BOARD OF MANAGEMENT
Audit and Risk Committee

Tuesday 4 March 2025 at 5.00pm **Room K-TO-624, Kingsway Campus** (MS Teams option available)

AGENDA

1.	**MEETING WITH AUDITORS & COMMITTEE MEMBERS WITH BOARD AND F&P COMMITTEE CHAIRS**		
2.	**WELCOME (approx. 5.30)**		
3.	**APOLOGIES**		
4.	**DECLARATIONS OF CONNECTION & INTEREST**		
5.	**MINUTE OF THE PREVIOUS MEETING** – 3 December 2024	Paper A for approval	
6.	**MATTERS ARISING**	Paper B for noting	
7.	**HEFISTIS CYBER RISK & MATURITY REPORT**	Paper C for approval	DR
8.	**EXTERNAL AUDIT**		
	8.1. Forvis Mazars Annual Audit Report	Paper D to follow	MS
	8.2. Financial Statements for the year ended 31 July 2024	Paper E to follow	NA
9.	**INTERNAL AUDIT**		
	9.1. Staff Development	Paper F for approval	HL
	9.2. Progress Report	Paper G for information	HL
	9.3. Procurement & Creditors Audit Progress	Paper H for information	NA
	9.4. Follow Up Summary	Paper I for information	NA/ST
10.	**RISK MANAGEMENT POLICY**	Paper J for approval	ST
	(i) Risk Policy Update		
	(ii) Risk Appetite Session Outcomes		
	(iii) Risk Management Policy		
11.	**STRATEGIC RISK REGISTER**		
	(i) Risk Register Update	Paper K for approval	ST
	(ii) Strategic Risk Register		
12.	**GARDYNE THEATRE ISSUE**	Paper L for information	ST
13.	**DATE OF NEXT MEETING** – Tuesday 3 June 2025 at 5.00pm in Room K-TO-624, Kingsway Campus		

Agenda Item 5.0

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 4 March 2025

MINUTE OF THE PREVIOUS MEETING **PAPER A**

BOARD OF MANAGEMENT

Audit and Risk Committee

Tuesday 3 December 2024 at 4.30pm in room K-TO-604 and via MS Teams

Minute of the Audit & Risk Committee meeting held on Tuesday 3 December 2024 at 4.30pm in Room K-TO-604 Kingsway Campus and via Microsoft Teams.

PRESENT: Helen Honeyman (Chair Audit)
Derek Smith
Margo Williamson
Matthew Beattie
Ged Bell

IN ATTENDANCE: Stuart Inglis (Henderson Loggie)
Laurie O'Donnell
Michael Speight (Forvis Mazars)
Bridget Mauro (Forvis Mazars)
S Taylor (Vice Principal Support and Organisation)
Nicky Anderson (Director of Finance)
P Muir (Board Administrator)

1. WELCOME

H Honeyman welcomed members of the Audit & Risk Committee and L O'Donnell as an observer.

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

2. APOLOGIES

Apologies were noted from R McLellan, S Middleton, D Archibald and J Buchanan.

3. DECLARATIONS OF INTEREST OR CONNECTION

S Inglis declared an interest in relation to the Procurement of Internal Audit services and withdrew from the meeting for that item.

4. MINUTE OF THE PREVIOUS MEETING

The minutes of the Audit and Risk Committee meeting held on 17 September 2024 were approved as an accurate record.

5. MATTERS ARISING

The matters arising have been progressed as noted.

6. AUDIT & RISK COMMITTEE ANNUAL REPORT TO THE BOARD

The Audit & Risk Committee Annual Report to the Board was discussed in detail.
H Honeyman noted discussion within the auditor meeting regarding changes, timescales, and delays being faced. She noted discomfort with the current position, acknowledging no fault of individuals, but highlighting the possible impact on the Audit sign-off date.

While appreciating the ongoing work and handovers, she stressed the importance of avoiding similar tight deadlines in the future and requested these concerns to be reflected in the report.

M Williamson enquired about the progress of the audit sign-off process and the likelihood of meeting the deadline.

N Anderson provided an update on the accounts and adjustments, noting that further checks by M Speight (Forvis Mazars) with the technical department were required.

M Speight provided an update on the status of the audit progress, highlighting the technical treatment of the job evaluation funding was a significant hurdle. While 95% of the work was on track, final approvals and backpay accrual figures still required completion. M Speight stated ongoing discussions with the technical team were being held to address these issues, with confidence that the audit would be sufficiently complete pending the final steps. He acknowledged the associated risks but assured the Committee that contingency measures were in place to ensure the audit's completion within the required timeframe.

H Honeyman acknowledged the team's work but reiterated the importance of flagging risks to the Board. She also queried contingency plans if the sign-off timeline was not met and the implications for funding.

S Taylor noted that contingency arrangements were possible if needed to allow sign off to be completed after the Board meeting. If required lateness of the final reports could be signalled to SFC, but this would be avoided if at all possible. M Speight noted that with proper communication, a delay would not pose a major problem.

S Inglis emphasised the need to update the highlighted areas within the Audit & Risk Annual report to the Board to reflect the final reports to be approved. This was noted.

The draft report was approved (with amendment as noted) for submission to the Board.
H Honeyman and S Taylor to progress.

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.

S Inglis highlighted one issue which was the allocation of credits on a course where 110 Credits recorded in UNIT-e did not align with the Credits outlined in the course framework or those actually undertaken by students. However, S Inglis confirmed that this had no impact overall.

S Inglish noted the average credits claimed for full-time students slightly exceeded the Funding Council guidance, with ongoing discussions which confirmed no issues or impact for the current year.

S Taylor highlighted the importance of conversations with SFC around average credits and noted that these additional credits were group tutor and guidance time for students, which were essential elements of successful programmes. S Taylor also noted that the average credit figure had reduced, with closer alignment.

The positive report was approved.

7.2. STUDENT SUPPORT FUNDS

S Inglis summarised the report on the discretionary, hardship, bursary, childcare, and EMA funds. It was confirmed that these returns were simplified and submitted to SAAS without reservation.

The report received a clean certificate, with one point noted for future improvement. The report was then welcomed and approved by the committee.

H Honeyman thanked everyone involved for their work in achieving such positive outcomes

7.3. SPORTS CENTRE BUSINESS PROCESS REVIEW

S Inglis introduced and highlighted the report, which was prepared by D Archibald.

S Inglis emphasised that the review's objective was to identify and eliminate inefficiencies within current processes, while also contributing to a broader evaluation by the College of the commercialisation and overall effectiveness of the Sports Centre operations at Gardyne Campus.

