BOARD OF MANAGEMENT
Audit and Risk Committee

Tuesday 3 March 2026 at 5.00pm **Room K-TO-624, Kingsway Campus** (MS Teams option available)

AGENDA

1.	**WELCOME**		
2.	**APOLOGIES**		
3.	**DECLARATIONS OF CONNECTION & INTEREST**		
4.	**MINUTE OF THE PREVIOUS MEETINGS** A&R Meeting & Joint A&R/F&I Meeting – 2 December 2025	Paper A for approval	
5.	**MATTERS ARISING**	Paper B for noting	
6.	**HEFESTIS CYBER SECURITY & MATURITY REPORT**	Paper C for information	DR
7.	**INTERNAL AUDIT**		
	7.1 Digital Strategy Audit Report	Paper D for approval	HL
	7.2 2025/26 Progress Report	Paper E for information	HL
	7.3 Follow Up Summary	Paper F for information	NA/ST
8.	**D&A RESPONSE TO SFC GOOD GOVERNANCE REPORT**	Paper G for approval	ST
9.	**STRATEGIC RISK REGISTER**		
	(i) Risk Register Update	Paper H for approval	ST
	(ii) Strategic Risk Register		
10.	**DATA REPORTING**	Verbal update	ST
11.	**EXTERNAL AUDIT**	Verbal update	MS

12. **DATE OF NEXT MEETING** – Tuesday 2 June 2026 at 5.00pm in Room K-TO-624, Kingsway Campus.

Agenda Item 4.0

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 3 March 2026

MINUTE OF THE PREVIOUS MEETING — PAPER A

BOARD OF MANAGEMENT

Audit and Risk Committee

Tuesday 2 December 2025 at 4.30pm in room K-TO-226 and via MS Teams

Minute of the Audit & Risk Committee meeting held on Tuesday 2 December 2025 at 4.30pm in Room K-TO-226 Kingsway Campus and via Microsoft Teams.

PRESENT:	Helen Honeyman (Chair Audit)	Richard Gordon
	Brian Mooney	Jenna Lawrence
IN ATTENDANCE:	Stuart Inglis (Henderson Loggie)	
	Michael Speight (Forvis Mazars)	Konzekerani Chigwenembe (Forvis Mazars)
	Ruth Holland (Forvis Mazars)	
	Steve Taylor (Vice Principal Support and Organisation)	
	Nicky Anderson (Director of Finance)	
	Megan MacQueen (Executive Coordinator)	Holly Farningham (Finance Manager)

1. WELCOME

H Honeyman welcomed members of the Audit & Risk Committee and J Lawrence to her first Audit and Risk committee as the elected staff member on the board.

It was confirmed that an independent meeting with audit representatives had been held directly prior to the meeting.

2. APOLOGIES

Apologies were noted from C Cussick, K McIntosh and D Archibald

3. DECLARATIONS OF INTEREST OR CONNECTION

No declarations of interest or connection were noted.

4. MINUTE OF THE PREVIOUS MEETING

The minutes of the Audit and Risk Committee meeting held on 23 September 2025 were approved as an accurate record.

5. MATTERS ARISING

The matter arising in relation to Cyber Security training had been raised but not progressed. This would remain under review.

6. AUDIT & RISK COMMITTEE ANNUAL REPORT TO THE BOARD

The Committee reviewed and approved the Annual Report to the Board.

7. INTERNAL AUDIT

7.1. STUDENT ACTIVITY

S Inglis summarised the report, highlighting that this was one of the mandatory audits undertaken each year. The report had a positive outcome with some minor recommendations noted. The main aspect of the report is the management summary which was submitted to SFC and adequate procedures are in place for the recording of data.

S Inglis highlighted that the team have followed up on previous years recommendations and how credits have been adjusted. Paragraph 231 and 232 of report states the College can claim the credits as students had made the required date of the course and incorrect credits were claimed and errors were found. Full time students on FE Course equates 17 credits.

H Honeyman asked if the SFC have ever contacted asking for credits returned, due to high credit numbers but S Taylor noted it has come up in the Outcome agreement meetings with SFC and they are comfortable and have no issues due to credits being used for guidance hours i.e. student guidance and group tutor activities.

H Honeyman thanked S Inglis and the College team for the positive report.

The report was approved.

7.2. STUDENT SUPPORT FUNDS

S Inglis summarised the report on the required audit by SFC that the College and HCLA need to follow. SAAS, Bursary and EMA were all audited. Minor point on EMA covering letter to SFC and found a mis payment to EMA for £450 but has been corrected by the College.

Recommendations around updating he childcare funding policy were noted. S Inglis noted that there was a technical comment included each year around the College bank account as the required use of the government banking service did not align fully with the policy from the Awards Agency.

S Taylor stated that he would follow up with student funding team regarding the award letter recommendation as this has arisen as a recommendation and was resolved two years ago. H Honeyman passed on her thanks to team for the very positive report.

The report was approved.

7.3. FOLLOW UP SUMMARY

S Taylor presented the summary and no follow up actions at this meeting. H Honeyman noted that this was a very positive position.

8. DATA REPORTING

S Taylor provided a verbal update confirming that there had been no reportable data breaches. A recent cyber review has been completed, with results to be presented at the next meeting.

H Honeyman asked about phishing activity; R Gordon confirmed phishing remains the sector's biggest threat, but awareness campaigns and monitoring are ongoing. Increasingly complex AI-driven threats were also noted.

The update was welcomed.

9. STRATEGIC RISK REGISTER

S Taylor provided a summary, highlighting key areas of risk. Financial sustainability was noted as a significant concern and a high red risk that is subject to ongoing discussion and review as the board and Committee meetings.

Discussion took place around RAAC Risk. Further structural engineering report in October with no change with condition of RAAC in building. S Taylor confirmed there is a 'plan B' in place if RAAC situation does get worse.

Following a question from B Mooney, S Taylor highlighted the sector are awaiting the outcome of the support staff pay awards, it has already been approved by Unison and Unite; however still waiting on GMB. The pay deal has been budgeted for, and the three-year deal (if approved) would provide greater financial clarity moving forward.

The potential to include a risk on governance was discussed including the potential for this to duplicate other risks within the register. There is an increased focus on governance practice, and any additional risk would potentially focus on this and how it interacted with areas such as financial sustainability. Following discussion it was suggested that this be raised for further consideration with the Chairs' Committee. S Taylor to progress.

The risk register was approved.

10. DATE OF NEXT MEETING

Tuesday 3 March 2026 at 5.00pm in room K-TO-624, Kingsway Campus.

Action Point Summary

Action	Responsibility	Date
Chairs Committee to consider potential risk on governance practice / failures	S Taylor	3 March 2026

BOARD OF MANAGEMENT

Joint Audit & Risk and Finance & Infrastructure Committee

Tuesday 2 December 2025 at 5.15pm in room K-TO-226 and via MS Teams

---

Minute of the Joint Audit & Risk and Finance & Property Committee meeting held on Tuesday 2 December 2025 at 17:15pm in Room K-TO- 604 Kingsway Campus and via Microsoft Teams

PRESENT:	Helen Honeyman (Chair)	Stephen Oakley
	Laurie O'Donnell	Brian Mooney
	Brian Lawrie	Simon Hewitt
	Ged Bell	Richard Gordon
	Kirstin Marsh	Robert Young
	Colin Smith	Jenna Lawrence
	Derek Stewart	
IN ATTENDANCE:	Steve Taylor (Vice Principal)	Megan MacQueen (Executive Coordinator)
	Holly Farningham (Finance Manager)	Nicky Anderson (Director of Finance)
	Andy Ross (Director of Infrastructure)	Billy Grace (Head of Estates)
	Michael Speight (Mazars)	Stuart Inglis (Henderson Loggie)
	Konzekerani Chigwenembe (Mazars)	Ruth Holland (Mazars)

1. WELCOME

H Honeyman welcomed members of the Joint Audit & Risk and Finance & Infrastructure Committees.

2. APOLOGIES

Apologies were noted from K McIntosh, D Mackenzie, D Smith, D Fordyce and C Cusick.

3. DECLARATIONS OF INTEREST OR CONNECTION

There were no declarations of interest or connection.

4. AUDIT LESSONS & IMPROVEMENT PLANNING UPDATE

N Anderson provided an update on the audit lessons and improvement planning. The plan was agreed in June 2025 and attached at appendix A. N Anderson asked all members to note that all improvements identified are complete with further actions detailed in section 4 of the report.

A key action had been identified while revising the Fixed asset Register and arrangements to revise this were in place and agreed with the auditors. N Anderson expects this will require a presentational change in the 2025/26 accounts but it should not affect the overall net book value of the assets.

B Lawrie asked if the word 'rigorous' could be removed from the risk register wording as could be misinterpreted. This was agreed. S Taylor to progress.

G Bell noted the low-level risks and praised the team on the progress made and asked what the likelihood is of completing the audit on time. N Anderson noted the audit is on time for completion and M Speight confirmed that there were only a couple of small points to finalise after discussions today.

M Speight noted it's a different situation compared to last year, adding the only item out with their control was a GTL letter has been rejected twice by the bank and this needs to signed off for audit to be completed.

The paper was noted.

5. INTERNAL AUDIT ANNUAL REPORT

S Inglis provided a report for summary and paper is for approval, noting there are no areas for concern. The overall opinion of the report is that the College has adequate arrangements for promoting and securing value of money. The key risks for risk register were highlighted.

B Lawrie made observation re using government banking service under instructions from SFC. B Lawrie asked if there was a benefit for College using interest bank account. N Anderson confirmed this was raised at the Audit and Risk Committee and a separate bank account is used to generate interest.

The annual internal audit report was approved.

6. DRAFT FORVIS MAZARS ANNUAL AUDIT REPORT

M Speight noted that the report is almost there and is deemed to be complete.

It was noted that not all journals were subject to review and in theory a Bacs payment could have been made by one person who has access to the approval process. It was advised for the team to look at controls in place for Journals. Page 6 of report is the two significant findings and noted in report with BACs payment process and journals. Appendix A with the other recommendations and with further polishing the risks can become low.

M Speight noted that three areas of risk were identified. Controls of journals feeds into this and recommend the completeness review of journals and taken onboard. Job evaluation is another risk.

Financial management was identified as meeting all requirements, however financial sustainability was a concern across the sector and whilst it is a risk for the College, it is being managed..

Forecast shows a cash budget is in a deficit this year, with steps being taken to ensure the College is financially sustainable. The public reports from SFC and Audit Scotland were noted.

B Lawrie thanked College staff and auditors for working together and noted the technical impact that pensions assumptions had on the figures.

B Lawrie also asked about the RAAC financial impact and is this part of the financial sustainability within the report. S Taylor noted the RAAC situation needs individual attention due to the possibility for this to impact adversely on College finances. This had been highlighted to SFC and Scottish Government.

R Young asked if D&A was the only college in this position and asked if the College insurance covered any additional operating costs that may be incurred due to RAAC. N Anderson noted

that insurers won't cover these additional costs

B Grace noted that around five or six colleges and universities were affected.

B Lawrie praised an excellent report.

7. DRAFT FINANCIAL STATEMENTS YEAR ENDED 31 JULY 2025

N Anderson summarised the financial statements and noted this is not for disclosure and not included in the minute. A correction to Board membership to include G Bell was identified and N Anderson will update and send to auditors to sign off.

8. DRAFT LETTER OF REPRESENTATION (WITHIN PAPER J)

N Anderson noted the ask is for Audit Committee members to recommend the draft Annual Accounts and Draft letter of Representation (included in the Forvis Mazars Annual Report (final), paper J page 58 to Board for approval on 9th December.

This was approved.

9. DATE OF NEXT MEETING

To be confirmed in 2025/26 Board Calander

Action Point Summary

Action	Responsibility	Date
Final minor changes to the Financial Statements to be made prior to approval by the Board of Management	N Anderson	9 December 2025

Agenda Item 5.0

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 3 March 2026

MATTERS ARISING PAPER B

BOARD OF MANAGEMENT
Audit & Risk Committee
Tuesday 3 March 2026

Matters Arising

Paper B for information

The following actions were noted from the Tuesday 2 December 2025 Audit & Risk Committee meeting.

Agenda Item No	Action	Current status	Open / Closed
9.0	Chairs Committee to consider potential risk on governance practice / failures **S Taylor**	Awaiting Chairs Committee meeting	Open

The following actions were noted from the Tuesday 2 December 2025 Joint Audit & Risk and Finance & Infrastructure Committee meeting.

Agenda Item No	Action	Current status	Open / Closed
7.0	Final minor changes to the Financial Statements to be made prior to approval by the Board of Management **N Anderson**	Completed for Board meeting	Closed

Author & Executive Sponsor: Steven Taylor, Vice Principal Support Services and Operations

Agenda Item 6.0

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 3 March 2026

HEFESTIS CYBER SECURITY & MATURITY REPORT

PAPER C

TLP:AMBER+STRICT

2025



Dundee and Angus College 2025 – 2026 Information and Cyber Security Report

Draft Version

CYBER ASSESSMENT FRAMEWORK VERSION 4.0 REPORT

CISO OFFICE

HEFESTIS LTD | Stirling Business Centre, Wellgreen, Stirling, FK8 2DS

Contents

Executive Summary 2
Overview 2
Interpretation 2
Recommendations Summary 3
Framework Comparison: PSCRF V2 vs CAF V4 4
Benefits of CAF V4 Adoption 4
Dundee and Angus College Assurance, Risk and Maturity Position 5
CAF version 4.0 audit scores by area 5
Introduction 6
Maturity Compliance 7
Introduction 7
Key aspects of the methodology 7
Interpretation 9
Overall Compliance Position 9
Objective-Level Analysis 9
Objective A – Managing Security Risk 9
Objective B – Protecting Against Cyber Attack 9
Objective C – Detecting Cyber Security Events 9
Objective D – Minimising Impact of Incidents 9
Key Strengths 10
Key Improvement Opportunities 10
Security Maturity Scorecards 2025 11
Partial Compliance Scorecard 11
Achieved Practices Scorecard 11
Combined Tier Scorecard 12
Recommendations 13
Recommendations by Objective 14
Conclusion 14
Appendices 1
APP01 Maturity Posture: 1
APP 02 Risk Posture: 1

Executive Summary

Overview

This report represents a progressive, transitional analysis from the Scottish Public Sector Cyber Resilience Framework (PSCRF V2) to the Cyber Assessment Framework (CAF V4), introduced in August 2025. It outlines Dundee and Angus College's current assurance, risk, and maturity position, highlighting key updates and compliance progress following the transition to CAF V4.

Over the past three years, the Dundee and Angus College has aligned with the Scottish Government's PSCRF V2, significantly enhancing its information and cyber security maturity and overall risk posture. This alignment has reinforced institutional goals for improved information and cyber security (ICS) governance, control, and resilience.

With the PSCRF standard reaching end of support in August 2025, the Scottish Government now recommends transitioning to the UK Government and NCSC-sanctioned CAF V4 for future cybersecurity reporting. This report details the College's current standing within that new framework and its alignment with previous standards.

Interpretation

Dundee and Angus College demonstrates a strong overall cyber maturity under CAF V4, achieving a combined compliance score of **95.4%** (Partial: **96.2%**, Achieved: **94.6%**) compared with PSCRF compliance levels of 88.3% as of August 2025.

It should be noted that these are not entirely like-for-like frameworks, but substantially similar in coverage of ICS maturity for assurance purposes as articulated within the Framework Comparison section.

Key strengths include full compliance in Governance, Service Protection, Identity and Access Control, System Security, Staff Awareness, Security Monitoring, Threat Hunting, and Incident Response, reflecting effective organisational control and operational resilience. Minimising the Impact of Incidents remains a clear strength, with full compliance in response planning and lessons learned activities.

However, several areas require targeted action or improvement:
Managing Security Risk: Governance and risk management are strong, but **asset management (80%)** and **supply chain security (71.4%)** require deeper assessment and improvement.
Protecting Against Cyber Attack: While service protection policies and system security are mature, **data security (81.6%)** shows weaknesses, particularly in understanding data classification (30.6%) and stored data handling (77.5%).
Detecting Cyber Security Events: Monitoring and threat-hunting capabilities are fully compliant, but continued assurance and testing should be maintained.

