on 26 November 2025.

3.10. The auditors have reported that: -

In our opinion, NESCol has adequate and effective arrangements for risk management, control and governance. Proper arrangements are in place to promote and secure Value for Money. From the internal audit work conducted during 2024/25 we have not identified any downward trends in relation to risk management, control or governance. The Strategic Risk Register to be presented at the November 2025 meeting of the Audit and Risk Committee shows that 18 of 21 risks are above their target score, however none have been scored as 'red' risks (>19 on a 5x5 scale):
This opinion has been arrived at taking into consideration the work we have undertaken during 2025/26 and in previous years since our initial appointment in 2019/20.

4. External Audit Service

4.1. Audit Scotland

With effect from 01 January 2002, Audit Scotland has been responsible for the audit of all incorporated further education colleges in Scotland. External audit services for the financial year ended 31 July 2025 were provided by Audit Scotland themselves. This was the second year of Audit Scotland's appointment term. The audit started in early October, as planned. The auditors presented their Annual Report to the College's Audit and Risk Committee on 26 November 2025. No audit qualifications were necessary to the financial statements for the year to 31 July 2025.

Main Judgement on financial statements

Our audit opinions on the annual report and accounts of North East Scotland College are unmodified and confirm that the accounts are free from material misstatement. There were no significant findings or key audit matters to report. All audit adjustments required to correct the financial statements have been properly reflected in the audited annual report and accounts.

Wider scope and Best Value audit Conclusion

The college has broadly effective and appropriate arrangements in place to secure Best Value and cover the wider scope audit areas ie Financial Management; Financial Sustainability, Vision, Leadership and Governance; and Use of Resources to Improve Outcomes.

4.2. Aberdeen Skills and Enterprise Training Limited (ASET).

The College retains authority to appoint the external auditor of its wholly owned trading subsidiary. Hall Morrice carried out the external audit of ASET for the 12-month reporting period to 31 July 2025. As in previous years, Hall Morrice issued an unqualified audit opinion on the financial statements of ASET.

5. Risk Management

5.1. The Committee last reviewed the College's Risk Management Policy at its meeting of 29th November 2023 and discussed the College's Strategic Risk Register at each meeting throughout 2024-25.

6. Governance

6.1. The Committee ensures compliance with the Code of Good Governance for Scotland's Colleges.

6.2. At the 26th November 2025 meeting a formal review of compliance was presented and reviewed. The report highlighted good compliance and provided reassurance.

7. Fraud and Impropriety

7.1. No instances of fraud, theft or impropriety have been brought to the Committee's attention during the year or up to the date of approval of this report.

8. Self-Evaluation

8.1. The Regional Board undertakes an annual self-evaluation, including a review of its effectiveness against the Code of Good Governance for Scotland's Colleges which is considered by the Committee.

10.2 The Committee undertakes an annual self-evaluation reflecting upon performance against remit and the provision of Executive support which also feeds into the Board's annual self-evaluation

10.3 The Committee Chair is annually evaluated by the capturing of Members' observations of the office bearer's performance through the use of an anonymous online questionnaire. The questionnaire feedback is discussed at the Committee Chair's Annual Development Meeting with the Regional Chair.

9. Events since 31 July 2025

9.1. There are no other matters which have been brought to the Committee's attention which would impact on the opinion expressed in this report.

10. Conclusion

10.1. The Committee has obtained assurance that internal control systems are adequate and effective. This is based on the evidence provided by the results of

the internal audit service provider in the 12 months to 31 July 2025 and the external auditor's unqualified opinion on the financial statements for the 12-month reporting period to 31 July 2025.

10.2. The Committee is satisfied that, on the basis of the information provided to it by internal auditors, arrangements operate to allow the College to secure value for money.

10.3. The Committee is satisfied that the Regional Board has complied with the 'mandatory requirements' set by the Scottish Funding Council and has discharged its responsibilities in relation to audit and accounting.

10.4. The Committee is satisfied with the performance of Audit Scotland as external auditor to the College for the 12-month reporting period to 31 July 2025 and Henderson Loggie as internal auditor to the College for the 12 months to 31 July 2025.

10.5. The various reports and Committee minutes have been circulated to Board members.

Jim Gifford
Chair
Audit and Risk Committee

6 January 2026