S Inglis noted that meetings were conducted with stakeholders, including staff from the Sports Centre, the HR Manager, the Head of Estates, and the Head of Finance. Additional meetings were held with customers and other relevant parties. Through these discussions, opportunities were identified for improving the performance in the operating model for the Sports Centre.

S Inglis highlighted key findings and included several recommendations to enhance effectiveness. S Inglis stated two high-priority recommendations were related to access security and maintaining safe staff levels. Management confirmed that Risk assessments concerning potential staffing level risks have been reviewed, and appropriate arrangements put in place at the time of the fieldwork for the report in early 2024. Residual areas for improvement have been identified, with a completion date set for 31 January 2025.

The remainder of the report included four medium-priority and one lower-priority recommendation. These related to areas such as Sports Centre charges, equipment, and building maintenance.

M Williamson remarked that the report was thorough and enjoyable to read, with no surprises for management. She emphasised the importance of Health and Safety and access, recognising the assurance provided within these areas.

H Honeyman asked about the partial acceptance of recommendations related to safe staffing levels, querying whether shutting the facility down was ever considered.

S Inglis clarified that, during discussions, assurance was provided that the identified risks, such as all staff being called away while pool supervision was required, were effectively managed and unlikely to materialise.

S Taylor added that the partial acceptance referred to issues had already been addressed and noted that the final elements of the recommendation did not relate to Health and Safety concerns.

The report was approved.

7.4. FOLLOW UP SUMMARY

S Taylor presented the summary and noted that work was progressing well in terms of Audit recommendations.

H Honeyman noted that it was a request of the committee that Procurement be reviewed again in 12 months. This would be added into the 2025/26 audit schedule. **S Taylor to progress.**

H Honeyman thanked S Taylor for the update and noted that the Committee was pleased to see the progress made.

7.5. PROCUREMENT AND CREDITORS AUDIT UPDATE

N Anderson summarised the update on recommendations from the Procurement and Creditors Audit.

N Anderson highlighted that the procurement strategy was included on the agenda for the Finance & Property Committee. She noted that a draft procurement policy and procurement authorisation process had been prepared, along with proposed changes to procurement thresholds. These documents will be circulated shortly, pending approval.

N Anderson discussed the "No PO, No Pay" policy which was reviewed, and communication to staff regarding the importance of purchase orders (POs) is underway, with a plan in place to improve enforcement.

N Anderson noted that it is not possible to build authorisation system controls into the P2P process, but the existing measures provide adequate control over changes to bank details.

H Honeyman acknowledged the challenges in fully implementing the "No PO, No Pay" policy and welcomed the desire to move closer to this where possible.

L O'Donnell highlighted the importance of fostering a supportive culture for staff, ensuring they are empowered to do their jobs while working to find the right balance of support and protection.

The update was welcomed.

8. DATA REPORTING

S Taylor reported that there had been no reportable data breaches. He noted that the annual report on cyber security and resilience would be presented at the March 2025 meeting.

Following recent staffing changes S Taylor highlighted that the College would transition to a shared service arrangement through HEFETIS for data protection support. This change was noted.

9. INTERNAL AUDIT PROCUREMENT

S Inglis left the meeting for this item.

N Anderson provided a summary of the Internal Audit Procurement process, noting that a mini-competition and interviews with potential suppliers would be conducted in February – March 2025. The outcome of this process will be presented to the Audit and Risk Committee in June 2025.

10. STRATEGIC RISK REGISTER

S Taylor provided a summary, highlighting key areas of risk. Financial sustainability was noted as a significant concern and is scheduled for discussion at the Finance and Property Committee meeting.

S Taylor highlighted those credits claimed from different funding pots-based on Scottish Funding Council (SFC) and SFE funding, which operate in arrears- had resulted in some ESF funds being reclaimed. Although additional funds were previously allocated, some of these had had to be returned due to these adjustments.

S Taylor stated work on the risk appetite session is progressing and will be progressed for the March 2025 meeting. There were no changes signaled to current Strategic Risks.

The paper was approved.

11. DATE OF NEXT MEETING

Tuesday 4 March 2025 at 5.00pm in room K-TO-624, Kingsway Campus.

Action Point Summary

Action	Responsibility	Date
Audit & Risk Annual report to be updated for submission to the Board	S Taylor	13 December 2024
Procurement and creditors audit to be included in the 2025/26 audit plan.	S Taylor	September 2025

Agenda Item 6.0

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 4 March 2024

MATTERS ARISING **PAPER B**

BOARD OF MANAGEMENT
Audit & Risk Committee
Tuesday 4 March 2025

Matters Arising

Paper B for information

The following actions were noted from the Tuesday 3 December 2024 Audit & Risk Committee meeting.

Agenda Item No	Action	Current status	Open / Closed
6.0	A&R Annual report to be updated for submission to the Board S Taylor	Completed	Closed
9.0	Internal Audit Services Procurement to progress S Taylor/ N Anderson	Scheduled for 17 June 2025	Open

The following actions were noted from the Tuesday 17 September 2024 Audit & Risk Committee meeting.

Agenda Item No	Action	Current status	Open / Closed
9.0	Review of Strategic Risk Register scoring to be completed S Taylor	Included in Agenda	Closed

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

Agenda Item 7.0

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 4 March 2025

HEFISTIS CYBER RISK & MATURITY REPORT PAPER C

TLP:AMBER+STRICT

2024

DUNDEE AND ANGUS COLLEGE

Dundee and Angus College: 2024 Annual Information and Cyber Security Report

PSCRF V2 REPORT

CISO OFFICE

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

Contents

Executive Summary

Dundee and Angus College has aligned itself with the Scottish Governments Public Sector Cyber Resilience Framework (PSCRF) to improve Information and Cyber Security (ICS) maturity and risk posture. Doing so strengthens the goals and progressive aims of information and cyber security. As a result, Dundee and Angus College are better aligned with not only the reporting requirements of the Scottish Government against progress in meeting the requirements of the framework but also the changes taking place within the public sector environment where the PSCRF is a core component.

The organisation's security maturity assessment reveals both areas of strength and opportunities for improvement across various domains. The report covers the period of January to October 2024. Baseline reporting has been updated and the latest Scottish government guidance applied, with the recommendation that ongoing deeper dives and TTX activity to evidence, identify and assure progress, efficiency opportunities and enhance risk management in information and cybersecurity be performed on progressive basis across the college over 2024-25.

It should be noted that following updated guidance from Scottish Government the cybersecurity scorecard has been re-calibrated to include a “partial” compliance weighting of 50% where current activities are reported as ongoing but not yet complete. This recognises the significant ongoing activity applied across the college to strengthen and improve the information and cyber security posture, upgrade digital services and integrate best practices thoroughly across the entire organisation.