Overall, the College exhibits strong alignment with CAF standards. Improvements in data security, supply chain assurance, and asset management are recommended to achieve full maturity reporting and strengthen resilience.

Recommendations Summary

The College has made significant progress in its digital and organisational improvement programme throughout 2024–25, successfully transitioning to CAF V4 and enhancing assurance through PSCRF-aligned practices. Ongoing deep-dive assessments, improved reporting mechanisms, and strengthened governance controls have contributed to a more mature cyber posture. These initiatives should continue into 2025–26, embedding CAF principles within all ongoing operations.

Immediate priorities include completing current upgrade projects and embedding identified improvements, guided by risk-benefit prioritisation. All actions have been mapped to CAF objectives for consistency and traceability, reflecting areas highlighted in prior PSCRF assurance cycles.

For 2026, strategic focus should shift toward embedding security by design and maintaining continuous CAF compliance reporting to sustain and monitor ICS maturity. Targeted improvement areas are as follows:

1. Data Security (B3): Understanding Data and Stored Data Management

2. Supply Chain Security (A4): Strengthening Third-Party Controls and Secure Development Practices

3. Asset Management (A3): Improving inventory and lifecycle management

Where these initiatives align with the existing improvement programme, they should progress as planned. Any identified gaps should be integrated into the CAF Assurance Plan to ensure sustained compliance, operational resilience, and continuous improvement in cyber maturity across the College.

Framework Comparison: PSCRF V2 vs CAF V4

PSCRF V2 is tailored for Scottish public sector bodies, offering a structured approach to embedding cyber resilience into governance, operations, and incident response. It promotes baseline, target, and advanced maturity stages, aligning with standards like Cyber Essentials and NIS.

CAF V4, developed by the UK's National Cyber Security Centre, not only aligns with existing standards but also introduces 108 new Indicators of Good Practice and emphasises dynamic, outcome-based assessments. It sets a higher technical bar, reflecting the evolving threat landscape and regulatory expectations. For those with existing assessments against recognised standards, NCSC advises mapping previously audited (PSCRF/ISO) controls to CAF outcomes to ensure comprehensive resilience consistent with previous findings.

Benefits of CAF V4 Adoption

- Enhanced governance and accountability mechanisms with measurable outcomes.
- Seamless transition from PSCRF.
- Structured risk management processes for identification, monitoring, and mitigation.
- Improved alignment with data protection and privacy regulations.
- Systematic continuous improvement cycles and integration of lessons learned.
- Broad stakeholder engagement and transparency.
- Advanced threat intelligence and proactive threat hunting assurance.

Dundee and Angus College Assurance, Risk and Maturity Position

On behalf of Dundee and Angus College, HEFESTIS has uploaded the current assurance, risk, and maturity position statement to the new CAF module for ongoing cybersecurity assurance. This supports continued auditing compliance, underpinned by existing PSCRF documentation and tooling.

The CAF 4.0 Compliance Statement identifies three new principles

- A2.b Understanding Threat,
- C1.f Understanding Users' and Systems' Behaviour, and
- C2.a Threat Hunting

Previous security maturity activities have yielded opportunities for improvement across various domains, developing a year on year improvement in information and cyber security posture and practice.

It is proposed that ongoing and future information and cyber security management be monitored against the CAF as an appropriate, supported replacement assurance framework.

The report covers the period of January to November 2025. Calendar years are used as standard. Baseline reporting has been updated and converted to the CAF with the latest NCSC guidance applied.

It is recommended that ongoing deeper dives and Tabletop Exercise (TTX) activity to evidence, identify and assure progress, efficiency opportunities and enhance risk management in information and cybersecurity be performed on a progressive basis using the CAF standard across the College with continuance of current organisational reporting and controls.

The College currently displays a score of 95.4% against the CAF. This is expected to rise even further over the course of 2025/6 following ongoing assurance monitoring, reflecting improvements in threat management and ongoing planned cybersecurity enhancements. Previously recorded compliance levels reached 88.3 % against the PSCRF assessment.

The current College position, whilst containing many elements of continuous improvement, provides a robust foundation for ongoing assurance and risk management activity, with a focus on enhancing business efficiency and socialisation of good practice, leveraged to provide evidenced and auditable ongoing ICS resilience strengthening.

CAF version 4.0 audit scores by area.

A review of existing PSCRF evidence gathered over October 2023 to April 2025 was conducted over September to October 2025 following ingestion, alignment and review of the previously reported ICS maturity compliance scoring to the CAF as an evidenced baseline for comparison. The review and 2025 scoring have been updated consistent with the latest 2025 criteria and guidance provided by NCSC with no adjustment required, however ongoing monitoring will continue to assure consistent reporting against evolving standard versions and evolving cyber related threats. The transition to stable ongoing CAF v4.0 evaluation is therefore presented as complete.

Introduction

The purpose of this report is to provide senior management with a comprehensive assessment of the organisation's information and cyber security maturity. In today's digital landscape, where cyber threats are constantly evolving and becoming more sophisticated, understanding and enhancing security posture is paramount to safeguarding of assets, data, and reputation. By evaluating the security maturity across various domains, we can identify strengths, weaknesses, and areas for improvement, enabling us to make informed decisions and allocate resources effectively.

This report serves as a strategic tool for senior management to gain insights into the organisation's current state of security and to prioritise initiatives that will strengthen resilience against cyber threats. It is underpinned by a structured framework for assessing capabilities, benchmarking against industry best practices, and establishing a roadmap for continuous improvement. By proactively addressing security gaps and enhancing the maturity level, we not only mitigate risks but also bolster trust and confidence among stakeholders, including staff, students, partners, and regulators.

Moreover, in an environment where regulatory requirements and compliance standards are constantly evolving, maintaining a robust security posture is not just a matter of good practice but also a legal and regulatory obligation. This report helps to demonstrate organisational commitment to compliance and risk management, assuring that we meet the necessary regulatory requirements and adhere to industry standards.

The insights gained from this report are intended to empower senior management in making informed decisions, prioritise investments, and allocate resources effectively to strengthen and maintain improvements in security posture. By fostering a culture of security awareness and continuous improvement, we can mitigate risks, protect assets and help safeguard the long-term success and sustainability of the organisation.

Progress is recorded for assurance and auditing purposes within the new College CAF module, which aligns and is consistent with previous PSCRF reporting and evidence, providing ongoing reporting of all related activity from a single source.

Deep dive and project related activity have continued over 2025 and should continue over 2026 for ongoing monitoring and improvement purposes.

Maturity Compliance

Introduction

This report summarises the organisation's compliance and maturity against the Cyber Assessment Framework (CAF) version 4.0. The assessment evaluates four key objectives: managing security risk, protecting against cyber attack, detecting cyber security events, and minimising the impact of incidents. Each objective is broken down into principles and sub-principles, scored across partial and achieved compliance levels to provide a combined maturity percentage.

Overall, the organisation demonstrates strong alignment with CAF standards, achieving an average combined score of 95.4%. Governance, asset management, staff awareness, and incident response are fully compliant, reflecting robust strategic and operational controls. However, areas such as data security, identity and access management, supply chain security, and security monitoring show partial compliance, indicating opportunities for improvement.

This summary provides a clear view of current strengths and weaknesses, enabling prioritisation of actions to enhance resilience and achieve full CAF compliance. ***See table (overleaf) and Interpretation section for further information.**

Key aspects of the methodology

The methodology followed in this assessment involves a systematic review of an organisation's policies, procedures, and practices against the criteria outlined in the framework. This includes conducting interviews, deep dives and reviews of documentation to gather information about the current state of security and identify areas for improvement.

1. **Scoping and Preparation:** Defining the scope of the assessment and identifying the key stakeholders and resources involved. This ensures that the assessment is targeted and comprehensive, covering all relevant aspects of the organisation's security posture.
2. **Data Collection:** Gathering data through various methods, including interviews with key personnel, review of documentation such as policies and procedures, and analysis of technical controls and systems. This allows us to assess the effectiveness of security measures and identify any gaps or vulnerabilities.
3. **Analysis and Evaluation:** Analysing the collected data against the criteria specified in the framework to evaluate the organisation's maturity level across different domains. This involves assessing the adequacy of governance structures, the effectiveness of risk management practices, the robustness of technical controls, and the responsiveness of incident response procedures, among other factors.
4. **Gap Identification and Prioritisation:** Identifying gaps or deficiencies in security posture and prioritising them based on their potential impact and criticality. This enables us to focus efforts and resources on addressing the most significant risks and vulnerabilities first.
5. **Recommendations and Roadmap:** Based on the findings of the assessment, developing actionable recommendations and a roadmap for enhancing security maturity. This includes proposing specific initiatives, investments, and measures to strengthen resilience against cyber threats and improve overall security posture.

By following this methodology and leveraging the UK national Cyber Assessment Framework, we can conduct a thorough and systematic assessment of security maturity, identify areas for improvement, and develop a strategic roadmap for enhancing cyber resilience and safeguarding the organisation against emerging threats.

CAF V4.0 Maturity Compliance Summary

Objective	Principle	Compliance Status	Scoring (%)		
			Partial	Achieved	Combined
	CAF Standard Mean (Cumulative Total Score %)		**96.2**	**94.6**	**95.4**
CAF Objective A - Managing security risk	**Principle: A1 Governance**				
	A1.a Board Direction	**Compliant**		100.0	100.0
	A1.b Roles and Responsibilities	**Compliant**		100.0	100.0
	A1.c Decision-making	**Compliant**		100.0	100.0
	% Compliance			**100.0**	**100.0**
	Principle: A2 Risk Management				
	A2.a Risk Management Process	**Compliant**	100.0	100.0	100.0
	A2.b Understanding Threat	**Non-Compliant**	100.0	87.5	93.8
	A2.c. Assurance	**Compliant**		100.0	100.0
	% Compliance		**100.0**	**95.8**	**97.9**
	Principle: A3 Asset Management				
	A3.a Asset Management	**Non-Compliant**		80.0	80.0
	% Compliance			**80.0**	**80.0**
	Principle: A4 Supply Chain				
	A4.a Supply Chain	**Non-Compliant**	85.7	60.0	72.9
	A4.b Secure Software Development and Support	**Non-Compliant**	60.0	80.0	70.0
	% Compliance		**72.9**	**70.0**	**71.4**
CAF Objective B - Protecting against cyber attack	**Principle: B1 Service Protection Policies and Processes**				
	B1.a Policy and Process Development	**Compliant**	100.0	100.0	100.0
	B1.b Policy and Process Implementation	**Compliant**	100.0	100.0	100.0
	% Compliance		**100.0**	**100.0**	**100.0**
	Principle: B2 Identity and Access Control				
	B2.a Identity Verification, Authentication and Authorisation	**Compliant**	100.0	100.0	100.0
	B2.b Device Management	**Compliant**	100.0	100.0	100.0
	B2.c Privileged User Management	**Compliant**	100.0	100.0	100.0
	B2.d Identity and Access Management (IdAM)	**Compliant**	100.0	100.0	100.0
	% Compliance		**100.0**	**100.0**	**100.0**
	Principle: B3 Data Security				
	B3.a Understanding Data	**Non-Compliant**	50.0	11.1	30.6
	B3.b Data in Transit	**Compliant**	100.0	100.0	100.0
	B3.c Stored Data	**Non-Compliant**	75.0	80.0	77.5
	B3.d Mobile Data	**Compliant**	100.0	100.0	100.0
	B3.e Media Equipment Sanitisation	**Compliant**	100.0	100.0	100.0
	% Compliance		**85.0**	**78.2**	**81.6**
	Principle: B4 System Security				
	B4.a Secure by Design	**Compliant**	100.0	100.0	100.0
	B4.b Secure Configuration	**Compliant**	100.0	100.0	100.0
	B4.c Secure Management	**Compliant**	100.0	100.0	100.0
	B4.d. Vulnerability Management	**Compliant**	100.0	100.0	100.0
	% Compliance		**100.0**	**100.0**	**100.0**
	Principle: B5 Resilient Networks and Systems				
	B5.a Resilience Preparation	**Compliant**	100.0	100.0	100.0
	B5.b Design for Resilience	**Compliant**	100.0	100.0	100.0
	B5.c Backups	**Compliant**	100.0	100.0	100.0
	% Compliance		**100.0**	**100.0**	**100.0**
	Principle: B6 Staff Awareness and Training				
	B6.a Cyber Security Culture	**Compliant**	100.0	100.0	100.0
	B6.b Cyber Security Training	**Compliant**	100.0	100.0	100.0
	% Compliance		**100.0**	**100.0**	**100.0**
CAF Objective C - Detecting cyber security events	**Principle: C1 Security Monitoring**				
	C1.a Sources and Tools for Logging and Monitoring	**Compliant**	100.0	100.0	100.0
	C1.b Securing Logs	**Compliant**	100.0	100.0	100.0
	C1.c Generating Alerts	**Compliant**	100.0	100.0	100.0
	C1.d Triage of Security Alerts	**Compliant**	100.0	100.0	100.0
	C1.e Personnel Skills for Monitoring Tools and Detection	**Compliant**	100.0	100.0	100.0
	C1.f Understanding User's and System's Behaviour, and Threat Intelligence (within Security Monitoring)	**Compliant**	100.0	100.0	100.0
	% Compliance		**100.0**	**100.0**	**100.0**
	Principle: C2 Threat Hunting				
	C2.a Threat Hunting	**Compliant**	100.0	100.0	100.0
	% Compliance		**100.0**	**100.0**	**100.0**
CAF Objective D - Minimising the impact of cyber security incidents	**Principle: D1 Response and Recovery Planning**				
	D1.a Response Plan	**Compliant**	100.0	100.0	100.0
	D1.b Response and Recovery Capability	**Compliant**		100.0	100.0
	D1.c Testing and Exercising	**Compliant**		100.0	100.0
	% Compliance		**100.0**	**100.0**	**100.0**
	Principle: D2 Lessons Learned				
	D2.a Incident Root Cause Analysis	**Compliant**		100.0	100.0
	D2.b Using Incidents to Drive Improvements	**Compliant**		100.0	100.0
	% Compliance			**100.0**	**100.0**
	CAF Standard Mean (Cumulative Total Score %)		**96.2**	**94.6**	**95.4**

Interpretation

Overall Compliance Position

CAF Standard Mean (Cumulative Total Score):
Partial: 96.2%
Achieved: 94.6%
Combined: 95.4%
This indicates a very high overall maturity, with most principles fully compliant. Only a few areas show partial compliance, suggesting targeted improvements are needed.

Objective-Level Analysis

Objective A – Managing Security Risk

A1 Governance: All sub-principles (Board Direction, Roles, Decision-making) are fully compliant (100%) → Achieved.
A2 Risk Management: Risk Management Process and Assurance are compliant (100%), but Understanding Threat is non-compliant at 87.5%. Overall compliance is strong at 97.9%.
A3 Asset Management: Non-compliant at 80%, indicating a gap in asset inventory and lifecycle management.
A4 Supply Chain: Both sub-principles are non-compliant, scoring 60–85.7%, with an overall compliance of 71.4%.
Observation: Governance and risk management are strong, but asset management and supply chain security require improvement, particularly third-party assurance and secure development practices.

Objective B – Protecting Against Cyber Attack

B1 Service Protection Policies: Fully compliant (100%) → Achieved.
B2 Identity & Access Control: All sub-principles are fully compliant (100%) → Achieved.
B3 Data Security: Weaknesses in Understanding Data (30.6%) and Stored Data (77.5%), while other controls are strong. Overall compliance is 81.6%.
B4 System Security: Fully compliant (100%) → Achieved.
B5 Resilient Networks: Fully compliant (100%) → Achieved.
B6 Staff Awareness: Fully compliant (100%) → Achieved.
Observation: Data security is the weakest area under Objective B, especially data classification and handling.

Objective C – Detecting Cyber Security Events

C1 Security Monitoring: Fully compliant (100%) → Achieved.
C2 Threat Hunting: Fully compliant (100%) → Achieved.
Observation: Detection capabilities are mature and fully implemented.