The organisation demonstrates strengths – a B rating or above, in over 88% of the assessed areas – all assessed areas reflect a rating of D or above.

Mean tier 1 compliance scoring is 89.4 %.

Mean tier 2 (Advanced) compliance scoring is 84.3 %.

The overall compliance (Tiers 1 and 2 combined) gives a weighted scoring of 86.8%

This current information and cyber security position for the college compared against the PSCRF V2 standard is therefore above the current 60% minimum (basic) compliance level and 88% within advanced levels. This is an outstanding result.

However, opportunity for further improvement has been identified over 2024 in 5 areas against the latest PSCRF standard which may be considered for implementation over the remainder of 2024 and over 2025. (See recommendations section) Considering and prioritising these areas for further improvement through completion of existing improvement activities and targeted initiatives will be critical to enhancing the organisation's combined security posture and resilience to a fully advanced level against cyber threats.

The current college position, whilst containing some elements of work in progress, 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 not only maintain but also provide evidenced and auditable ongoing ICS improvement.

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, ensuring that we meet the necessary regulatory requirements and adhere to industry standards.

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

The assessment of the organisation's security maturity is based on the Scottish Government's Public Sector Cyber Resilience Framework. This framework provides a structured approach for evaluating and improving cyber resilience across various domains, tailored specifically for the public sector but applicable to organisations across different sectors and industries.

The Scottish Government has produced an updated version of the PSCRF (v2) that is scheduled for release this year. HEFESTIS has been involved in the feedback groups and helped shape the final requirements of the framework. HEFESTIS has further been permitted by the Scottish Government to use the new framework prior to its release and is in the processes of transitioning all members to it. The changes to the framework include the reduction of duplication, removal of outdated requirements and the addition of new requirement where needed.

The framework is built upon internationally recognised standards and best practices, including the UK Governments Network and Information Systems Cyber Assurance Framework, the National Cyber Security Centre (NCSC) 10 Steps and the ISO/IEC 27001 standard for information security management systems. It encompasses a comprehensive set of criteria and guidelines for assessing key areas of cyber resilience, including governance, risk management, technical controls, incident response, and awareness and training.

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.

Key aspects of the methodology

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 Scottish Government's Public Sector Cyber Resilience 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.

Security Maturity Scorecard: 89.4%

Using a scorecard format to present security maturity levels across different domains or categories provides a structured and aesthetic vehicle to communicate complex information. Presented are the Scorecards for Dundee and Angus College as measured against the requirements within the Scottish Government produced PSCRF.

It is the stated aim from the Scottish Government that all organisations should adopt the controls in Tier 1; those that are subject to the NIS Regulations, such as health boards, and those holding sensitive data such as universities and colleges should fulfil all controls in Tier 1 and those in Tier 2.

Tier 1 Scorecard

Manage	Protect	Detect	Respond & Recover
A Organisational Governance	B Information Security Management	A Incident Detection	A Incident Management
B Risk Management	A People		A Business Continuity
C Supplier Management	C Service Resilience		
A Asset Management	A Access Control		
	B Media Management		
	A Environmental Security		
	B Physical Building Security		
	A System Management		
	A Operational Security		
	A Network Security		

Tier 2 Scorecard 84.3%

Manage		Protect		Detect		Respond & Recover	
A	Organisational Governance	C	Information Security Management	A	Incident Detection	A	Incident Management
B	Risk Management	A	People			A	Business Continuity
D	Supplier Management	B	Service Resilience				
B	Asset Management	A	Access Control				
		C	Media Management				
		A	Environmental Security				
		C	Physical Building Security				
		A	System Management				
		A	Operational Security				
		B	Network Security				

Combined Tier Scorecard 86.8%

Manage	Protect	Detect	Respond & Recover
A Organisational Governance	B Information Security Management	A Incident Detection	A Incident Management
B Risk Management	A People		A Business Continuity
D Supplier Management	C Service Resilience		
A Asset Management	A Access Control		
	B Media Management		
	A Environmental Security		
	B Physical Building Security		
	A System Management		
	A Operational Security		
	B Network Security		

Detailed Analysis

The following section of the report examines in more detail the assessment areas as defined in the Scottish Governments Public Sector Cyber Resilience Framework and the organisations position as described by the response to the requirements and the managing controls that are currently in place and evidenced.

It is structured to highlight the organisational groups that holds accountability or responsibility for the areas that exist within their remit.

It should be noted that the comparison between year 2024 and 2023 are between the combined Tier 1 and Tier 2 PSCRFv2 for 2024 and the 2023 assessed areas from last year's report – any estimated scores are based on direct indicative comparison with the combined ISO levels used for previous reporting cycles.

This takes into consideration the changes to the framework in terms of added or removed requirements but is not a "like for like" comparison against previous reports which were based on a different set of ICS standards and controls.

The following section follows the PSCRF Categories by duty area and numbered category (1 to 17) for consistency. Each area is graded against it's combined score for Tiers 1 and 2. Summarised analysis for each category is provided.

Senior Management

"Senior Management" refers to the upper echelon of executives within an organisation, typically holding top leadership positions responsible for making crucial decisions and setting the overall direction of the company.

Overall, senior management plays a critical role in steering the organisation towards success by providing leadership, setting strategic direction, and ensuring effective management of resources and operations.

1. Organisational Governance

Appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the organisation's network and information systems.

A	A score of A signifies that the organisation has implemented robust measures to protect organisational structures policies and processes and systematically manage security risks to the organisation's network and information systems. This indicates a recognition of the importance of governance in ensuring effective security management. The organisation has documented policies and procedures in place. There is clarity regarding roles and responsibilities within the governance framework, however there could be room for improvement in terms of ensuring accountability and communication channels for addressing security concerns at all levels of the organisation. Additionally, while there is evidential alignment between security objectives and overall business goals, there remains room for continuous improvement in ensuring maintenance of excellent ongoing levels of organisational management.

2. Risk Management

Appropriate steps are in place to identify, assess and understand security risks to the network and information systems. This includes an overall organisational approach to risk management.

B	A score of B indicates that the organisation possesses a solid foundation in understanding risk management principles. It has established processes and procedures for identifying, assessing, and prioritising risks across various aspects of its operations. The organisation conducts regular ICS risk assessments, which involve evaluating both internal and external factors that could potentially impact its objectives. However, while the organisation demonstrates a mature understanding of risk management concepts, there may be room for improvement in terms of implementing proactive risk mitigation strategies. While risks are being identified and assessed, there may be opportunities to embed the effectiveness of the risk response strategies and mechanisms in place. This could involve investing existing capabilities to address high-priority ICS risks more widely across the organisation, whilst continuously evaluating and adjusting risk management processes to adapt to changing threats and circumstances.

Procurement / Contracts / Legal

"Procurement / Contracts / Legal" refers to a set of interrelated functions within an organisation that deal with acquiring goods, services, and legal support.

3. Supplier Management

The organisation understands and manages security risks that arise as a result of dependencies on external suppliers and third-party services.

D	Achieving a score of D indicates that further understanding and implementation of key principles and practices may be required, though there may be areas for refinement and enhancement concerning organisation-wide relationships with external suppliers. There may be limited visibility into suppliers' security practices, exposing the organisation to potential risks in the supply chain. Inadequate due diligence during supplier selection and limited ongoing monitoring of supplier performance may contribute to vulnerabilities and compliance issues. *It is noted that use of technologies enhancing supplier assessment processes, establishing clear security requirements, and improving communication channels are being introduced to reinforce the crucial steps needed to mitigate risks associated with third-party dependencies and strengthen the organisation's overall security posture.

Technical Team

A "Technical Team" is a group of professionals within an organisation who possess specialised skills and knowledge in various technical domains. Members of a technical team typically collaborate to design, develop, implement, and maintain the technological aspects of products, services, or systems within the organisation.

The composition of a technical team can vary depending on the organisation's industry and needs, but it often includes individuals with expertise in software development, hardware engineering, IT infrastructure, systems analysis, and other technical disciplines.

The technical team plays a vital role in supporting and advancing the organisation's technological infrastructure, contributing to its overall success.

4. Asset Management

Everything required to deliver, maintain, or support networks and information systems and services is determined and understood.

🟩 A	A score of A shows that the organisation has implemented robust measures to manage its assets, indicating an advanced level of maturity in this area. The organisation has established processes and systems in place for identifying, tracking, and securing its assets effectively. This includes both physical assets, such as equipment and facilities, as well as digital assets, such as software, data and intellectual property. Moreover, there are clear and developing policies and procedures governing asset management practices, ensuring consistency and accountability across the organisation. Overall, achieving a score of A in Asset Management signifies a proactive and diligent approach to safeguarding the organisation's assets, which is essential for maintaining operational efficiency and mitigating security risks.

5. Information Security Management

Proportionate security measures are in place to protect information, data, services, and systems from cyber-attack.

B	Achieving a score of B indicates a solid understanding and implementation of key principles and practices, though there may be areas for refinement and enhancement. The organisation has established frameworks and procedures for managing information security. While these measures provide a foundational level of security, there may be opportunities to further strengthen the organisation's posture. This could involve improvements in areas such as regular security assessments and audits, and the implementation of more advanced security technologies and controls to address emerging threats. By continually reviewing and updating its information security management practices, the organisation can better protect sensitive data, mitigate risks, and ensure compliance with relevant regulations and standards, thus further bolstering its overall security maturity.

6. Service Resilience

Network and information systems are designed to be resilient to cyber security and operational adverse incidents.

C	Achieving a score of C shows that the organisation has implemented foundational measures for ensuring the continuity and resilience of its services, though there may be areas for improvement. The organisation has mechanisms in place to identify critical services, assess potential risks to their availability, and develop strategies for mitigating disruptions. While these efforts contribute to a level of preparedness, there may be opportunities to enhance resilience further. This could involve conducting more comprehensive risk assessments, implementing cloud based segmentation more widely or failover mechanisms (remaining network), and enhancing communication and coordination strategies for responding to incidents. By strengthening its service resilience capabilities, the organisation can minimise the impact of disruptions, maintain business continuity, and sustain customer confidence, thereby advancing its overall security maturity.

7. Access Control

Access to information, services and systems is controlled, managed, and monitored through policies and procedures.

A	In Access Control, achieving a score of A shows that the organisation has implemented robust measures to control access to its resources and data. There are established policies and procedures in place for managing user authentication, authorisation, and permissions. However, there may remain incremental areas for improvement to enhance access control practices further. There may be a need to refine access control policies to ensure that access rights are granted on a need-to-know basis, limiting the risk of unauthorised access. Regular monitoring and auditing of access permissions can also help identify and address any discrepancies or potential security gaps. By continuously improving access control measures, the organisation can better protect sensitive information, prevent data breaches, and maintain the confidentiality, integrity, and availability of its resources.

8. Media Management

Fixed and portable storage media and devices are managed, and data / information is appropriately protected.

B	Achieving a score of B indicates a solid understanding and implementation of key principles and practices, though there may be areas for refinement and enhancement for managing media, such as digital and physical storage devices, which store sensitive information. This score suggests that there are limited controls in place to protect against unauthorised access, loss, or theft of media containing confidential/sensitive data on remote, unmanaged devices including student devices. Consequently, the organisation may be at a heightened risk of data breaches, leakage of sensitive information, and non-compliance with data protection regulations. Improvements should be found to implement robust media management policies and procedures, including encryption, access controls, and secure disposal methods. Additionally, staff/student training and awareness programs should be prioritised to educate employees about the importance of media security and their role in safeguarding sensitive data.

9. System Management

Information systems are protected from cyber-attack throughout their lifecycle.

A	In System Management, achieving a score of A indicates that the organisation has established advanced measures to safeguard its day-to-day operations against security threats and risks for managing its IT systems. While there are robust systems in place for deploying, monitoring, and maintaining IT infrastructure, these processes will require ongoing maintenance to ensure the highest levels of ICS in the longer term. There may remain gaps in areas such as configuration management, and system monitoring, leaving the organisation vulnerable to security threats and operational disruptions. To improve system management practices, the organisation may consider ongoing continuous improvement with regular review of automated systems management tools, reinforcing existing clear procedures for system configuration and change management, and enhancing monitoring capabilities to detect and respond to potential issues proactively.

10. Operational Security

Appropriate technical and organisational measures are in place to protect systems and digital services from cyber attack.

A	In Operational Security, achieving a score of A indicates that the organisation has established advanced measures to safeguard its day-to-day operations against security threats and risks. There are established policies, procedures, and controls in place to protect against malware, ensure the integrity of data and systems, and email security. However, there may be areas for incremental continuous improvement to enhance operational security practices even further. This could involve implementing data loss prevention technologies, conducting regular security assessments and audits, and enhancing alert response capabilities to address security incidents effectively. By continuously refining operational security measures, the organisation can continue to mitigate risks, prevent disruptions to business operations, and maintain the confidentiality, integrity, and availability of its assets and resources, thus maintaining its overall security posture.

11. Network Security

Appropriate measures are in place to ensure the protection of information systems and information held in networks.