Objective D – Minimising Impact of Incidents

D1 Response & Recovery: Fully compliant (100%) → Achieved.
D2 Lessons Learned: Fully compliant (100%) → Achieved.
Observation: Incident response and continuous improvement processes are robust.

Key Strengths

Governance, Service Protection, Identity & Access Control, System Security, Resilient Networks, Staff Awareness, Security Monitoring, Threat Hunting, and Incident Response are fully mature. Overall CAF compliance exceeds 95%, indicating strong alignment with CAF v4.0.

Key Improvement Opportunities

Data Security (Objective B3) – particularly Understanding Data (30.6%) and Stored Data (77.5%).
Asset Management (Objective A3) – 80%.
Supply Chain Security (Objective A4) – 71.4%.

Security Maturity Scorecards 2025

Grade
A > 90%
B > 70%
C > 50%
D > 30%
E > 20%
F < 20%

A "Red Amber Green" scorecard format from F: dark red <20% to A: dark green >90% is applied to represent security maturity levels across different domains or categories providing a structured vehicle to communicate complex information. Presented are the Scorecards for the College measured against the 4 objectives and 14 principles which constitute the CAF.

Partial Compliance Scorecard

Score Card Partial

CAF Objective A - Managing security risk		CAF Objective B - Protecting against cyber attack		CAF Objective C - Detecting cyber security events		CAF Objective D - Minimising the impact of cyber security incidents	
A	Principle: A1 Governance	A	Principle: B1 Service Protection Policies and Processes	A	Principle: C1 Security Monitoring	A	Principle: D1 Response and Recovery Planning
A	Principle: A2 Risk Management	A	Principle: B2 Identity and Access Control	A	Principle: C2 Threat Hunting	A	Principle: D2 Lessons Learned
A	Principle: A3 Asset Management	B	Principle: B3 Data Security				
B	Principle: A4 Supply Chain	A	Principle: B4 System Security				
		A	Principle: B5 Resilient Networks and Systems				
		A	Principle: B6 Staff Awareness and Training				

Achieved Practices Scorecard

Score Card Achieved

CAF Objective A - Managing security risk		CAF Objective B - Protecting against cyber attack		CAF Objective C - Detecting cyber security events		CAF Objective D - Minimising the impact of cyber security incidents	
A	Principle: A1 Governance	A	Principle: B1 Service Protection Policies and Processes	A	Principle: C1 Security Monitoring	A	Principle: D1 Response and Recovery Planning
A	Principle: A2 Risk Management	A	Principle: B2 Identity and Access Control	A	Principle: C2 Threat Hunting	A	Principle: D2 Lessons Learned
B	Principle: A3 Asset Management	B	Principle: B3 Data Security				
B	Principle: A4 Supply Chain	A	Principle: B4 System Security				
		A	Principle: B5 Resilient Networks and Systems				
		A	Principle: B6 Staff Awareness and Training				

Combined Tier Scorecard

Score Card Combined

CAF Objective A - Managing security risk		CAF Objective B - Protecting against cyber attack		CAF Objective C - Detecting cyber security events		CAF Objective D - Minimising the impact of cyber security incidents	
A	Principle: A1 Governance	A	Principle: B1 Service Protection Policies and Processes	A	Principle: C1 Security Monitoring	A	Principle: D1 Response and Recovery Planning
A	Principle: A2 Risk Management	A	Principle: B2 Identity and Access Control	A	Principle: C2 Threat Hunting	A	Principle: D2 Lessons Learned
B	Principle: A3 Asset Management	B	Principle: B3 Data Security				
B	Principle: A4 Supply Chain	A	Principle: B4 System Security				
		A	Principle: B5 Resilient Networks and Systems				
		A	Principle: B6 Staff Awareness and Training				

Recommendations

Dundee and Angus College is well progressed within, but not yet at the end of a programme of digital and organisational improvement continued over 2024/25. The organisation has, over the course of this period, transitioned not only to the new CAF criteria but also to a stronger level of information and cyber security assurance provided through PSCRF evidenced responses.

Ongoing reporting, control and resilience improvement and strengthening continue to be achieved through recurrent engagement to explore each of the assessment areas in depth, which should now be transitioned to include the context of CAF Principles.

It is therefore recommended that the current regime of effective organisational reporting and control with deep dive and TTX activity persist over 2025 - 6.

The immediate priority should be on completion of existing project activity particularly relating to upgrade and socialisation of improvements which are currently work in progress as a structured project with additional enhancement activity prioritised on a risk benefit basis. These activities have been remapped against the CAF for consistency. It should be noted that areas identified for action via 2023 – 2025 PSCRF assurance and project activity are also reflective of the CAF maturity posture.

For 2026, we would recommend that the following areas of activity be initiated and quality assured including security by design and adherence to CAF compliance reporting in the longer term for ongoing maintenance and monitoring of ICS maturity posture. Where the following lower scoring areas are included for activity within the existing cybersecurity improvement project scope and objectives, they should be undertaken as currently planned to ensure that additional identified controls are put in place and strengthened over the remainder of 2025 – 26 (potentially beyond for larger scale, more complex activities) with the objective of satisfying the security requirements of the College, its risk appetite and improving organisational cyber resilience.

Any additional improvement activity identified within the following lower-scoring control areas, which are not currently within the scope of the cybersecurity improvement project, should be considered for inclusion over the remainder of 2025 to 2026 in the context of assurance against the CAF standard. The CAF Assurance Plan, in conjunction with existing information and cybersecurity improvement evidence and action plans, should be used to track and substantiate ongoing ICS management, maturity improvement, monitoring, and compliance activity.

Recommendations by Objective

Data Security (Objective B3) requires targeted improvement, particularly in understanding and classification of data, which scored 30.6%, and stored data at 77.5%. While mobile data controls are already strong, the overall data security posture needs enhancement through improved governance of unmanaged devices and stricter media management practices aligned with PSCRF Area 8.

Identity and Access Control (Objective B2) remains a critical area for improvement despite strong overall compliance. Device management and IdAM processes should be strengthened to ensure consistent enforcement of authentication and authorisation policies. Planned activities should continue to be monitored via the Cyber Security Team, with alignment to PSCRF Areas 6 and 10.

Security Monitoring (Objective C1) achieved full compliance overall, but alert generation and behavioural analysis warrant a deeper review to maintain resilience and adaptability against evolving threats. This should be addressed through enhanced monitoring capabilities and advanced analytics, linked to PSCRF Area 13.

Supply Chain Security (Objective A4) scored 71.4%, indicating a need for further assurance and control over third-party risk management and secure development practices. A comprehensive review should be undertaken to strengthen contractual and operational security measures, aligned with PSCRF Area 11.

Conclusion

Dundee and Angus College has demonstrated excellent best practice in several areas and should be commended for the scale and breadth of information and cybersecurity improvements being progressed across the organisation. That same approach has now been extended into areas where it has been shown to need additional or ongoing resource application and attention. These efforts focus on the strengthening, management and improvement of security controls to elevate the maturity in these areas at and to an appropriate, achievable, and sustainable level.

Continuous enhancement of security maturity is crucial for constructing a proactive, adaptable, and robust cybersecurity stance, capable of efficiently managing risks, addressing threats, and safeguarding the organisation and its stakeholders in a constantly evolving digital environment.

Maintaining continual investment and dedication to cybersecurity endeavours is imperative for organisations to manage risk, safeguard assets, ensure compliance, uphold brand reputation, and maintain operational continuity. By dedicating resources to cybersecurity, organisations can address cybersecurity challenges proactively and position themselves for sustained success in an increasingly digital landscape.

Appendices

APP01 Maturity Posture:

A summary of the ICS current maturity compliance levels for each CAF principle area



Maturity Posture.pdf

APP 02 Risk Posture:

The ICS risk profile generated from the current CAF compliance levels in each principle area presented as a dynamic risk register



Risk Posture.pdf

*Only for use with Pervade CS Conversion module©

Maturity Posture

	Date of last Update	19/11/2025	Average Maturity Score	95.4		
Objective	CATEGORY	Description	Compliance Areas	Partial Maturity (%)	Achieved Maturity (%)	Combined Maturity Score (%)
	Principle	Description:Maturity is calculated as a percentage of each compliant sub-category articulated within the PSCRF (version 2.0) against each and all categories over the scope of the entire organisation. Maturity is evaluated on a scale of 0 to 100 with 0 being no compliance and 100 being fully compliant with both tiers 1 and 2 of the control assessment	Arranged by sub category	Mitigations and controls in place - Automatically updated from assessment framework	Mitigations and controls in place - Automatically updated from assessment framework	Automatically updated from assessment framework
Maturity Level	0. Organisational Maturity (Average)	Organisational Maturity is calculated as an average of the level of compliance against all PSCRF (version 2.0) categories. The scope includes the entire organisation. Maturity levels are expressed as a percentage	All compliance areas	96.2	94.6	95.4
CAF Objective A - Managing security risk	Principle: A1 Governance	The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.	A1.a Board Direction A1.b Roles and Responsibilities A1.c Decision-making		100.0	100.0
	Principle: A2 Risk Management	The organisation takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.	A2.a Risk Management Process A2.b Understanding Threat A2.c. Assurance	100.0	95.8	97.9
	Principle: A3 Asset Management	Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).	A3.a Asset Management		80.0	80.0
	Principle: A4 Supply Chain	The organisation understands and manages security risks to networks and information systems supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.	A4.a Supply Chain	72.9	70.0	71.4
CAF Objective B - Protecting against cyber attack	Principle: B1 Service Protection Policies and Processes	The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support operation of essential functions.	B1.a Policy and Process Development B1.b Policy and Process Implementation	100.0	100.0	100.0
	Principle: B2 Identity and Access Control	The organisation understands, documents and manages access to networks and information systems supporting the operation of essential functions. Users (or automated functions) that can access data or systems are appropriately verified, authenticated and authorised.	B2.a Identity Verification, Authentication and Authorisation B2.b Device Management B2.c Privileged User Management B2.d Identity and Access Management (IdAM)	100.0	100.0	100.0
	Principle: B3 Data Security	Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on essential functions. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the operation of essential functions. It also covers information that would assist an attacker, such as design details of networks and information systems.	B3.a Understanding Data B3.b Data in Transit B3.c Stored Data B3.d Mobile Data B3.e Media Equipment Sanitisation	85.0	78.2	81.6
	Principle: B4 System Security	Network and information systems and technology critical for the operation of essential functions are protected from cyber attack. An organisational understanding of risk to essential functions informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.	B4.a Secure by Design B4.b Secure Configuration B4.c Secure Management B4.d. Vulnerability Management	100.0	100.0	100.0
	Principle: B5 Resilient Networks and Systems	The organisation builds resilience against cyber attack and system failure into the design, implementation, operation and management of systems that support the operation of your essential function(s).	B5.a Resilience Preparation B5.b Design for Resilience B5.c Backups	100.0	100.0	100.0
	Principle: B6 Staff Awareness and Training	Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the operation of your essential function(s).	B6.a Cyber Security Culture B6.b Cyber Security Training	100.0	100.0	100.0
CAF Objective C - Detecting cyber security events	Principle: C1 Security Monitoring	The organisation monitors the security status of network and information systems supporting the operation of essential function(s) in order to detect security events indicative of a security incident.	C1.a Sources and Tools for Logging and Monitoring C1.b Securing Logs C1.c Generating Alerts C1.d Triage of Security Alerts C1.e Personnel Skills for Monitoring Tools and Detection C1.f Understanding User's and System's Behaviour, and Threat Intelligence (within Security Monitoring)	100.0	100.0	100.0
	C2.a Threat Hunting	Capabilities exist to ensure security defences remain effective and to detect cyber security events and incidents adversely affecting, or with the potential to adversely affect, essential function(s).	C2.a Threat Hunting	100.0	100.0	100.0
CAF Objective D - Minimising the impact of cyber security incidents	Principle: D1 Response and Recovery Planning	There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential function(s) in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.	D1.a Response Plan D1.b Response and Recovery Capability D1.c Testing and Exercising	100.0	100.0	100.0
	Principle: D2 Lessons Learned	When an incident occurs, your organisation takes steps to understand its causes, informing appropriate remediating action.	D2.a Incident Root Cause Analysis D2.b Using Incidents to Drive Improvements		100.0	100.0

*Only for use with Pervade CS Conversion module©

Risk Register CAF 4.0

	Date of last Update	19/11/2025	Average Risk Mitigation Score	1.2			
Objective	CATEGORY	Description	Compliance Areas	Partial Mitigation (%)	Achieved Mitigation (%)	Indiciative Risk Score (low 0 to high 25)	Target Risk Score
	Principle	Description:Maturity is calculated as a percentage of each compliant sub-category articulated within the PSCRF (version 2.0) against each and all categories over the scope of the entire organisation. Maturity is evaluated on a scale of 0 to 100 with 0 being no compliance and 100 being fully compliant with both tiers 1 and 2 of the control assessment	Arranged by sub category	Mitigations and controls in place - Automatically updated from assessment framework	Mitigations and controls in place - Automatically updated from assessment framework	Automatically updated from assessment framework	
Maturity Level	0. Organisational Maturity (Average)	Organisational Maturity is calculated as an average of the level of compliance against all PSCRF (version 2.0) categories. The scope includes the entire organisation. Maturity levels are expressed as a percentage	All compliance areas	96.2	94.6	1.2	4
CAF Objective A - Managing security risk	Principle: A1 Governance	The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.	A1.a Board Direction A1.b Roles and Responsibilities A1.c Decision-making		100.0	0.0	4
	Principle: A2 Risk Management	The organisation takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.	A2.a Risk Management Process A2.b Understanding Threat A2.c. Assurance	100.0	95.8	0.5	4
	Principle: A3 Asset Management	Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).	A3.a Asset Management		80.0	5.0	4
	Principle: A4 Supply Chain	The organisation understands and manages security risks to networks and information systems supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.	A4.a Supply Chain	72.9	70.0	7.1	4
CAF Objective B - Protecting against cyber attack	Principle: B1 Service Protection Policies and Processes	The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support operation of essential functions.	B1.a Policy and Process Development B1.b Policy and Process Implementation	100.0	100.0	0.0	4
	Principle: B2 Identity and Access Control	The organisation understands, documents and manages access to networks and information systems supporting the operation of essential functions. Users (or automated functions) that can access data or systems are appropriately verified, authenticated and authorised.	B2.a Identity Verification, Authentication and Authorisation B2.b Device Management B2.c Privileged User Management B2.d Identity and Access Management (IdAM)	100.0	100.0	0.0	4
	Principle: B3 Data Security	Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on essential functions. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the operation of essential functions. It also covers information that would assist an attacker, such as design details of networks and information systems.	B3.a Understanding Data B3.b Data in Transit B3.c Stored Data B3.d Mobile Data B3.e Media Equipment Sanitisation	85.0	78.2	4.6	4
	Principle: B4 System Security	Network and information systems and technology critical for the operation of essential functions are protected from cyber attack. An organisational understanding of risk to essential functions informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.	B4.a Secure by Design B4.b Secure Configuration B4.c Secure Management B4.d. Vulnerability Management	100.0	100.0	0.0	4
	Principle: B5 Resilient Networks and Systems	The organisation builds resilience against cyber attack and system failure into the design, implementation, operation and management of systems that support the operation of your essential function(s).	B5.a Resilience Preparation B5.b Design for Resilience B5.c Backups	100.0	100.0	0.0	4
	Principle: B6 Staff Awareness and Training	Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the operation of your essential function(s).	B6.a Cyber Security Culture B6.b Cyber Security Training	100.0	100.0	0.0	4
CAF Objective C - Detecting cyber security events	Principle: C1 Security Monitoring	The organisation monitors the security status of network and information systems supporting the operation of essential function(s) in order to detect security events indicative of a security incident.	C1.a Sources and Tools for Logging and Monitoring C1.b Securing Logs C1.c Generating Alerts C1.d Triage of Security Alerts C1.e Personnel Skills for Monitoring Tools and Detection C1.f Understanding User's and System's Behaviour, and Threat Intelligence (within Security Monitoring)	100.0	100.0	0.0	4
	C2.a Threat Hunting	Capabilities exist to ensure security defences remain effective and to detect cyber security events and incidents adversely affecting, or with the potential to adversely affect, essential function(s).	C2.a Threat Hunting	100.0	100.0	0.0	4
CAF Objective D - Minimising the impact of cyber security incidents	Principle: D1 Response and Recovery Planning	There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential function(s) in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.	D1.a Response Plan D1.b Response and Recovery Capability D1.c Testing and Exercising	100.0	100.0	0.0	4
	Principle: D2 Lessons Learned	When an incident occurs, your organisation takes steps to understand its causes, informing appropriate remediating action.	D2.a Incident Root Cause Analysis D2.b Using Incidents to Drive Improvements		100.0	0.0	4

Agenda Item 7.1

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 3 March 2026

INTERNAL AUDIT

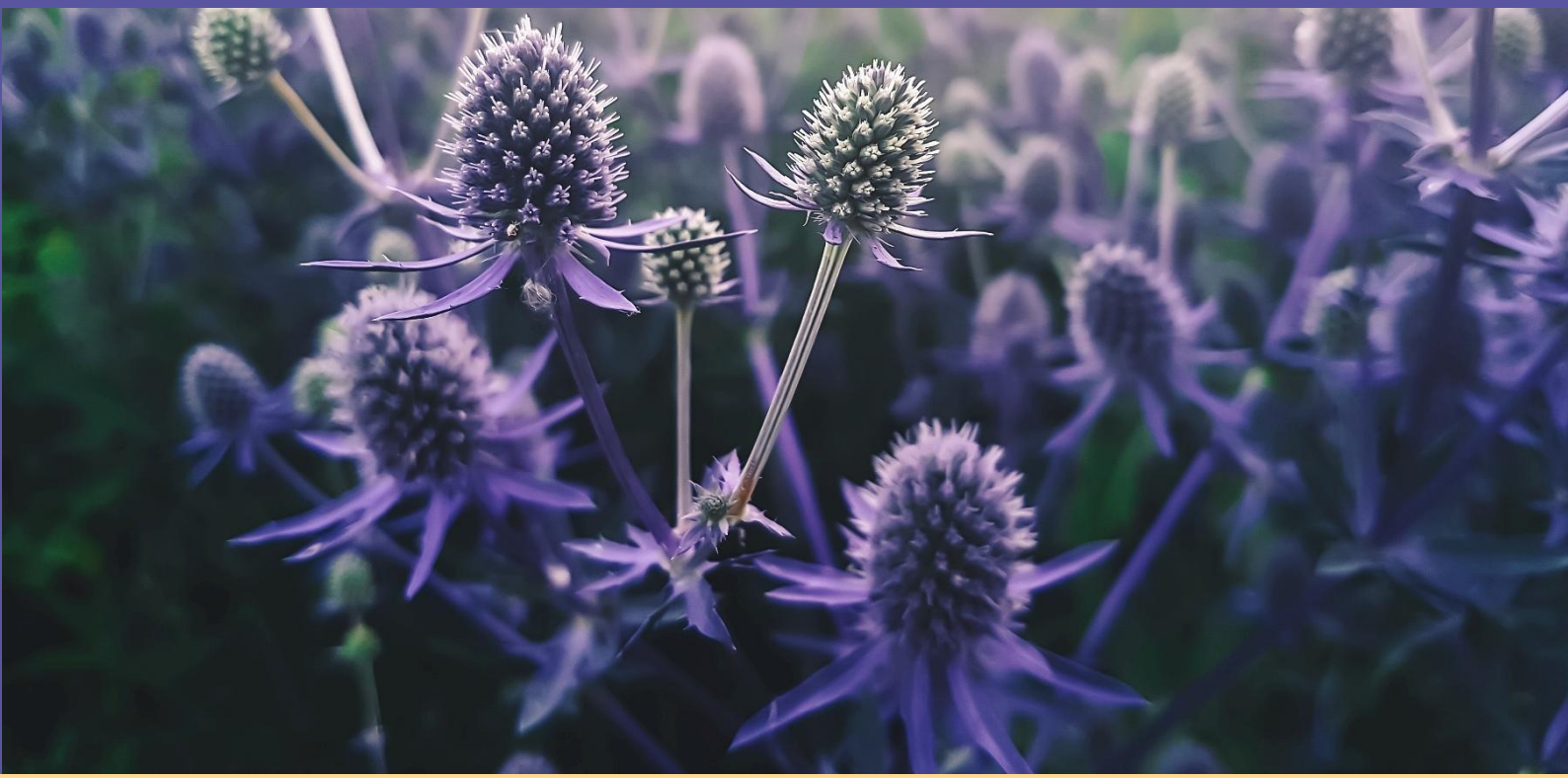
7.1 – DIGITAL STRATEGY AUDIT REPORT PAPER D

LEVEL OF ASSURANCE
Satisfactory

Dundee and Angus College

Digital Strategy Implementation

Internal Audit report No:	**2026/02**
Draft issued:	**13 February 2026**
2nd draft issued:	**20 February 2026**
Final issued:	**24 February 2026**



Henderson Loggie

Contents

		Page
Section 1	**Management Summary**	
	• Overall Level of Assurance	1
	• Risk Assessment	1
	• Background	1
	• Scope, Objectives and Overall Findings	1 - 2
	• Audit Approach	3
	• Summary of Main Findings	3
	• Acknowledgements	3
Section 2	**Main Findings and Action Plan**	**4 - 12**

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

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 Dundee and Angus College ('the College') Risk Register as at December 2025:

- Risk 3.1: Failure to reach aspirational standards in learning, teaching, and service delivery (Residual Risk Score: 4, Moderate);
- Risk 4.2: Failure to achieve ambitions of Digital strategy; strategy and development is ineffective (Residual Risk Score: 6, Moderate); and
- Risk 4.4: ICT infrastructure fails to support effective data security / data protection (Residual Risk Score: 8, Moderate).

Background

As part of the Internal Audit programme at the College for 2025/26, we carried out a review of the systems in place for Digital Strategy Implementation. 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 College has recently refreshed its Digital Strategy which sets out a framework for the use of digital technologies to support the College's business and curriculum objectives. A supporting Digital Services Roadmap has also been produced which translates the Digital Services operational plan into a clear timeline with milestones, responsibilities, and monitoring arrangements.. The Digital Strategy and Roadmap also support the College's 2030 Strategy.

Scope, Objectives and Overall Findings

Digital technology is key to delivering a wide range of College services in a more economic, efficient and effective way. Having a clearly articulated strategic approach to digital can bring several benefits such as:

- establishing a common vision for use of digital and the intended outcomes for learners, staff and external stakeholders linked to the College's strategic objectives;
- helping to ensure that College's use of digital technology is aligned with its key strategic objectives and other plans and strategies and is informed by a good understanding of current and future trends;
- reducing the risk of duplication of processes and systems within the College;
- consideration of resourcing digital over the short, medium and longer term together; and
- providing a framework against which to monitoring progress over the short, long and medium term.

Scope, Objectives and Overall Findings (continued)

This audit reviewed the processes for the development of the new Digital Strategy within the College and reviewed and assessed progress and outcomes relative to the iteration of the Digital Strategy which was in place up to 2025. We reviewed the adequacy and effectiveness of the governance, processes, and key controls over the definition, maintenance and delivery of the Digital Strategy to help the College meet its business objectives.

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

Objective	Findings			
The objective of the audit was to obtain reasonable assurance that:	**Level of Assurance**	**1**	**2**	**3**
		No. of Agreed Actions		
1. The Digital Strategy is aligned with the objectives outlined in the Strategic Plan and other supporting strategies.	**Good**	0	0	0
2. The Digital Strategy is aligned with Scotland Digital, the national digital strategy for the sector developed by Colleges Scotland.	**Good**	0	0	0
3. All internal and external stakeholders have been identified and provided opportunities to provide input and inform the identification of requirements of the IT Digital Strategy.	**Good**	0	0	0
4. The aims set out in the strategy are underpinned by projects which are aligned with an information systems and digital infrastructure development roadmap.	**Satisfactory**	0	0	1
5. An appropriate governance structure is in place that ensures that digital related projects, initiatives and requests are aligned to the Digital Strategy.	**Good**	0	0	0
6. The College is using / planning to use digital technology to meet learner and staff needs and deliver better outcomes, and is able to demonstrate this. This includes consideration of the potential impact of artificial intelligence on the College's teaching and learning approach.	**Good**	0	0	0
7. There is regular reporting to the Executive Team and Board on progress to deliver the Digital Strategy and the effectiveness of the Strategy.	**Satisfactory**	0	0	1
Overall Level of Assurance	**Satisfactory**	**0**	**0**	**2**
		System meets control objectives with some weaknesses present.		

Audit Approach

Through discussions with the Director of Infrastructure and Digital Services Manager, and review of relevant documentation, we assessed whether the digital strategic planning process and monitoring controls accord with good practice and are aligned with sector and national digital objectives.

Summary of Main Findings

Strengths

- The College has developed a coherent Digital Strategy structured around five themes of: Inclusion & Accessibility; Curriculum & Digital Skills; Business & Service Transformation; Partnerships; Infrastructure, Sustainability & Cyber.
- The Digital Strategy is aligned with the College 2030 Strategy, and other supporting strategies, including the People Strategy.
- The College has set out a clear commitment to developing strong digital leadership and a culture that supports innovation and collaboration. This approach aligns well with the Colleges Scotland National Digital Strategy.
- The Digital Strategy and associated Roadmap identify a strong cloud-first and Microsoft-aligned architecture providing a stable foundation for long-term capability development.
- There is a robust delivery Roadmap for 2025–2026 which translates the Digital Services operational plan into a clear timeline with milestones, responsibilities, and monitoring arrangements for digital projects.
- There was effective staff and student engagement during development of the Digital Strategy.

Weaknesses and Opportunities

- The Digital Strategy commits to establishing a five-year rolling investment plan to support digital transformation. The Roadmap covers only the period from 2025 to 2026, creating a misalignment between strategic resourcing intentions and operational planning. There is a risk that the College will be unable to deliver the full intent of the Digital Strategy because multi-year funding, sequencing, and dependency management are not yet planned beyond 2025/26.
- The College has an established set of governance groups, including the Digital Strategy Group and the Infrastructure Change Group, both of which report to the Senior Leadership Team (SLT). These groups meet quarterly and support upward reporting of progress on development and implementation of the Digital Strategy. However, through our review of Board and sub-committee minutes we did not identify any evidence that the College has formally reported progress on the Digital Strategy Action Plan to the Board since 2019. Reporting on digital activity over that period has been limited to general strategic project updates, cyber / infrastructure updates, and organisational strategy discussions, none of which have explicitly provided an update on the delivery of the Digital Strategy or the impact which has been achieved.

Acknowledgments

We would like to take this opportunity to thank the staff at Dundee and Angus College who helped us during the course of our review.

Main Findings and Action Plan

Objective 1 - The Digital Strategy is aligned with the objectives outlined in the Strategic Plan and other supporting strategies.

The new iteration of the Digital Strategy was reviewed, which will underpin the 2030 Our College Strategy currently under development. We were advised that this updated Digital Strategy will be presented for Board consideration and approval in March 2026. The new Digital Strategy demonstrates a clear commitment to developing strong digital leadership and fostering a culture of innovation and collaboration. This aligns with the College's leadership and governance aims outlined in the 2030 Strategy. Both strategies recognise the importance of leadership in driving transformation through innovation.

The College places a strong emphasis on digital inclusion and accessibility, and the Digital Strategy commits to providing equitable access to devices, assistive technologies, and compliance with accessibility standards. The College, in line with sector guidance, aims to embed digital skills within the curriculum and integrate emerging tools such as Artificial Intelligence (AI), Virtual Reality (VR), and Augmented Reality (AR). These actions support the College 2030 Strategy's aim to ensure digital accessibility, providing assistive technologies, embedding data within College operations and aligning learning, teaching and services with sustainability and transformative technologies such as AI and automation..

The Digital Strategy includes structured digital onboarding and career-long professional learning for staff. This aligns with the College 2030 Strategy's commitment to enhancing the skills, growth and futures of staff through comprehensive and career long professional learning.

The College has adopted a cloud-first approach to Digital / IT services which prioritises sustainability and cyber security. These commitments support the College 2030 Strategy's objectives toco-create and maintain digitally enabled, sustainable and state-of-the-art facilities and environments.

We also noted that the Digital Strategy demonstrates good alignment with other supporting strategies, including the People Strategy and Sustainability Strategy.

The College 2030 Strategy sets a target of fully implementing the Digital Strategy by 2030. The Digital Strategy does not clearly link its initiatives to specific targets identified in the 2030 Strategy. We noted that the College has taken the deliberate decision not to include key performance indicators (KPIs) in the Digital Strategy as the College's established practice is to assess implementation of strategies through the structures and processes that are in place for monitoring departmental operational plans, which reflect objectives and initiatives linked to strategic outcomes (see **R2** under Objective 7).

Digital Strategy Implementation

Objective 2 - The Digital Strategy is aligned with Scotland Digital, the national digital strategy for the sector developed by Colleges Scotland.

The College has set out a clear commitment to developing strong digital leadership and a culture that supports innovation and collaboration. This approach aligns well with the Colleges Scotland National Digital Strategy, which emphasises the need for sector-wide leadership and governance to drive digital transformation. Although the College strategy does not explain how it will link into national governance arrangements or participate in sector-wide oversight groups, we noted that the College's Director of Infrastructure and Digital Services Manager, and other staff, participate in Colleges Scotland, College Development Network and Jisc sector groups, therefore the College actively participates in shaping guidance for the sector.

The elements of the Jisc digital strategy toolkit applicable to the Further Education sector were utilised as good practice guidance to inform and shape the development of the Digital Strategy. Jisc was a key partner involved in co-producing the Colleges Scotland National Digital Strategy.

Objective 3 - All internal and external stakeholders have been identified and provided opportunities to provide input and inform the identification of requirements of the IT Digital Strategy.

In developing the Digital Strategy, we noted that the College has identified key internal and external stakeholders and has taken meaningful steps to provide opportunities for these individual groups to input into the development of the Digital Strategy. We noted evidence that demonstrates that internal stakeholders, particularly staff and students, were consulted directly and invited to comment on early drafts. Staff were kept informed through internal communications channels (including notices on the College's staff Teams site), and were encouraged to attend engagement workshops and submit feedback. The evidence reviewed demonstrates that their input was incorporated into revisions of the strategy. The Students' Association and Class Representatives were also formally engaged, with meetings held to discuss the draft strategy and provide structured feedback, resulting in amendments to the document and the creation of a more accessible student-friendly version. This demonstrates that the College was responsive to user feedback, as well as confirming a deliberate approach to ensure that the strategy is both relevant and comprehensible to learners.

We noted that early feedback received from staff and students on the draft Digital Strategy indicated some concerns around accessibility of language, jargon reduction, clarity around tools (e.g. the staff training matrix), and the relevance of the strategy to students. This feedback was captured and utilised to inform further development of the strategy. The Digital Strategy specifically references ongoing engagement and co-creation as a core "way of working," which aligns with the consultation activities that were undertaken during development of the strategy.

External stakeholder involvement included participation in both strategic and operational groups within Colleges Scotland, in order to understand sector level requirements and direction for digital transformation for Further Education in Scotland. Although we did not identify any evidence of direct engagement with other external stakeholders, such as employers, industry partners, or community organisations, the strategy does state intentions to work with those external groups during implementation of the strategy. We also recognise that the College maintains ongoing and strong relationships with employers and industry groups to identify current and future skills requirements, including digital skills, which the Digital Strategy addresses.

Digital Strategy Implementation

Objective 4 - The aims set out in the strategy are underpinned by projects which are aligned with an information systems and digital infrastructure development roadmap.

Our review identified that the new College Digital Strategy is broadly supported by the projects outlined in the Digital Services Roadmap for 2025 - 2026. The Roadmap translates the Digital Services operational plan into a clear timeline, with defined milestones, responsibilities, and monitoring arrangements for digital projects. This includes initiatives such as the rollout of new multi-functional devices, wireless connectivity, cloud onboarding, firewall upgrades, and the development of business intelligence dashboards. These projects align closely with the Digital Strategy's objectives to modernise infrastructure, strengthen cyber security, and improve operational efficiency.