B	A score of B shows that the organisation has implemented robust measures to protect its network infrastructure from security threats, but there are areas for improvement. While there are comprehensive network security controls in place, such as firewalls and patch management, these measures may not be fully optimised or comprehensive. There are gaps in areas such as network segmentation, and encryption, leaving the organisation vulnerable to cyberattacks and data breaches. To improve network security, the organisation should consider implementing more robust network security technologies and controls for remaining network estate and continuing cloud migration in the medium term. Additionally, regular vulnerability assessments and penetration testing can help identify and address weaknesses within the network infrastructure.

12. Incident Detection

Organisations shall have in place monitoring systems and procedures to detect cyber-attacks.

A	In Incident Detection, achieving a score of A shows that the organisation has implemented effective mechanisms for detecting security incidents, though there may be areas for improvement. There are established processes and tools in place to monitor network traffic, system logs, and other sources of security-related data for signs of suspicious activity. However, these detection mechanisms may require ongoing attention to ensure mitigation of any risks potentially leading to delayed detection or missed incidents. To enhance incident detection capabilities, the organisation should consider ongoing monitoring of and enhancement to advanced threat detection technologies, such as ATP and Security Information and Event Management (SIEM) systems and employing automated threat intelligence feeds, such as MISP to identify emerging threats proactively.

13. Incident Management

Well-defined incident management processes are in place, documented and regularly tested.

A	In Incident Management, achieving a score of A shows that the organisation has implemented advanced and effective mechanisms for responding to security incidents, there remain areas requiring improvement. This score indicates that incident response procedures are comprehensive, minimising delays or inadequacies in addressing security breaches and incidents. There may remain incremental gaps in areas such as incident prioritisation, communication protocols, and coordination among response teams which should be regularly monitored and updated to ensure they remain up to date. To continuously enhance incident management capabilities, the organisation should focus on refining incident response plans, conducting regular training exercises, and reinforcing clear escalation procedures. Additionally, regularly optimising incident response automation tools and leveraging external incident response services will help streamline response efforts and improve overall effectiveness.

14. Business Continuity

Information security continuity shall be embedded in the organisation's business continuity management systems.

A	In Business Continuity, achieving a score of A indicates that the organisation has implemented highly effective mechanisms for continuity planning with comprehensive strategies and measures to ensure business resilience. While there is robust continuity planning in place, it can always benefit from being frequently exercised and regularly tested. To maintain and continuously improve business continuity practices, the organisation should consider regularly updating business impact assessments to ensure relevance and quality of critical processes and dependencies, similarly regularly updating the detailed continuity plans that outline procedures for maintaining essential functions during disruptions and ensuring the ongoing quality of content relating to clear communication channels and roles and responsibilities for response teams. Additionally, regular testing and exercises of continuity plans are essential to validate their effectiveness in the longer term

Human Resources / Organisational Development

"Human Resources (HR) / Organisational Development (OD)" refers to the combined field of activities within an organisation that focuses on managing its human capital and optimising the overall effectiveness of the workforce. These two functions, while distinct, often work in tandem to create a productive and healthy work environment.

While HR primarily focuses on the administrative aspects of managing personnel, OD takes a broader view, concentrating on the development and improvement of the entire organisation. Together, these functions play a crucial role in ensuring that an organisation's human resources are aligned with its strategic goals and that the workplace fosters growth, collaboration, and continuous improvement.

15. People

The organisation has policies and procedures in place to ensure staff and contractors are screened, trained, and know their security responsibilities.

A	The organisation demonstrates a commendable and advanced level of maturity in people awareness and training. Effective measures have been undertaken to educate personnel about security best practices and their roles in safeguarding organisational assets. However, there is still requirement for ongoing revision and review to maintain high awareness levels and training initiatives. Considerations may include developing tailored training programmes, conducting regular awareness campaigns, providing targeted training for specific roles or departments, and incorporating security awareness into the organisational culture. Strengthening people awareness and training capabilities is essential for building a resilient human firewall, reducing the risk of human error, and fostering a security-conscious workforce. Investing in people awareness and training will continuously contribute to enhancing the organisation's overall cybersecurity posture and resilience against emerging threats.

Facilities / Estates

"Facilities / Estates" refers to the management and maintenance of physical assets and infrastructure within an organisation. These terms are often used interchangeably, encompassing responsibilities for buildings, grounds, and other physical facilities.

Together, Facilities and Estates management ensure that an organisation's physical assets are well-maintained, safe, and contribute to the overall effectiveness of its operations. This can involve a wide range of tasks, from day-to-day maintenance and security to long-term strategic planning for real estate assets. The specific responsibilities may vary depending on the nature and scale of the organisation.

16. Environmental Security

Appropriate procedures are in place to reduce the risks from internal and external environmental threats and hazards.

A	In Environmental Security, achieving a score of A reflects the organisation's robust measures to address environmental factors that could compromise security objectives. This indicates a high level of maturity in recognising and mitigating risks related to the environment in which the organisation operates. This suggests strength in measures to protect organisational assets and data from environmental threats such as natural disasters, power resilience, and environmental hazards. Strong environmental security capabilities are essential for safeguarding organisational resilience and ensuring the continuity of operations in the face of environmental disruptions.

17. Physical / Building Security

To prevent unauthorised physical access, damage and interference with the organisation's information systems and services.

B	A score of B signifies that the organisation has implemented effective measures to protect its physical premises against unauthorised access, intrusion, and other security threats. This score reflects a good level of maturity in addressing physical security concerns, demonstrating a comprehensive approach to safeguarding the organisation's assets, employees, students, and visitors. There are stringent access control measures in place, including physical barriers, electronic access systems, and surveillance technologies, to control entry and monitor activities within the premises effectively. However, improvement may be gained from ensuring that all of these controls are effectively applied and consistently controlled across the organisation. Additionally, consideration may be given to ensuring the organisation has established security protocols for managing visitors, securing sensitive areas, and responding to security incidents promptly.

Recommendations

Dundee and Angus College is well progressed within, but not yet quite at the end of a programme of digital and organisational improvement over 2023-24. The organisation, with HEFESTIS, has transitioned not only to the new PSCRF V2 criteria but also to a stronger level of information and cyber security assurance provided through evidenced responses.

Consistent reporting, control and resilience can continue to be achieved through recurrent engagement to explore each of the assessment areas in depth. Ongoing maintenance of processes, policies, systems and procedures with frequent security exercising are an excellent means of achieving and maintaining advanced security posture.

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 with additional enhancement activity prioritised on a risk benefit basis.
For now, we would recommend that the following ICS areas, especially where beneficial activity is already underway, be completed and quality assured including security by design, so that additional controls are put in place and strengthened over 2024 – 25 to satisfy the security requirements of the college and improve organisational cyber resilience.