The Roadmap also supports the Digital Strategy's commitment to enhancing the student experience through projects like migrating SVQ students to OneFile and reviewing the Future Talent offer. Similarly, the introduction of UniDesk and the creation of a digital training matrix align with the strategy's focus on service transformation and staff development. There is visible support for digital skills development as the Roadmap includes the launch of a digital training matrix and support offer (planned for May 2026), contributing to the strategy's objective of structured digital continuing professional development (CPD) for staff.

Observation	Risk	Recommendation	Management Response
The Digital Strategy commits to the establishment of a five-year rolling investment plan to support digital transformation. The Roadmap covers only the period from 2025 to 2026, creating a potential misalignment between strategic resourcing intentions and operational planning. The Digital Strategy makes substantial commitments relating to device access schemes, assistive technology, and targeted support for specific learner groups. However, these areas do not appear explicitly as defined milestones within the Digital Services Roadmap for 2025 - 2026. The Roadmap includes migration to OneFile for SVQs and participation in an AI roadmap, but lacks explicit milestones for competency standards, CPD pathways, curriculum digitisation, or adoption of emerging technologies. As the Roadmap only covers one year, influenced largely by the current annual funding and budgeting arrangements, it is not possible to formally determine how responsive the College's plans would be if additional funding were to become available, i.e. identifying projects that are proposed in future years being re-phased for earlier implementation if needed.	There is a risk that the College will be unable to deliver the full intent of the Digital Strategy because multi-year funding, sequencing, and dependency management are not planned beyond 2025/26, leading to reactive decision-making, higher cost, slippage of strategic outcomes, and lower value being realised.	**R1** Steps should be taken to ensure that the timeframe for the Digital Services Roadmap is extended to align with the Digital Strategy's requirement for a rolling multi-year digital investment framework. Longer term projects should be programmed in the extended Roadmap and aligned with the commitments and outcomes identified within the new Digital Strategy.	Digital team to create a multi-year operational plan to underpin implementation of the strategy and inform a rolling 3-year digital investment plan that aligns fully with the College Financial Strategy and budget process. **To be actioned by:** Director of Infrastructure **No later than:** 30 June 2026
			Grade **3**

Digital Strategy Implementation

Objective 5 - An appropriate governance structure is in place that ensures that digital related projects, initiatives and requests are aligned to the Digital Strategy.

The College has established a multi-layered governance framework, which is designed to ensure that digital projects are effectively aligned to the College's Digital Strategy. This governance structure operates across operational, executive, and strategic levels, providing both oversight and direction for digital transformation activities.

At the operational level, the College has a Digital Services team, which plays a central role in aligning operational digital activity with strategic objectives. The team reports to the Director of Infrastructure who has overall responsibility for monitoring digital initiatives, ensuring they progress in line with planned objectives, and raising issues or risks requiring escalation to the Executive Team.

In addition, an Infrastructure Change Group is in place which provides targeted oversight of infrastructure-related digital activity. This group meets quarterly on demand, reports to the Senior Leadership Team (SLT), and is led by the Director of Infrastructure. The group ensures that digital infrastructure change, such as network upgrades, cyber improvements or platform migration, are coordinated, risk-managed, and aligned with the College's longer-term digital vision.

At the executive level, the SLT and the Executive Team provide overarching oversight of digital delivery and have decision-making authority. The SLT meets fortnightly, while the Executive Team meets weekly, both meetings under the leadership of the Principal. These senior groups receive reports and recommendations from operational governance forums, enabling them to evaluate progress, confirm priorities, allocate resources, and assess cross-College impacts. Their oversight ensures that digital activities are not undertaken in isolation, but instead support the broader organisational priorities and operational requirements.

Strategic oversight is provided through the College's Board of Management and its sub-committees, specifically the Finance & Infrastructure Committee and the Audit & Risk Committee. Our review of Board and sub-committee papers noted that these committees regularly review strategic projects, infrastructure plans, financial sustainability, governance matters, and the College's Strategic Risk Register. Digital transformation, cybersecurity posture, and major digital investments form part a key pillar of these discussions, ensuring that the College maintains appropriate scrutiny and risk management over digital activities.

Operational groups, which contain cross-College representation from curriculum and support departments, have been established. These provide the mechanism for tracking technical and operational delivery of the digital projects and initiatives which are outlined in the Digital Services Roadmap and departmental operational plans.

This tiered structure enables the College to maintain visibility, control, and alignment across all stages of digital project development and delivery, supporting effective execution of the Digital Strategy.

Digital Strategy Implementation

Objective 6 - The College is using / planning to use digital technology to meet learner and staff needs and deliver better outcomes, and is able to demonstrate this. This includes consideration of the potential impact of artificial intelligence on the College's teaching and learning approach.

The Digital Strategy clearly articulates intentions across five specific themes: Inclusion & Accessibility, Curriculum & Digital Skills, Business & Service Transformation, Partnerships, and Infrastructure / Cyber / Sustainability, and references specific approaches such as cloud-first, assistive technologies, data-driven decision-making, and responsible use of emerging technologies such as AI. These show a credible plan to meet learner and staff needs, targeting learner experience and staff capability.

The Digital Strategy does not fully evidence current outcomes or provide measurable targets, baselines, or adopt KPIs, and its treatment of AI is principle-led rather than operationalised (e.g. no dated pilot, scale pathway, pedagogy changes, or evaluation framework). Consequently, the strategy explains the "what and why," but only partially explains the "how much, by when, and with what impact." However, we acknowledge that the College, and the wider HE/FE sector, is still navigating through the discovery phase for AI, and is exploring opportunities where AI can be sensibly integrated into teaching and learning and support activities. Therefore, we recognise that measurable targets and KPIs will be developed once the College has identified suitable use cases for AI in teaching and learning. Use of AI in learning and teaching is a complex issue and further guidance is required from various qualification bodies on how and where AI can be incorporated into existing course frameworks. The College, and the wider sector, continues to monitor developments in this area.

In the meantime, the College is focusing on data security and governance of AI, to ensure that AI tools are adopted in a safe, secure and ethical manner.

Digital Strategy Implementation

Objective 7 - There is regular reporting to the Executive Team and Board on progress to deliver the Digital Strategy and the effectiveness of the Strategy.

The College has an established set of governance groups, including the Digital Strategy Group and the Infrastructure Change Group, both of which report to the SLT. These groups meet quarterly and support upward reporting of progress on development and implementation of the Digital Strategy.

Under the previous Digital Strategy, which was published in 2019, an Action Plan was developed which contained objectives under each of the key outcomes and it was expected that this would be formally monitored every six months by the Digital Strategy Group with updates then subsequently reported to the College Executive Team and the Board. Progress updates on the previous version of the Digital Strategy have not been explicitly included in those updates since 2019 due to the disruption caused by the cyber-attack (2019) and the Covid pandemic (2020 – 2022) and the impact both events had on the phasing and ordering of the strategy and technology adoption. Similarly, the Finance & Infrastructure Committee reviews infrastructure updates and financial plans, however our review of papers noted that there is no explicit monitoring of Digital Strategy outcomes or delivery against the strategic themes being reported to the committee. However, from a review of Board and sub-committee papers published in recent years we noted that Board agendas include a standing item titled “Strategic Projects Update,” with the Board receiving updates on major initiatives across the College.

The strategy was reviewed more frequently, although less formally, by the then Head of ICT (now Director of Infrastructure), the then Learning and Digital Resources Manager (now Digital Services Manager) and Vice Principal, Curriculum & Attainment. Annual updates to the strategy were then reflected in College operational plans, with progress made with projects and initiatives linked to the digital objectives reported to SLT and the Executive Team.

As noted under Objective 1, the College has taken the deliberate decision not to include KPIs in the Digital Strategy as the College’s established practice is to assess implementation of strategies through the structures and processes that are in place for monitoring departmental operational plans, which reflect objectives and initiatives linked to strategic outcomes.

Objective 7 - There is regular reporting to the Executive Team and Board on progress to deliver the Digital Strategy and the effectiveness of the Strategy (continued).

To strengthen assurance, baseline measures and multi-year improvement, targets should be defined for each strategic theme which would allow the Executive Team and Board to assess effectiveness, not just activity. Example metrics would include:

Learners

- Digital inclusion (device access, training uptake)
- Online engagement (VLE analytics, attendance, AI learning tools usage)
- Accessibility compliance

Staff

- Digital competency by role
- CPD completion
- Adoption of digital pedagogies (e.g., AI-assisted assessment)

Systems & Infrastructure

- System performance
- Cyber posture (e.g. Cyber Assurance Framework maturity).

In addition, given AI's increasing strategic relevance, the Board should receive updates on: AI pilots and evaluation results, pedagogic implications (impact on feedback, assessment, curriculum design), academic integrity incidents related to AI, and AI governance (ethics, safety assessments, data protection impact assessments). No such reporting is present in the current governance evidence, despite the Strategy referencing AI.

Objective 7 - There is regular reporting to the Executive Team and Board on progress to deliver the Digital Strategy and the effectiveness of the Strategy (continued).

Observation	Risks	Recommendation	Management Response	
The Digital Strategy currently outlines ambitions and aspirations for digital delivery but does not contain measurable KPIs, and associated targets, to allow effective monitoring of delivery progress and/or impact.	Without defined KPIs and targets there is a risk that updates on digital delivery become descriptive rather than assurance-oriented, which limits the ability to make course corrections and to demonstrate progress and risk posture to the Audit & Risk Committee.	**R2** To improve Board reporting on implementation and the effectiveness of the Digital Strategy, the College should introduce: • a formal reporting cycle with standing Board agenda items which includes Digital Strategy progress; • a performance dashboard or balanced scorecard with appropriate KPIs and targets; • AI-specific reports and academic governance updates; and • benefits realisation reporting demonstrating impact, not just project status updates.	The current Estates Update to the Finance and Infrastructure Committee to be supplemented with a Digital Update incorporating key progress and reporting against Digital Strategy targets and outcomes. **To be actioned by:** Director of Infrastructure **No later than:** 30 June 2026	
			Grade	**3**

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

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

Agenda Item 7.2

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 3 March 2026

INTERNAL AUDIT

7.2 – 2025/26 PROGRESS REPORT

PAPER E

Dundee & Angus College

Internal Audit Progress Report

Audit & Risk Committee – 3 March 2026

Issued: 25 February 2026



Henderson Loggie

Internal Audit Progress Report
March 2026

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

Audit Area	Planned reporting date	Report status	Report Number	Overall Conclusion	Audit Committee	Comments
Annual Plan 2025/26	September 2025	Draft: 03/08/25 2nd Draft: 15/08/25 Final: 16/09/25	2026/01	N/A	16/09/25	
Budgetary Control	June 2026					Fieldwork due to commence on 13/04/26
Procurement and Creditors / Purchasing – Sustainable Procurement	September 2026					Fieldwork due to commence on 08/06/26
Digital Strategy Implementation	March 2026	Draft: 04/02/25 2nd Draft: 20/04/26 Final: 24/02/26	2026/02	**Satisfactory**	03/03/26	The audit reviewed the processes for the development of the new strategy and reviewed and assessed progress and outcomes relative to the strategy in place up to 2025.
Credits	December 2026					Fieldwork due to commence on 17/08/26

Audit Area	Planned reporting date	Report status	Report Number	Overall Conclusion	Audit Committee	Comments
Student Support Funds	December 2026					Fieldwork due to commence on 10/08/26
Follow Up Reviews	September 2026					Fieldwork due to commence on 06/07/26

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: 100 West George Street, G2 1PP **T:** 0141 471 9870

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

Agenda Item 7.3

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 3 March 2026

INTERNAL AUDIT

7.3 – FOLLOW UP SUMMARY

PAPER F

BOARD OF MANAGEMENT

Audit & Risk Committee
Tuesday 3 March 2025

Audit Recommendations Follow-up Summary

Paper for information

1. Introduction

This report provides an update on outstanding internal and external audit recommendations. These include a combination of actions:

- that are not yet due to be completed or;
- where the originally anticipated deadline has passed or;
- that are partially completed.

2. Recommendations

Members are asked to note the progress below and are asked to approve the revised implementation deadlines detailed in section 5 of this report.

3. Background

The following provides a summary of current progress in respect of audit recommendations up to 20 February 2026.

Audit Area	Rec. priority	Considered, but not agreed	Number agreed	Number fully implemented/ complete	Number partially implemented	Behind original implementation date	On target
2024/25 Student Activity	1	-	1	-	-	-	1
2024/25 Student Support Funds	2	-	2	2	-	-	-
Total		**0**	**3**	**2**	**0**	**0**	**1**

The recommendation priorities are detailed below. They denote the level of importance that should be given to each recommendation within the audit reports.

Priority 1	Material risk, requires attention of management and the Audit and Risk Committee
Priority 2	Significant risk, should be addressed by management
Priority 3	Minor risk or enhancement to efficiency and effectiveness

4. Progress to 20 February 2026

All outstanding recommendations are now fully implemented and were reported at the December 2025 meeting.

5. Link to Strategic Risk Register

Consideration of the outstanding actions is intended to provide Members with reassurance that actions for improvement are being progressed and addressed.

Progressing these Internal Audit and other outstanding actions will support the mitigation of the relevant risks identified within the Strategic Risk Register.

Authors: Steve Taylor, Vice Principal Support Services and Operations &
Nicky Anderson, Director of Finance
Executive Sponsor: Steve Taylor, Vice Principal Support Services and Operations

Appendix A

Outstanding Recommendations Update 20 February 2026

Year	Audit Area Report Title	Priority Action Grade	Report Grade	Action	Responsible Officer	Deadline	Progress (as at 20 February 2026
2025	2024/25 Student Activity Data	3	NA	**Systems and Procedures for Compilation of Returns Flexible / Work-Based Learning** **R1** The College should ensure evidence of progression and participation / engagement is retained to evidence eligibility of the Credits claimed for flexible / work-based learning students. Where curriculum staff identify that no evidence is available, or that students are no longer engaging, this should be notified to the Student Records team to ensure that the Credits are removed from the Credits claim.	Administration Project Manager, and Data Management Team Leader	31 July 2026	**On Target**
2025	2024/25 Student Support Funds	3	NA	**R1** The College should consider updating the Childcare Funding Support policy to include circumstances where the College may pay more than a 50% retainer to childcare providers during College holidays, reflecting current practice.	Accommodation & Childcare Officer	17 November 2025	**Completed** Update Implemented for 2026/27 policy
2025	2024/25 Student Support Funds	3	NA	**R2** Ensure that revised award letters are always issued, and copies retained, where reassessment of student awards is made during the year	Accommodation & Childcare Officer	17 November 2025	**Completed**

Agenda Item 8.0

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 3 March 2026

D&A RESPONSE TO SFC GOOD GOVERNANCE REPORT

PAPER G

BOARD OF MANAGEMENT

Audit & Risk Committee
Tuesday 3 March 2026

D&A College Reflections from the SFC Expectations of Good Governance Report

Paper for information

1. Background

Following on from the well documented issues impacting on the University of Dundee, the Scottish Funding Council published an outline of their expectations from the college and university sectors in respect of good governance practice.

In advance of this publication, the College had already completed its own self-evaluation of practice in respect of the matters arising at the University of Dundee, including an action plan relative to the lessons learned checklist outlined within the independent investigation report undertaken by Professor Pamela Gillies.

This further reflection and updated action plan pulls together the work undertaken in advance of the SFC publication alongside the key elements and recommendations made by SFC into a single update report and action plan.

2. SFC Expectations of Good Governance

The SFC expectations report provides a summary of college and university sector wide analysis of Governance Effectiveness Reviews (GER), previously called Externally Facilitated Effectiveness Reviews alongside the finding from the Professor Gillies report.

These reviews are also linked into a number of key points and recommendations to be considered as part of the wider SFC Outcomes Framework and Assurance Model in place for colleges and universities. This includes a number of recommendations in respect of future Governance Effectiveness Reviews.

In addition to a number of recommendations in respect of governance practice and activities the SFC report highlights two specific points for the college and university sectors to take into account and arising from the Gillies report as follows.