- Supplier Management
- Service resilience
- Media Management
- Network Security
- Physical Building Security

It is through ongoing assurance with focused deep dives in these areas that we will be able to evaluate the ongoing improvement activities and work streams needed, not only to meet the requirements but to also provide the evidence for that claim. This evidence should continue to be managed and made available to internal and external audit as proof that requirements are being met and improvement achieved.

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 must now be extended into areas where it has been shown to need additional or ongoing resource application and attention. These efforts must 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 in and dedication to information and cyber security endeavours is imperative for any organisation aiming to manage risks, safeguard assets, ensure compliance, uphold brand reputation, and maintain operational continuity. By dedicating resources to continuous improvement, ICS challenges can be addressed proactively and the college stakeholders position themselves for sustained success in an increasingly complex digital landscape.

Appendices

APP01 PSCRF Summary Scoring

PDF
Assessment Summary.pdf

APP02 Maturity Posture

PDF
Maturity Posture.pdf

APP 03 Risk Posture

PDF
Risk Posture.pdf

PSCRF V2.0 Maturity Compliance Summary

DUTY	CATEGORY	Number of controls		
AREA	Sub-Category	Tier 1	Tier 2	Combined
Senior Management	**1. ORGANISATIONAL GOVERNANCE (Total Number of controls in each category)**	**7**	**13**	**20**
	1.1 Governance Framework (number of compliant controls in each sub-category)	4	2.5	6.5
	1.2 Leadership & responsibility	2	4	6
	1.3 Adoption Audit and Assurance of Security standards	1	6	7
	1.4 Regulatory Compliance	0	0	0
	% Compliance	**100.00**	**96.15**	**98.08**
	2. RISK MANAGEMENT	**18**	**15**	**33**
	2.1 Policy & Processes	4	4.5	8.5
	2.2 Cyber / Information Risk Assessment	3	1.5	4.5
	2.3 Risk Treatment & Tolerance	1.5	3	4.5
	2.4 Risk Governance	7.5	2.5	10
	% Compliance	**88.89**	**76.67**	**82.78**
Procurement / Contracts / Legal	**3. SUPPLIER MANAGEMENT**	**24**	**9**	**33**
	3.1 Supply Chain Assurance	3	0	3
	3.2 Roles and Responsibilities	0.5	0.5	1
	3.3 Access control	1	1.5	2.5
	3.4 Security in Procurements	0.5	1.5	2
	3.5 Security in Cloud Services	7.5	0.5	8
	% Compliance	**52.08**	**44.44**	**48.26**
	4. ASSET MANAGEMENT	**7**	**8**	**15**
	4.1 Hardware Assets	2	6	8
	4.2 Software Assets	2.5	0	2.5
	4.3 Infrastructure management	2	1	3
	% Compliance	**92.86**	**87.50**	**90.18**
	5. INFORMATION SECURITY MANAGEMENT	**23**	**19**	**42**
	5.1 Security Policy & Processes	7	3	10
	5.2 Lifecycle Management	3	1	4
	5.3 Storage	1	1.5	2.5
	5.4 Information / Data Classification	0.5	1	1.5
	5.5 Information Asset Register	3	3	6
	5.6 Information / Data Transfer Controls	4	2	6
	% Compliance	**80.43**	**60.53**	**70.48**

Technical Team	**6. SERVICES RESILIENCE**	**1**	**6**	**7**
	6.1 Services Resilience Systems are appropriately segregated and resource limitations are mitigated	0.5	5	5.5
	% Compliance	**50.00**	**83.33**	**66.67**
	7. ACCESS CONTROL	**21**	**10**	**31**
	7.1 Account Management	7	0	7
	7.2 Identity Authentication	4	3	7
	7.3 Privilege Management	6	6	12
	7.4 Administrator Account Management	4	1	5
	% Compliance	**100.00**	**100.00**	**100.00**
	8. MEDIA MANAGEMENT	**15**	**6**	**21**
	8.1 Storage Media	4	0	4
	8.2 Mobile Media / Devices	8.5	2	10.5
	8.3 Cryptography	0.5	1.5	2
	% Compliance	**86.67**	**58.33**	**72.50**
	9. SYSTEM MANAGEMENT	**15**	**18**	**33**
	9.1 Secure Configuration	8	4	12
	9.2 Secure Design / Development	1	7	8
	9.3 Change Control Procedures	3	3	6
	9.4 System Testing	3	4	7
	% Compliance	**100.00**	**100.00**	**100.00**
	10. OPERATIONAL SECURITY	**24**	**8**	**32**
	10.1 Malware Policies & Protection	5	0	5
	10.2 Email Security.	4	0	4
	10.3 Application Security	3.5	0	3.5
	10.4 Vulnerability Management & Scanning	5	2	7
	10.5 Data Exfiltration Monitoring	1	1	2
	10.6 Browser Management	2	0	2
	10.7 Monitor / Audit User Activity	3	5	8
	% Compliance	**97.92**	**100.00**	**98.96**
	11. NETWORK SECURITY	**30**	**14**	**44**
	11.1 Patch Management	5	0	5
	11.2 End-Point Device Management	3	3	6
	11.3 Internal Segregation	2	3	5
	11.4 Wireless Security	3	0	3
	11.5 Boundary / Firewall Management	7	1	8
	11. 6 Administrator Control	3	1	4
	11.7 IP & DNS Management Organisational IP ranges are known, recorded and managed;	3	0	3
	11.8 IoT Management Internet-facing devices should be securely configured and segregated as a	2	3	5
	% Compliance	**93.33**	**78.57**	**85.95**
	12. INCIDENT DETECTION	**9**	**10**	**19**
	12.1 Detection Capability	1	7	8
	12.2 Security Monitoring	8	3	11
	% Compliance	**100.00**	**100.00**	**100.00**

	13. INCIDENT MANAGEMENT	**20**	**7**	**27**
	13.1 Incident Response Protocol	9.5	3.5	13
	13.2 Incident Reporting Procedure	5	0	5
	13.3 Post-Incident Review & Learning	5	3	8
	% Compliance	**97.50**	**92.86**	**95.18**
	14. BUSINESS CONTINUITY	**10**	**24**	**34**
	14.1 Data Recovery Capability	1	1	2
	14.2 Back up Policies & Procedures	3	3	6
	14.3 Disaster Recovery Policies & Procedures	2	4.5	6.5
	14.4 BC/DR Testing Policies & Procedures	1	6	7
	14.5 Data Protection Impact Assessments (DPIA)	2	2	4
	14.6 BC Contingency Plan	1	7	8
	% Compliance	**100.00**	**97.92**	**98.96**
Human Resources / Organisational Development	**15. PEOPLE**	**16**	**10**	**26**
	15.1 Prior to Employment	2	0	2
	15.2 During Employment.	3	5	8
	15.3 Staff Training & Awareness Culture	7.5	2	9.5
	15.4 Staff Skills Assessment	2	1	3
	15.5 Mobile / Remote Working Policy	1	1	2
	% Compliance	**96.88**	**90.00**	**93.44**
Facilities / Estates	**16. ENVIRONMENTAL SECURITY**	**4**	**0**	**4**
	16.1 Equipment Location	2	0	2
	16.2 Power Resilience	2	0	2
	% Compliance	**100.00**	**100.00**	**100.00**
	17. PHYSICAL / BUILDING SECURITY	**3**	**3**	**6**
	17.1 Access Control	0.5	0.5	1
	17.2 Internal Security	2	1.5	3.5
	% Compliance	**83.33**	**66.67**	**75.00**
	TOTALS	**247**	**180**	**427**
	Weighting %	**58%**	**42%**	

*Only for use with Pervade CS Conversion module©

Maturity Posture

	Date of last Update	16/10/2024	Average Maturity Score	86.8		
DUTY AREA	CATEGORY	Description	Compliance Areas	Tier 1 Maturity (%)	Tier 2 Maturity (%)	Combined Maturity Score (%)
	Sub-Category	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	89.4	84.3	86.8
Senior Management	1. ORGANISATIONAL GOVERNANCE	Appropriate organisational structures, policies and processes in place to understand, assess and systematically manage security risks to the organisation's network and information systems.	1.1 Governance Framework 1.2 Leadership & responsibility 1.3 Adoption Audit and Assurance of Security standards 1.4 Regulatory Compliance	100.0	96.2	98.1
	2. RISK MANAGEMENT	Appropriate steps are in place to identify, assess and understand security risks to the network and information systems. This includes an overall organisational approach to risk management.	2.1 Policy & Processes 2.2 Cyber / Information Risk Assessment 2.3 Risk Treatment & Tolerance 2.4 Risk Governance	88.9	76.7	82.8
Procurement / Contracts / Legal	3. SUPPLIER MANAGEMENT	The organisation understands and manages security risks that arise as a result of dependencies on external suppliers and third party services.	3.1 Supply Chain Assurance 3.2 Roles and Responsibilities 3.3 Access control 3.4 Security in Procurements 3.5 Security in Cloud Services	52.1	44.4	48.3
Technical Team	4. ASSET MANAGEMENT	Everything required to deliver, maintain or support networks and information systems and services is determined and understood.	4.1 Hardware Assets 4.2 Software Assets 4.3 Infrastructure management	92.9	87.5	90.2
	5. INFORMATION SECURITY MANAGEMENT	Proportionate security measures are in place to protect information, data, services and systems from cyber-attack.	5.1 Security Policy & Processes 5.2 Lifecycle Management 5.3 Storage 5.4 Information / Data Classification 5.5 Information Asset Register 5.6 Information / Data Transfer Controls	80.4	60.5	70.5
	6. SERVICES RESILIENCE	Network and information systems are designed to be resilient to cyber security and operational adverse incidents.	6.1 Services Resilience Systems are appropriately segregated and resource limitations are mitigated	50.0	83.3	66.7
	7. ACCESS CONTROL	Access to information, services and systems is controlled, managed and monitored through policies and procedures.	7.1 Account Management 7.2 Identity Authentication 7.3 Privilege Management 7.4 Administrator Account Management	100.0	100.0	100.0
	8. MEDIA MANAGEMENT	Fixed and portable storage media and devices are managed and data / information is appropriately protected.	8.1 Storage Media 8.2 Mobile Media / Devices 8.3 Cryptography	86.7	58.3	72.5
	9. SYSTEM MANAGEMENT	Information systems are protected from cyber-attack throughout their lifecycle.	9.1 Secure Configuration 9.2 Secure Design / Development 9.3 Change Control Procedures 9.4 System Testing	100.0	100.0	100.0
	10. OPERATIONAL SECURITY	Appropriate technical and organisational measures are in place to protect systems and digital services from cyber attack	10.1 Malware Policies & Protection 10.2 Email Security. 10.3 Application Security 10.4 Vulnerability Management & Scanning 10.5 Data Exfiltration Monitoring 10.6 Browser Management 10.7 Monitor / Audit User Activity	97.9	100.0	99.0
	11. NETWORK SECURITY	Appropriate measures are in place to ensure the protection of information systems and information held in networks.	11.1 Patch Management 11.2 End-Point Device Management 11.3 Internal Segregation 11.4 Wireless Security 11.5 Boundary / Firewall Management 11. 6 Administrator Control 11.7 IP & DNS Management Organisational IP ranges are known, recorded and managed; 11.8 IoT Management Internet-facing devices should be securely configured and segregated as appropriate.	93.3	78.6	86.0
	12. INCIDENT DETECTION	Organisations shall have in place monitoring systems and procedures to detect cyber-attacks.	12.1 Detection Capability 12.2 Security Monitoring	100.0	100.0	100.0
	13. INCIDENT MANAGEMENT	Well-defined incident management processes are in place, documented and regularly tested.	13.1 Incident Response Protocol 13.2 Incident Reporting Procedure 13.3 Post-Incident Review & Learning	97.5	92.9	95.2
	14. BUSINESS CONTINUITY	Information security continuity shall be embedded in the organisation's business continuity management systems	14.1 Data Recovery Capability 14.2 Back up Policies & Procedures 14.3 Disaster Recovery Policies & Procedures 14.4 BC/DR Testing Policies & Procedures 14.5 Data Protection Impact Assessments (DPIA) 14.6 BC Contingency Plan	100.0	97.9	99.0
Human Resources / Organisational Development	15. PEOPLE	The organisation has policies and procedures in place to ensure staff and contractors are screened, trained and know their security responsibilities.	15.1 Prior to Employment 15.2 During Employment. 15.3 Staff Training & Awareness Culture 15.4 Staff Skills Assessment 15.5 Mobile / Remote Working Policy	96.9	90.0	93.4
Facilities / Estates	16. ENVIRONMENTAL SECURITY	Appropriate procedures are in place to reduce the risks from internal and external environmental threats and hazards.	16.1 Equipment Location 16.2 Power Resilience	100.0	100.0	100.0
	17. PHYSICAL / BUILDING SECURITY	To prevent unauthorised physical access, damage and interference with the organisation's information systems and services.	17.1 Access Control 17.2 Internal Security	83.3	66.7	75.0