- The report notes that the dual role of the University Secretary as Chief Operating Officer is a potential conflict of interest, requiring careful management to ensure primary responsibility to the Chair of Court. This is not a common arrangement in the Scottish university sector, but instances outside of the University of Dundee do occur. SFC recognises that institutions are autonomous and that staffing matters are not for the SFC. Therefore, we encourage institutions to consider carefully whether this arrangement is appropriate and how best to secure the University Secretary's independence where a dual role is in place.

- Overlapping attendance, whether or not formal memberships, between Finance Committee and Audit Committee, which can undermine the crucial independence of the Audit Committee. Although the sector codes of governance do not explicitly prohibit this, the spirit of the codes and SFC's view is that impact on the independence of the Audit Committee is detrimental to its oversight and assurance function. We therefore encourage the relevant bodies that own the sector codes of governance to consider carefully whether this should continue to be permitted in future iterations of the codes.

Both of these points have already been identified within the D&A self-evaluation considered at the September 2025 meeting.

3. D&A Response

Following receipt of the SFC expectations document the College has undertaken the following steps to ensure that governance arrangements and College practice aligns with the practice outlined within the SFC expectations document.

3.1 Externally Facilitated Effectiveness Review

The Externally Facilitated Effectiveness Review approved by the Board at the December 2024 meeting has been reviewed and assessed relative to the requirements of the College Development Network (CDN) guidance and the additional comment made by SFC as part of the national review undertaken for SFC by independent consultants 'On Board'.

In terms of this assessment it is noted that:

a) The 2024 Externally Facilitated Effectiveness Review fully meets all of the requirements outlined within the relevant CDN guidance in place at the time of its completion.

b) The review is also assessed as meeting the further recommendations outlined by SFC within the September 2025 Expectations of Good Governance report as follows: includes:

- the timing and submission of the report to SFC
- the link and review in relation to the requirements of the CDN guidance and the Code of Good Governance; and
- the focus on evaluation and assurance, including specific assessment and comment on both risk management and financial governance.

The SFC expectations document highlights some recommendations to be developed in respect of future GER guidance for the college and university sectors and this will be reviewed when available as part of the next scheduled review. This includes reducing the timeframe between reviews to 3 years. Given this, it is anticipated that the next review will be scheduled for completion August - December 2027.

3.2 Professor Gillies 'Lessons Learned' Report

As part of the arrangements described in section 1 above the College undertook a review of practice against the recommendations detailed within the Gillies report. This review confirmed that governance arrangements at D&A adhered strongly to almost all of the checklist points. The points for development in respect of this report were highlighted to the board in September 2025 and will be progressed as agreed at that time.

4. Action Planning

The actions arising from the review of information relating to the situation at the University of Dundee, alongside the lessons learner report by Professor Gillies and the SFC Good Governance expectations report were shared with the Finance & Infrastructure and Audit & Risk Committees and then on to the Board (September 2025). An update on progress against these actions as at March 2026 is enclosed and work in respect of the small number of remaining actions will continue to be progressed. A further update on progress provided to the September 2026 Board meeting.

5. Link to Strategic Risk Register

Information in this report is intended to provide Board members with reassurance that actions and activities are being progressed and addressed that support the mitigation of the following risk within the Strategic Risk Register.

1.3 Difficulties or over commitment arising within large scale/national College led initiatives or projects impact negatively on:
- Ability of the College to meet key regional strategies/objectives
- Financial loss or unmanageable financial risk
- Reputational loss

2.2 Failure to achieve institutional sustainability

2.6 Demands of capital developments / maintenance impacts on financial sustainability or delivery of learning and/or services

3.7 Industrial Relations Problems (including industrial action)

Author and Executive Sponsor: Steve Taylor, Vice Principal Support Services and Operations

Appendix A

Education, Children and Young People Committee 19 March 2025 - University Financial Issues - Learning/considerations for D&A

External Challenges for Dundee University:	D&A Reflection / Action	Progress as at March 2026 Green = completed Amber = In progress Red = Limited / No progress
Cross subsidy with international tuition fees closing their funding gap	D&A Overseas fees are relatively small with minimal annual targets set. Student numbers are identified within activity reporting & assumed fee levels identified clearly within budget and monitored in monthly budget monitoring	Student numbers (credits) clearly planned and regularly monitored and action taken as necessary.
Changes in immigration policy/visa regulations had negative impact on international student recruitment	As above	Arrangements in place
Inflation	We are budgeting more clearly for known significant inflation areas and document our assumptions	Budget assumptions documented and subject to regular review
National Insurance increase	Scenario planning and active monitoring on potential areas of costs increases are included as part of budget development. We are budgeting more clearly for known significant inflation areas and document our assumptions	Budget assumptions documented and subject to regular review
Government, Cabinet and Minister / MSP understanding of how HE / education works, the role of governance / Boards and the funding models / constraints the sector/s work in	Continue to engage with key Government stakeholders through a range of opportunities to explain challenges; purposefully engage with stakeholders to discuss and explain impacts and needs. Continue to engage with Board Members individually and as a group to build understanding of College financial landscape.	Engagement arrangements in place and ‘lines to take’ shared.
Inadequate financial discipline and control	Budget planning and regular monitoring arrangements in place with identification and discussion on reasons for variances and remedial action as required. Improvements in budget setting process and regularity / clarity of monitoring are being progressed.	Documented budget setting and reporting arrangements in place. Management accounts shared with Board.

External Challenges for Dundee University:	D&A Reflection / Action	Progress as at March 2026 Green = completed Amber = In progress Red = Limited / No progress
Poor investment decisions, including digital decisions	Major investment decisions are considered at SLT and approval by Committee or Board above clear minimal thresholds. All infrastructure projects above defined thresholds are subject to post project evaluation. Infrastructure project management arrangements in place with clear escalation of issues / changes to full SLT. Board governance arrangements have been confirmed and enacted to support major infrastructure developments.	Arrangements in place
Weak compliance in financial control	Improvements in budget setting process and regularity / clarity of monitoring have been progressed, including monthly budget meetings between finance staff and key budget holders. Improvements in financial control and segregation of duties have been made as they were identified.	Documented budget setting and reporting arrangements in place. Finance process and systems enhancement plan being implemented
Lack of accountability	Budget holders and support staff know their responsibilities around budget management. Cultural change to fully own it. Clear rationale for budgets & understanding of budget assumptions and judgements so that variances can be explained and understood. Decision rationale and decision log for key SLT decisions is completed at each fortnightly in person SLT meeting. Monthly budget meetings between finance staff and key budget holders in place. Budget Holders are now responsible for projection of income/expenditure. Finance provide support, advice and challenge to ensure projections are as accurate as possible. Improvement in communications of Committee/Board decisions and rationale has been enacted within SLT meetings to ensure full SLT awareness.	Arrangements in place

External Challenges for Dundee University:	D&A Reflection / Action	Progress as at March 2026 Green = completed Amber = In progress Red = Limited / No progress
Inadequate oversight at Executive and Court levels of financial position, not least in ensuring strategic ambitions were underpinned by financial rigour.	Budget planning and monitoring arrangements in place with discussion on variances and remedial action as required. Budget monitoring presented for discussion on monthly basis at SLT and quarterly at each Finance and Infrastructure Committee and Board meeting. Further discussion / updating on the key financial info SLT want and need is in the finance improvement plan & on SLT agenda. Cipfa Finance for non-financial managers training has been scheduled for SLT. We will follow up this training to support translation to our own College finance landscape.	Arrangements in place. Cipfa training undertaken by SLT
Did not address longstanding challenge of structural deficit caused by an imbalance in the university being very research intensive & being cross subsidised by international student fees	3-to-5-year budgeting and Financial Strategy are part of our budget setting process. D&A history of longer-term financial planning and sustainability. A further update of the long-term financial strategy will be completed for December 2025.	Arrangements in place. Financial Strategy to be discussed/approved at the March 2026 Board meeting.
Lack of discipline on following through on savings decisions	All savings plans have named SLT lead with feedback on process and outcomes to SLT, Board and wider College. Efficiencies progress and financial implications are clear and included in budget monitoring reporting.	Arrangements in place
Was not appropriate oversight or challenge at Executive and Court level – Executive and Court “can only make decisions on the basis of the information you are given” and “dealt with the info they had”. “We were asking questions and told it was fine, and we had a high degree of confidence we could balance the budget”.	Financial training for (SLT) non-financial managers has been scheduled. Training on other key SLT remits for non-specialists is to be further discussed.	Cipfa training undertaken by SLT members

External Challenges for Dundee University:	D&A Reflection / Action	Progress as at March 2026 Green = completed Amber = In progress Red = Limited / No progress
Gaps in competence at leadership level	Financial training for (SLT) non-financial managers has been scheduled. Training on other key SLT remits for non-specialists is to be further discussed.	Cipfa training undertaken by SLT members
Top post graduate student numbers dropped by two thirds over 2 years – Had a serious impact on international student numbers	Key student application and recruitment data provided to and discussed at SLT alongside remedial steps being taken to deliver on targets. Information provided and highlighted to LT&Q Committee and Board. Activity issued highlighted as key risk area to A&R where required. All SLT members are aware of the need to be tuned into the wider impacts of changes in student (and other) activity. Links in year between operational and financial monitoring are noted.	Arrangements in place
Planned for 25% reduction in international student income but Dundee Uni actual closer to 50%	As above. We have documented our budget setting assumptions so that SLT understands them and review the reasons for in-year variances in budget monitoring reports	Documented budget setting and reporting arrangements in place.
Budget predicated on a large amount of savings being delivered that were then not delivered. Member – “we were not kept in the loop as to whether they (savings) were going to be delivered”.	Strict monitoring of savings/efficiencies assumptions in budget. All savings plans have named SLT lead with feedback on process and outcomes to SLT, Board and wider College.	Arrangements in place
July 23 cash balance £74m; July 24 cash balance reduced by £30m	Cashflow data and forecasts included in budget monitoring reports with discussion on variances and remedial action as required. Budget monitoring reports shared for discussion on monthly basis at SLT and each Finance and Infrastructure and Board meeting Further discussion / updating on the key financial info SLT want and need is in the finance improvement plan & on SLT agenda.	Documented budget setting and reporting arrangements in place. Management accounts (inc cash flow statement) discussed at F&I Committee and shared with Board.

Governance/Scrutiny Challenges for Dundee University	D&A Reflection / Action	Progress as at March 2026 Green = completed Amber = In progress Red = Limited / No progress
"False assumption we were breaking even when we were well-off break-even position"	Budget planning and monitoring arrangements in place with discussion on variances and remedial action as required. Budget monitoring shared for discussion on monthly basis at SLT and each Finance and Infrastructure and Board meeting. Committee and Board metrics show key areas of operational and financial activity in single report. Further discussion / updating on the key financial info SLT want and need is in finance improvement plan & on SLT agenda. Financial training for (SLT) non-financial managers has been scheduled. Training on other key SLT remits for non-specialists is to be further discussed.	Documented budget setting and reporting arrangements in place. Cipfa training undertaken by SLT
"We were concerned student numbers were dropping but robustly assured the path for growth was right" and "we accepted assurances we were still going to break even"	As above	Arrangements in place
"We were shown numbers where savings *were going to come in* across the organisation"	Strict monitoring of savings / efficiencies assumptions in budget. Details as above.	Arrangements in place
It was public information in 2023 that Nigerian currency dropped by 70% - why were these questions not asked? "You are not employed just to listen to the Finance Director, you have wider experience" "We were always assured there were compensatory savings which were going to finance this."	Horizon scanning – built into & inform operational, financial and risk monitoring. Data and assumptions underpinning key operational and financial plans is clearly documented and regularly reviewed	Budget assumptions documented and subject to regular review

Governance/Scrutiny Challenges for Dundee University	D&A Reflection / Action	Progress as at March 2026 Green = completed Amber = In progress Red = Limited / No progress
VPs would regularly attend Court, and that practice stopped in October 2023 when court received input from a limited set of people – (Principal, Depute Principal, Dir of Finance and Dir of HR - VP International Students did not attend.	Board Committee structure includes key SLT members in all Committees. Attendance of other key staff at Board where there are reports to be considered. Board are aware of, and practice constructive challenge, with this reviewed externally every 3 – 5 years and subject to Board evaluation.	Arrangements in place

Risk Management Challenges for Dundee University	D&A Reflection / Action	Progress as at March 2026 Green = completed Amber = In progress Red = Limited / No progress
Dundee Uni Key Risks 1. Cyber 2. Student experience 3. Staff experience 4. Research excellence 5. Financial sustainability Committee commented surprise Student recruitment was not a top risk and challenged SFC review of this. Committee also commented that the top risk on Risk Register is Cyber Security, not insolvency, even though Uni is now saying they are at risk of insolvency if they do not get liquidity funding	Strategic Risk Register is considered at each Committee meeting and in detail at each A&R Committee and 2 x annually by Board. Strategic Risk Register is built from College strategy and key operational requirements, with this informing regular audit plan scoping. Management accounts presented to Finance and Infrastructure Committee and Board include specific financial risk register to highlight key risks. Strategic Risks are reviewed by internal and external audit annually. Consider if we link risk management with operational and financial info well enough and regularly enough	Arrangements in place

Risk Management Challenges for Dundee University	D&A Reflection / Action	Progress as at March 2026 Green = completed Amber = In progress Red = Limited / No progress
The risk on international student numbers was “green until it went red”.	Student recruitment and activity data is shared with LT&Q and Board for transparency. Risk register update reports are shared biannually with the Board for transparency. Student numbers are identified within activity reporting & assumed fee levels identified clearly within budget setting and monitoring	Budget assumptions documented and subject to regular review. Student activity levels shared with Board.

Communication and Engagement Challenges for Dundee University	D&A Reflection / Action	Progress as at March 2026 Green = completed Amber = In progress Red = Limited / No progress
Recovery plan written with financial lens only – need to look more holistically & involve stakeholders	D&A Approach utilises key guiding principles to avoid ‘finance lens only’ approach. Guiding principles shared as part of savings exercises & discussed with unions.	Arrangements in place
Staff and union engagement – no co-design / co-production of recovery plan	As above. Savings planning incorporates open consultation arrangements for all staff including anonymous options where preferred. Clear arrangements in place for union consultation and engagement. Staff and union membership of Committees and Board. Previous examples elicited significant engagement and ideas to enhance options/approaches.	Arrangements in place
Senior staff in institution feel that decisions are locked down and feel it is still that way.	As above	Arrangements in place

Communication and Engagement Challenges for Dundee University	D&A Reflection / Action	Progress as at March 2026 Green = completed Amber = In progress Red = Limited / No progress
Staff concerned there is a culture that they cannot raise issues	As above	Arrangements in place
Senior Accountants knew there were issues – how were issues raised?	College operates an open door approach with open opportunities to raise concerns or provide feedback by any member of staff through the consultation inbox or anonymous hotline.	Arrangements in place
Committee asked, 'how many people' (headcount) affected by 632 FTE at risk number.	This data is not usually available at the start of the consultation period as FTE and headcount will change depending upon final decisions and VS applications.	Arrangements in place

Appendix B

Gillies Report Lessons Learned Checklist – Learning & Considerations for D&A

Gillies Report Lesson:	D&A Action	Progress as at March 2026 Green = completed Amber = In progress Red = Limited / No progress
1. The UEG, or equivalent, should actively consider and challenge the management accounts of the institution from a position of understanding of the totality of operations. There needs to be: a. An integrated income & expenditure, cashflow and balance sheet. b. Transparent cash reporting and cash management i.e. budgeted and allocated cash, unallocated operational cash. c. Control and reporting of capital projects in a way that is not separate to or segregated from the whole university financial reporting; and d. Transparent treasury management (especially if RCFs or loan finance is being used or is available);	SLT development scheduled to improve financial awareness for non-financial members.	Cipfa training undertaken by SLT
2. Active and critical appraisal and challenge of the Risk Register;	Continue current practice / approaches	Arrangements in place
3. Where there are obvious sensitivities (high risk rating) on student recruitment or financial sustainability, there should be regular updates to the Finance Committee (or equivalent) as a check and balance on budgets and forecasts;	Continue current practice / approaches	Arrangements in place

Gillies Report Lesson:	D&A Action	Progress as at March 2026 Green = completed Amber = In progress Red = Limited / No progress
4. Where there are loan or RCF covenants, depending on headroom these should be reported to UEG on a monthly or quarterly basis (in real time and based on the prior month's management accounts);	NA	NA – Colleges do not receive RCF Funding
5. There needs to be a culture (in practice) of the validity and value of questioning at all levels in a way that is without fear;	Continue current practice / approaches	Arrangements in place
6. The Chair of UEG (ordinarily the Principal) should be receptive to challenge;	Continue current practice / approaches	Arrangements in place
7. Curiosity should be encouraged (and whether at UEG, ARC, Finance Committee or Court) –one person's 'innocent question' ("I don't really understand but…") is often a catalyst for another person and the engagement leads to a far richer understanding and potentially uncovering of risks and issues that are worthy of debate;	Continue current practice / approaches	Arrangements in place
8. There should be clear and unambiguous early communication to Court and its committees regarding matters of importance to the whole university;	Continue current practice / approaches	Arrangements in place
9. Minutes should reflect challenges and not bias. They should also make clear how decisions were arrived at;	Continue current practice / approaches	Arrangements in place
10. Both the UEG and all members of Court should live the nine principles of public life;	Continue current practice / approaches	Arrangements in place

Gillies Report Lesson:	D&A Action	Progress as at March 2026 Green = completed Amber = In progress Red = Limited / No progress
11. The ARC should be able to stand back on any matter and review or enquire. The ARC should be the conscience of the University –the ultimate back stop for any matter.	Continue current practice / approaches	Arrangements in place
12. The University of Dundee had a practice of the Chair of FPC 'in attendance at ARC' and the Chair of ARC 'in attendance at FPC'. This overlap can appear functional in theory but from a best practice perspective often falls over in practice. The respective Chairs can readily get sucked into the detail and, in particular, the Chair of ARC returns to ARC with a pre-set and (likely) biased view. ARC should retain an element of independence in the overall governance and certainly absolute objectivity –this is readily lost. Best practice would be for no overlap –there will be members of the Executive that do attend both and the different lenses are helpful;	Continue current practice / approaches	Arrangements in place
13. In extremis, and it is seen (UK wide), institutions have a habit of forming a 'Committee of Chairs of Committees' or similar. In doing so, the Chair of ARC automatically loses their objectivity. The 'conscience of the University' is lost and objectivity over new and emerging risks can readily be overridden by a bias from prior (and detailed) consideration in a different context to ARC's considerations;	Chair of Audit & Risk Committee will not be involved in any future Board group established to respond to 'emergency' or 'in extremis' issues.	Arrangements in place
14. Papers must (not should) be provided in advance of meetings (and regardless of UEG, Court or its committees). Papers should be provided to give members time to read and consider in advance;	Continue current practice / approaches	Arrangements in place

Gillies Report Lesson:	D&A Action	Progress as at March 2026 Green = completed Amber = In progress Red = Limited / No progress
15. Papers should never be provided retrospectively, this is poor practice, regardless of the considered confidentiality of content good governance cannot happen in a vacuum and the Executive need to work within the Board and Committee structure of the University	Continue current practice / approaches	Arrangements in place
16. There are few instances in Scotland where the University Secretary (or equivalent) is the Chief Operating Officer of the institution, but this dual role can create conflicts of interest that are difficult to resolve in real time. While there will be a direct reporting line to the Chair of Court / Governing Body, there will also be a reporting line to the Principal. These two lines often work 'until they do not'. Care should be taken to ensure the primary responsibility is always to the Chair of Court;	Complete current review and enact Board decision.	Arrangements agreed September 2025 and awaiting implementation
17. The Finance Manual could usefully be updated for 'responsibilities of the Principal' and in particular in the role as 'Accountable Officer' and the responsibilities of Chair of Court;	Enact change as necessary once known.	Requirements not yet known.
18. A values-led University culture, which privileges transparency and accountability, is likely to actively support evidence-based collaborative decision making, integrity and openness to challenge and debate.	Continue current practice / approaches	Arrangements in place and outlined through People, Culture & Wellbeing Committee

Scottish Funding Council Expectations of Good Governance – Learning & Considerations for D&A

Scottish Funding Council Expectations of Good Governance	D&A Action	Progress as at March 2026 Green = completed Amber = In progress Red = Limited / No progress
1. There is a need for greater clarity around what assurances are needed or desired and this would provide benefit to SFC and to Governing Bodies – our guidance will support the sectors in understanding our expectations in this space. SFC expects that GER reports provide assurance over compliance with the relevant sector governance code in practice and that the governance arrangements in place at institutions are both adequate (i.e., designed appropriately) and effective (i.e., operating as intended). This includes effective scrutiny stemming from the culture of the governing body and committees being one that is curious, challenging and holds the executive to account. It also includes appropriate governance oversight of the institution's strategy, internal control and risk management framework and financial viability and sustainability. GER reports should be clear about the evidence on which assurances are based.	Timing and arrangements for Governance Effectiveness Reviews to confirm to revised future CDN/ Colleges Scotland / SFC guidance	Requirements not yet known
2. SFC recognises that institutions are autonomous and that staffing matters are not for the SFC. Therefore, we encourage institutions to consider carefully whether this arrangement is appropriate and how best to secure the University Secretary's independence where a dual role is in place.	Complete current review and enact Board decision.	Arrangements agreed and awaiting implementation

Scottish Funding Council Expectations of Good Governance	D&A Action	Progress as at March 2026 Green = completed Amber = In progress Red = Limited / No progress
3. Overlapping attendance, whether or not formal memberships, between Finance Committee and Audit Committee, which can undermine the crucial independence of the Audit Committee.		Arrangements in place

Agenda Item 9.0

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 3 March 2026

STRATEGIC RISK REGISTER **PAPER H**

(i) RISK REGISTER UPDATE
(ii) STRATEGIC RISK REGISTER

BOARD OF MANAGEMENT
Audit and Risk Committee
Tuesday 3 March 2026

Strategic Risk Register Update

Paper for approval

1. Strategic Risk Register

A copy of the March 2026 draft Strategic Risk Register is enclosed. This is noted for approval.

2. Financial Sustainability Risk

College Risk Management practice requires that any strategic risks that remain as Major or Fundamental post mitigation will be reported to the Committee at each meeting.

Following the decision of the Board of Management in March 2022 to recommend increasing the post mitigation risk in respect of future financial sustainability, the post mitigation likelihood was increased from 3 to 4 and the overall risk rating increased to 16. This moved this risk into the Major Risk (**Red**) category, and it is unlikely that this risk will be reduced in the near future.

The need to address the impact of 20% cuts in sector funding over the past 5 years, and the need to support areas of future opportunity and development, have been the subject of on-going discussion and review with the Board and has underpinned a range of savings plans and measures.

Details of the savings plan enacted to support future financial sustainability (including the impact of this on operations) have been discussed in detail at each Board Committee and the Board meetings in September and December 2025, with all targeted savings achieved and impacts carried forward to the forecasts for the 2026/27 annual budget and subsequent years. This input will continue for the foreseeable future.

The activities developed to address the funding cuts and financial sustainability risk cut across a range of areas, and arrangements are in place to support arrangements and minimise adverse risk in areas such as HR practice and industrial relations (Risks 3.3 and 3.7) and PR / publicity (Risk 3.5). These will remain under review, with the overall risk rolled into the higher level Financial Sustainability risk measure.

3. Reinforced Autoclaved Aerated Concrete (RAAC) Risk

An update on the most up to date picture regarding the RAAC present within the Kingsway Campus was provided for the Board in December 2025, with the RAAC present within the Kingsway tower and Construction/Engineering facilities continuing to represent a concern. All required mitigations remain in place relative to the specialist structural engineering advice received and a structural survey completed in October 2025 has not highlighted any significant change in the condition of the RAAC present within campus accommodation.

Given the passage of time since the initial three to five year timeframe was given around the need to remove the risks associated with RAAC (with these now on a one to three year timeframe) further work has been progressed to develop an alternative plan should exit be required from one or more campus facilities.

This work would require decant into commercial facilities within the city and would require additional set up costs of c£2 million and recurrent funding of c£1.3 million to support the commissioning and operation of these alternative facilities.

The pressing timeline and indicative costs have been shared with SFC, who are aware that – should this risk crystalise- additional emergency funding support would be necessary to mitigate the impact. Details of these risks and costs have been shared with the Scottish Funding Council and Scottish Government.

Updates have also been shared with the Board on the future infrastructure vision for the whole College estate, including future developments to remove RAAC from our estate. As this work progresses further detailed updates will be provided via the Finance and Infrastructure Committee and full Board.

The next specialist survey is due to be completed in October 2026.

4. 2025/26 Credit Activity

Close management of 2025/26 credit activity levels is being undertaken given the reductions in activity to support financial sustainability. The reductions being progressed in-year in 2025/26 (predominantly reductions in the normal January start programme) are expected to fall within the 2% lower activity threshold available to the College (96,341 credits) and discussions are on-going with the Scottish Funding Council over sector activity levels and thresholds for 2026/2027.

Arrangements for future years are also under discussion nationally, including a more significant review of the funding methodology and approach.

5. HR/People Risks

As with any savings plan, restructure or other significant period of change, the risk associated with the engagement, motivation and goodwill of staff can be adversely impacted. Consideration and mitigation of this risk has been at the forefront of the recent savings plan and has been an important feature of the approach adopted to consult and involve staff in the savings exercise.

Whilst these steps are always extremely challenging, staff engagement through the various steps has been encouraging and feedback around the arrangements has been positive and solution focused in most instances.

As staff have left the College through Voluntary Severance or non-replacement of vacancies, teams have taken steps to review and amend priorities and ways of working to accommodate the reduced staffing.

The People element of the savings plan arrangements and the approaches adopted have been subject to significant discussion within the People, Culture and Wellbeing Committee.

Arrangements to progress the biennial staff survey will continue, with this scheduled for March / April 2026. The results of the survey will be used to inform future organisation development and communication arrangements as well as focusing on specific issued or feedback at team level.

Outcomes from the staff survey will be shared with the People, Culture and Wellbeing Committee in May and September 2026.

6. Governance Expectations & Risks

A further detailed review has been undertaken in respect of the heightened focus on governance (especially financial governance) arising from the issues at the University of Dundee and subsequent SFC governance asks. This review is included as item 8 on the meeting agenda.

7. Strategic Risk Register

No changes have been proposed to the Strategic Risk register at this time.

8. Approvals

In respect of the above information approval for the following actions is sought.

- Consider and approve or otherwise the proposed changes to Risk matrix scoring to reflect Risk Appetite.
- Note the updates provided and approval of the Strategic Risk Register

Author and Executive Sponsor: Steve Taylor, Vice Principal Support Services and Operations

DUNDEE AND ANGUS COLLEGE



STRATEGIC RISK REGISTER

2025 - 2026

As at March 2026

Post Holders					Score	Impact	Likelihood
	ELT	Executive Leadership Team	Prin	Principal			
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	DirSE	Director of Student Experience	2	Minor	Unlikely
	VPSO	Vice Principal Support & Operations	DirFin	Director of Finance	3	Significant	Possible
	VPCP	Vice Principal Curriculum & Partnerships	HoE	Head of Estates	4	Major	Probable
	DirInf	Director of Infrastructure	Chair	Chair of the Board of Management	5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Lead Responsibility
1 Strategic and Structural										
1.1 LT&Q	Failure of College strategy to meet the needs of the D&A Region and/or national priorities (eg Employability, DYW, attainment, articulation)	4	4	16	• Robust strategic planning • Effective environmental scanning • Strong partnerships • Clear links between strategy and practice • Concerted demands for increased activity levels	4	1	4 ↔	• Robust monitoring via **OF&AM Framework** • Clear performance metrics • Amendment of strategic direction/ plans • Rolling curriculum review	Principal & Chair
1.2 Board	College may be disadvantaged by changes to either UK or Scottish Government policies	4	3	12	• Effective environmental scanning • Negotiation/influence at national level	4	2	8 ↔	• Review of changes and amendment of strategic direction/plans • Financial strategy sensitivities	Principal & Chair
1.3 Board	Difficulties or over commitment arising within large scale/national College led initiatives or projects impact negatively on: • Ability of the College to meet key regional strategies/objectives • Financial loss or unmanageable financial risk • Reputational loss	4	3	12	• Effective project/activity management in place • Clear governance structures • Project/initiative finances clearly incorporated within College financial strategy and plans • End of project and exit/contingency planning	3	2	6 ↔	• Regular project updates at Executive/Board level • Monitoring of project activities, plans and outcomes • Clear project Management arrangements in place • Budget reporting and management	Principal, VPCP

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Blue (1-3) = Minor Risk; Green (4 – 8) = Moderate Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk. Board Risk Appetite for the above risks is assessed as Open with risks scored as major being subject to regular scrutiny and risks scored as fundamental subject to review at every meeting.

Post Holders						Score	Impact	Likelihood
	ELT	Executive Leadership Team	Prin	Principal		1	Routine	Remote
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment		2	Minor	Unlikely
	Board	Board of Management	DirSE	Director of Student Experience		2	Minor	Unlikely
	VPSO	Vice Principal Support & Operations	DirFin	Director of Finance		3	Significant	Possible
	VPCP	Vice Principal Curriculum & Partnerships	HoE	Head of Estates		4	Major	Probable
	DirInf	Director of Infrastructure	Chair	Chair of the Board of Management		5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS: Risks	Impact	Likelihood	Score	TREATMENT: Mitigation Actions	Impact	Likelihood	Score	POST MITIGATION EVALUATION: Monitoring	Lead Responsibility
1 Strategic and Structural (cont)										
1.4 Board	College disadvantaged as a result of changes arising from major national educational body reviews: SFC, SQA, EdS	3	3	9	• Negotiation/influence at national level • Review of activities/ projects and response to new opportunities	3	1	3 ↔	• Robust monitoring via OA • Amendment of strategic direction/ plans • Rolling curriculum review	Principal
1.5 Board	Failure of D&A plans and activities to deliver on required carbon reductions and sustainability actions necessary to meet national targets and achieve College climate emergency ambitions.	4	3	12	• Robust CEAP in place • Multiple strands of activity/action • Embedding sustainable practices in normal activity and ways of working • Clear links between strategy and practice • Planned investment in carbon reduction • Sustainable procurement	3	2	6 ↔	• Robust monitoring and reporting of CEAP at SLT and Board level • Clear performance metrics • Amendment of strategic direction/ plans • Monitoring of scope 3 emissions	VPSO, DirInf, HoE

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Blue (1-3) = Minor Risk; Green (4 – 8) = Moderate Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk. Board Risk Appetite for the above risks is assessed as Open with risks scored as major being subject to regular scrutiny and risks scored as fundamental subject to review at every meeting.

Post Holders					Score	Impact	Likelihood
	ELT	Executive Leadership Team	Prin	Principal			
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	DirSE	Director of Student Experience	2	Minor	Unlikely
	VPSO	Vice Principal Support & Operations	DirFin	Director of Finance	3	Significant	Possible
	VPCP	Vice Principal Curriculum & Partnerships	HoE	Head of Estates	4	Major	Probable
	DirInf	Director of Infrastructure	Chair	Chair of the Board of Management	5	Critical	Very Likely

	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
Risk Number & Committee	**Risks**	**Impact**	**Likelihood**	**Score**	**Mitigation Actions**	**Impact**	**Likelihood**	**Score**	**Monitoring**	**Responsibility**
2 Financial										
2.1 **F&I**	Change in Funding Body and/or Funding Methodology and Allocation – Reduction or restriction in Funding	3	4	12	• Negotiation/influence at national level • Contingency plans for amended funding levels or requirements	3	2	8 ↔	• Advance modelling of new funding requirements, methodologies, and allocations • Monitoring impact of changes • Amendment of strategic or operational direction / plans • Financial strategy sensitivities	VPSO
2.2 **F&I**	Failure to achieve institutional sustainability	5	4	20	• Protection of funding through dialogue with SFC and SG • Input to create sector 'flexibilities' • Robust annual budget-setting and multi-year financial strategic planning • Effective budgetary control • Where required, swift action to implement savings	4	4	16 ↔	• Monthly monitoring of budgets • Regular review of financial strategy and non-core income sensitivity • Effective use of sector 'flexibilities' to support sustainability • Amendment of strategic priorities and timing to align with funding levels • Review and amendment of activity and budget planning to address over/under performance against activity (credit) target • Detailed monitoring of savings programmes • Detailed monitoring & management of CDEL/RDEL risks	VPSO

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: **Blue** (1-3) = Minor Risk; Green (4 – 8) = Moderate Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk. Board Risk Appetite for the above risks is assessed as Open with risks scored as major being subject to regular scrutiny and risks scored as fundamental subject to review at every meeting.

Post Holders					Score	Impact	Likelihood
	ELT	Executive Leadership Team	Prin	Principal			
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	DirSE	Director of Student Experience	2	Minor	Unlikely
	VPSO	Vice Principal Support & Operations	DirFin	Director of Finance	3	Significant	Possible
	VPCP	Vice Principal Curriculum & Partnerships	HoE	Head of Estates	4	Major	Probable
	DirInf	Director of Infrastructure	Chair	Chair of the Board of Management	5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Lead Responsibility
2 Financial (cont)										
2.3 **F&I**	National outcomes on salaries and conditions of service outstrip ability to pay	4	4	16	• Influence within Employers Association • Management of staffing expenditures	4	3	12 ↔	• Expenditure modelling • On-going discussions with staff • Financial strategy sensitivities • Workforce planning	VPSO
2.4 **A&R**	Financial Fraud	3	3	9	• Strong financial controls: segregation of duties and review of transactions. • Review of impact of any changes in structure or duties • Whistleblowing arrangements	2	2	4 ↔	• Continuous review of financial controls • Internal Audit programme	VPSO
2.5 **F&I**	D&A Foundation refuses/withholds funding for key College priorities	5	3	15	• On-going dialogue with Foundation Trustees • Appropriate bid arrangements in place	3	2	6 ↔	• Monitor and advise Board of Management	Prin & VPSO
2.6 **F&I**	Demands of capital developments / maintenance impacts on financial sustainability or delivery of learning and/or services	4	4	16	• Multi-year estates strategy and capital planning • Lobbying of SFC on capital and backlog maintenance funding • Planning for D&A Foundation bids	4	3	12 ↔	• Monitoring of capital plans and expenditures • Regular review of capital plans/timescales relative to funds	VPSO

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: **Blue** (1-3) = Minor Risk; Green (4 – 8) = Moderate Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk. Board Risk Appetite for the above risks is assessed as Open with risks scored as major being subject to regular scrutiny and risks scored as fundamental subject to review at every meeting.

Post Holders					Score	Impact	Likelihood
	ELT	Executive Leadership Team	Prin	Principal			
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	DirSE	Director of Student Experience	2	Minor	Unlikely
	VPSO	Vice Principal Support & Operations	DirFin	Director of Finance	3	Significant	Possible
	VPCP	Vice Principal Curriculum & Partnerships	HoE	Head of Estates	4	Major	Probable
	DirInf	Director of Infrastructure	Chair	Chair of the Board of Management	5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Lead Responsibility
2 Financial (cont)										
2.7 F&P	Failure to reach aspirational standards in financial strategy, budgeting, planning or audit	4	3	12	• Clear financial strategy aligning to College priorities and FFR • Appropriate zero based budgeting in place • Regular, timeous and accurate budget monitoring • Effective audit planning and completion	3	2	6 ↔	• Regular review of financial priorities to align / realign with available funds • Comprehensive monitoring and reporting of all finances • 'Real time' budget and data analysis underpins decision making • Effective audit planning and completion	VPSO DirFin

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: **Blue** (1-3) = Minor Risk; Green (4 – 8) = Moderate Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk. Board Risk Appetite for the above risks is assessed as Open with risks scored as major being subject to regular scrutiny and risks scored as fundamental subject to review at every meeting.

Post Holders					Score	Impact	Likelihood
	ELT	Executive Leadership Team	Prin	Principal			
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	DirSE	Director of Student Experience	2	Minor	Unlikely
	VPSO	Vice Principal Support & Operations	DirFin	Director of Finance	3	Significant	Possible
	VPCP	Vice Principal Curriculum & Partnerships	HoE	Head of Estates	4	Major	Probable
	DirInf	Director of Infrastructure	Chair	Chair of the Board of Management	5	Critical	Very Likely

	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
Risk Number & Committee	**Risks**	**Impact**	**Likelihood**	**Score**	**Mitigation Actions**	**Impact**	**Likelihood**	**Score**	**Monitoring**	**Lead Responsibility**
3 People and Performance										
3.1 **LT&Q**	Failure to reach aspirational standards in learning, teaching, and service delivery	4	3	12	• Clear quality arrangements and priority actions • Continuous self-evaluation and action planning • Rigorous CPD arrangements in place • Regular classroom observation and learner feedback arrangements	2	2	4 ↔	• Comprehensive monitoring of key PIs and student/staff feedback • Regular Stop and Review events • External review and validation findings	VPCP, VPSO DirC&A
3.2 **LT&Q**	Failure to achieve/maintain compliance arrangements, e.g. contracts; awarding bodies; audit.	4	3	12	• Robust strategic planning and monitoring • Effective environmental scanning • Strong partnerships • Clear links between strategy and practice • Concerted demands for increased activity levels	2	2	4 ↔	• Effective internal monitoring/review/verification arrangements • External review findings	VPCP, VPSO
3.3 **A&R**	Legal actions; serious accident; incident or civil/criminal breach	4	4	16	• Adherence to legislative and good practice requirements • Positive Union relations and staff communication • Effective management development programmes	3	2	6 ↔	• Monitoring and reporting in key areas – eg H&S, equalities, employee engagement • Continuous professional development • Internal audit programme • Staff surveys	Prin, VPSO, HoE

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Blue (1-3) = Minor Risk; Green (4 – 8) = Moderate Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk. Board Risk Appetite for the above risks is assessed as Open with risks scored as major being subject to regular scrutiny and risks scored as fundamental subject to review at every meeting.

Post Holders					Score	Impact	Likelihood
	ELT	Executive Leadership Team	Prin	Principal	1	Routine	Remote
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	2	Minor	Unlikely
	Board	Board of Management	DirSE	Director of Student Experience	3	Significant	Possible
	VPSO	Vice Principal Support & Operations	DirFin	Director of Finance	4	Major	Probable
	VPCP	Vice Principal Curriculum & Partnerships	HoE	Head of Estates	5	Critical	Very Likely
	DirInf	Director of Infrastructure	Chair	Chair of the Board of Management			

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Lead Responsibility
3 People and Performance (cont.)										
3.4 P,C&W	Failure to meet the aspirational standards in respect of the health, safety, wellbeing and development of staff and students	4	4	16 12	• Clear and proactive approaches to managing and promoting health, safety, and wellbeing • Continuous self-evaluation and action planning • Rigorous CPD arrangements in place • Regular staff and learner feedback arrangements	3	2	6 ↔	• Regular employee engagement monitoring • Open communication with staff • Comprehensive monitoring of key PIs and student/staff feedback • Regular union/management dialogue	VPSO
3.5 Board	Reputational Risk – Loss of reputation with key stakeholders	4	2	8	• Marketing strategy • Reputation plan • Positive marketing approaches	3	2	6 ↔	• Stakeholder engagement • Social media monitoring arrangements	VPCP, DirC&A
3.6 P,C&W	National bargaining outcomes impact adversely on College operations, activity, and flexibility	4	4	16	• Influence within Employers Association • Management of bargaining outcomes and implementation	4	3	12 ↔	• Positive union relations and staff communication • On-going discussions with staff • Innovation in approaches	VPSO, VPC&A

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Blue (1-3) = Minor Risk; Green (4 – 8) = Moderate Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk. Board Risk Appetite for the above risks is assessed as Open with risks scored as major being subject to regular scrutiny and risks scored as fundamental subject to review at every meeting.

Post Holders					Score	Impact	Likelihood
	ELT	Executive Leadership Team	Prin	Principal			
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	DirSE	Director of Student Experience	2	Minor	Unlikely
	VPSO	Vice Principal Support & Operations	DirFin	Director of Finance	3	Significant	Possible
	VPCP	Vice Principal Curriculum & Partnerships	HoE	Head of Estates	4	Major	Probable
	DirInf	Director of Infrastructure	Chair	Chair of the Board of Management	5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Lead Responsibility
3 People and Performance (cont.)										
3.7 **P,C&W**	Industrial Relations Problems (including industrial action)	4	5	20	• Adherence to legislative and good practice requirements • Positive Union relations and staff communication • Effective management development programmes • Industrial action continuity planning	4	2	8 ↔	• Regular union/management dialogue • Regular employee engagement monitoring • Open communication with staff • Industrial action continuity planning	VPSO
3.8 **A&R**	Significant Breach of data security / data protection	5	4	20	• Effective management of GDPR compliance • Mandatory staff CPD and awareness raising on data protection (relative to role)	4	2	8 ↔	• Active data protection monitoring and auditing • Effective information and data security policies in operation • Regular data security monitoring/testing • GDPR Action Plan • Staff CPD	VPCP, DirInf
3.9 **P,C&W**	Failure to meet Prevent and related obligations	5	3	15	• Prevent training • Staff awareness and contingency planning • Engagement/practice sharing with local agencies	5	1	5 ↔	• Business Continuity Plan including scenario testing • Information sharing with local agencies	VPCP, VPSO

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: **Blue** (1-3) = Minor Risk; Green (4 – 8) = Moderate Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk. Board Risk Appetite for the above risks is assessed as Open with risks scored as major being subject to regular scrutiny and risks scored as fundamental subject to review at every meeting.

Post Holders					Score	Impact	Likelihood
	ELT	Executive Leadership Team	Prin	Principal			
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	DirSE	Director of Student Experience	2	Minor	Unlikely
	VPSO	Vice Principal Support & Operations	DirFin	Director of Finance	3	Significant	Possible
	VPCP	Vice Principal Curriculum & Partnerships	HoE	Head of Estates	4	Major	Probable
	DirInf	Director of Infrastructure	Chair	Chair of the Board of Management	5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS: Risks	Impact	Likelihood	Score	TREATMENT: Mitigation Actions	POST MITIGATION EVALUATION: Impact	Likelihood	Score	Monitoring	Lead Responsibility
3 People and Performance (cont.)										
3.10 **P,C&W**	College arrangements do not minimise risk associated with Modern Slavery	4	2	8	• Clear and compliant procurement arrangements and procedures • Staff identity checking arrangements and use of PVG.	3	1	3 ↔	• Annual procurement monitoring/reporting • Regular employee engagement monitoring • Open communication with staff	VPCP, VPSO
3.11 **Board**	Failure to plan or respond adequately to future pandemic illness.	5	3	15	• Monitoring and rapid response to WHO and UK/Scottish Government information and alerts • Maintenance of COVID-19 good practice approaches to inform future use • Effective business continuity planning in place	4	2	8 ↔	• Pandemic readiness / response included in business continuity plan reviews and testing • COVID/Pandemic Response Group in place • Active monitoring and rapid adoption of pandemic guidance / control measures	Principal

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Blue (1-3) = Minor Risk; Green (4 – 8) = Moderate Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk. Board Risk Appetite for the above risks is assessed as Open with risks scored as major being subject to regular scrutiny and risks scored as fundamental subject to review at every meeting.

Post Holders					Score	Impact	Likelihood
	ELT	Executive Leadership Team	Prin	Principal	1	Routine	Remote
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	2	Minor	Unlikely
	Board	Board of Management	DirSE	Director of Student Experience	3	Significant	Possible
	VPSO	Vice Principal Support & Operations	DirFin	Director of Finance	4	Major	Probable
	VPCP	Vice Principal Curriculum & Partnerships	HoE	Head of Estates	5	Critical	Very Likely
	DirInf	Director of Infrastructure	Chair	Chair of the Board of Management			

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Lead Responsibility
3 People and Performance (cont.)										
3.12 P,C&W	Failure to attract, engage, retain or develop appropriately qualified staff.	4	3	12	• Clear People Strategy and Workforce Planning in place • Positive Union relations and staff communication • Effective management development & CPD programmes • Positive recruitment approaches and monitoring	4	1	4 ↔	• Absence & turnover monitoring • Exit interviews • Regular staff surveys 7 survey responding • Monitoring and responding to staff concerns, union issues and employee relations concerns	VPSO

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: **Blue** (1-3) = Minor Risk; Green (4 – 8) = Moderate Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk. Board Risk Appetite for the above risks is assessed as Open with risks scored as major being subject to regular scrutiny and risks scored as fundamental subject to review at every meeting.

Post Holders					Score	Impact	Likelihood
	ELT	Executive Leadership Team	Prin	Principal			
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	DirSE	Director of Student Experience	2	Minor	Unlikely
	VPSO	Vice Principal Support & Operations	DirFin	Director of Finance	3	Significant	Possible
	VPCP	Vice Principal Curriculum & Partnerships	HoE	Head of Estates	4	Major	Probable
	DirInf	Director of Infrastructure	Chair	Chair of the Board of Management	5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility
4 Infrastructure										
4.1 **A&R**	Major Disasters – eg Fire, MIS Failure, Failure of Emergency Procedures, RAAC or similar infrastructure failure	5	3	15	• Sound systems of administration • Clear fire and disaster recovery arrangements • Staff CPD	5	1	5 ↔	• Business Continuity Plan including scenario testing	Principal, VPSO, DirInf
4.2 **F&I**	Failure to achieve ambitions of Digital strategy; strategy and development is ineffective	4	3	12	• Planning, careful phasing of changes to processes and systems • Effective management of ICT arrangements • Clear investment plan	3	2	6 ↔	• Regular review/reporting on milestones, systems effectiveness etc • Regular CPD	VPSO, DirInf
4.3 **A&R**	Significant breach of ICT/Cyber security resulting in loss of service sufficient to impact College student / staff outcomes	4	3	12	• Effective management of ICT arrangements • Active ICT/data security monitoring and cyber security policy	4	2	8 ↔	• Staff CPD on cyber security issues • Regular security monitoring/testing • Cyber resilience plan	VPSO, DirInf
4.4 **A&R**	ICT infrastructure fails to support effective data security / data protection	5	3	15	• Effective infrastructure and systems design and implementation • Effective management of ICT arrangements and GDPR compliance	4	2	8 ↔	• Active data protection monitoring and auditing • Effective information and data security policies in operation • Regular data security monitoring/testing	VPSO, DirInf

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: **Blue** (1-3) = Minor Risk; Green (4 – 8) = Moderate Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk. Board Risk Appetite for the above risks is assessed as Open with risks scored as major being subject to regular scrutiny and risks scored as fundamental subject to review at every meeting.

Post Holders					Score	Impact	Likelihood
	ELT	Executive Leadership Team	Prin	Principal			
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	DirSE	Director of Student Experience	2	Minor	Unlikely
	VPSO	Vice Principal Support & Operations	DirFin	Director of Finance	3	Significant	Possible
	VPCP	Vice Principal Curriculum & Partnerships	HoE	Head of Estates	4	Major	Probable
	DirInf	Director of Infrastructure	Chair	Chair of the Board of Management	5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS: Risks	Impact	Likelihood	Score	TREATMENT: Mitigation Actions	POST MITIGATION EVALUATION: Impact	Likelihood	Score	Monitoring	Responsibility
4 Infrastructure (cont)										
4.5 **F&I**	Lack of investment in ageing / beyond serviceable life infrastructure (inc RAAC, Asbestos and M&E failure concerns) impacts on financial sustainability and/or delivery of learning and/or services	4	5	20	• Creation of long-term infrastructure principles and vision • Multi-year estates strategy and capital planning • Lobbying of SG and SFC on capital and backlog maintenance funding • Identification of alternative funding routes • Planning for D&A Foundation bids	4	4	16 ↔	• Lobbying of SG, SFC and UK Gov on campus vision and needs • Prioritisation of capital plans and expenditures • Regular review of capital plans/timescales relative to funds	Principal VPSO

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Blue (1-3) = Minor Risk; Green (4 – 8) = Moderate Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk. Board Risk Appetite for the above risks is assessed as Open with risks scored as major being subject to regular scrutiny and risks scored as fundamental subject to review at every meeting.