*Only for use with Pervade CS Conversion module©

Risk Register

	Date of last Update	16/10/2024		Average Indicative Risk Score		3.5			Average Current Risk Score		9.0	
DUTY	CATEGORY	Description	Compliance Areas	Raised by	Raised on Date	Tier 1 Completion (%)	Tier 2 Completion (%)	Indiciative Risk Score (low 0 to high 25)	Current Risk Profile			
AREA	Sub-Category	Description:Due to lack of detailed implementation of the following information and cyber security controls there is a risk to the organisation that the associated duty areas and sub-categories will be ineffective unless the associated compliance areas are in place.	Arranged by sub category	Original risk recorded by (Default = initial entry)	Date risk was identified	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	Probability	Impact	Current Risk Score	Target Risk Score
Threat	0. Threat level (Environmental)	Comprehensive integrated controls to mitigate against the threat of disruption from malicious cyber activity related to current level of activity in the sector. Current threat level in education sector is highest (Source Microsoft Security Intelligence https://www.microsoft.com/en-us/wdsi/threats)	All compliance areas	Default	09/12/2022			3.5	3	3	9	12
Senior Management	1. ORGANISATIONAL GOVERNANCE	Appropriate organisational structures, policies and processes in place to understand, assess and systematically manage security risks to the organisation's network and information systems.	1.1 Governance Framework 1.2 Leadership & responsibility 1.3 Adoption Audit and Assurance of Security standards 1.4 Regulatory Compliance	Default	09/12/2022	100.0	96.2	0.6	3	3	9	4
	2. RISK MANAGEMENT	Appropriate steps are in place to identify, assess and understand security risks to the network and information systems. This includes an overall organisational approach to risk management.	2.1 Policy & Processes 2.2 Cyber / Information Risk Assessment 2.3 Risk Treatment & Tolerance 2.4 Risk Governance	Default	09/12/2022	88.9	76.7	4.7	3	3	9	4
Procurement / Contracts / Legal	3. SUPPLIER MANAGEMENT	The organisation understands and manages security risks that arise as a result of dependencies on external suppliers and third party services.	3.1 Supply Chain Assurance 3.2 Roles and Responsibilities 3.3 Access control 3.4 Security in Procurements 3.5 Security in Cloud Services	Default	09/12/2022	52.1	44.4	13.2	3	3	9	4
Technical Team	4. ASSET MANAGEMENT	Everything required to deliver, maintain or support networks and information systems and services is determined and understood.	4.1 Hardware Assets 4.2 Software Assets 4.3 Infrastructure management	Default	09/12/2022	92.9	87.5	2.6	3	3	9	4
	5. INFORMATION SECURITY MANAGEMENT	Proportionate security measures are in place to protect information, data, services and systems from cyber-attack.	5.1 Security Policy & Processes 5.2 Lifecycle Management 5.3 Storage 5.4 Information / Data Classification 5.5 Information Asset Register 5.6 Information / Data Transfer Controls	Default	09/12/2022	80.4	60.5	8.1	3	3	9	4
	6. SERVICES RESILIENCE	Network and information systems are designed to be resilient to cyber security and operational adverse incidents.	6.1 Services Resilience Systems are appropriately segregated and resource limitations are mitigated	Default	09/12/2022	50.0	83.3	7.2	3	3	9	4
	7. ACCESS CONTROL	Access to information, services and systems is controlled, managed and monitored through policies and procedures.	7.1 Account Management 7.2 Identity Authentication 7.3 Privilege Management 7.4 Administrator Account Management	Default	09/12/2022	100.0	100.0	0.0	3	3	9	4
	8. MEDIA MANAGEMENT	Fixed and portable storage media and devices are managed and data / information is appropriately protected.	8.1 Storage Media 8.2 Mobile Media / Devices 8.3 Cryptography	Default	09/12/2022	86.7	58.3	7.9	3	3	9	4
	9. SYSTEM MANAGEMENT	Information systems are protected from cyber-attack throughout their lifecycle.	9.1 Secure Configuration 9.2 Secure Design / Development 9.3 Change Control Procedures 9.4 System Testing	Default	09/12/2022	100.0	100.0	0.0	3	3	9	4
	10. OPERATIONAL SECURITY	Appropriate technical and organisational measures are in place to protect systems and digital services from cyber attack	10.1 Malware Policies & Protection 10.2 Email Security. 10.3 Application Security 10.4 Vulnerability Management & Scanning 10.5 Data Exfiltration Monitoring 10.6 Browser Management 10.7 Monitor / Audit User Activity	Default	09/12/2022	97.9	100.0	0.2	3	3	9	4
	11. NETWORK SECURITY	Appropriate measures are in place to ensure the protection of information systems and information held in networks.	11.1 Patch Management 11.2 End-Point Device Management 11.3 Internal Segregation 11.4 Wireless Security 11.5 Boundary / Firewall Management 11. 6 Administrator Control 11.7 IP & DNS Management Organisational IP ranges are known, recorded and managed; 11.8 IoT Management Internet-facing devices should be securely configured and segregated as appropriate.	Default	09/12/2022	93.3	78.6	4.0	3	3	9	4
	12. INCIDENT DETECTION	Organisations shall have in place monitoring systems and procedures to detect cyber-attacks.	12.1 Detection Capability 12.2 Security Monitoring	Default	09/12/2022	100.0	100.0	0.0	3	3	9	4
	13. INCIDENT MANAGEMENT	Well-defined incident management processes are in place, documented and regularly tested.	13.1 Incident Response Protocol 13.2 Incident Reporting Procedure 13.3 Post-Incident Review & Learning	Default	09/12/2022	97.5	92.9	1.4	3	3	9	4
	14. BUSINESS CONTINUITY	Information security continuity shall be embedded in the organisation's business continuity management systems	14.1 Data Recovery Capability 14.2 Back up Policies & Procedures 14.3 Disaster Recovery Policies & Procedures 14.4 BC/DR Testing Policies & Procedures 14.5 Data Protection Impact Assessments (DPIA) 14.6 BC Contingency Plan	Default	09/12/2022	100.0	97.9	0.3	3	3	9	4
Human Resources / Organisational Development	15. PEOPLE	The organisation has policies and procedures in place to ensure staff and contractors are screened, trained and know their security responsibilities.	15.1 Prior to Employment 15.2 During Employment. 15.3 Staff Training & Awareness Culture 15.4 Staff Skills Assessment 15.5 Mobile / Remote Working Policy	Default	09/12/2022	96.9	90.0	1.9	3	3	9	4
Facilities / Estates	16. ENVIRONMENTAL SECURITY	Appropriate procedures are in place to reduce the risks from internal and external environmental threats and hazards.	16.1 Equipment Location 16.2 Power Resilience	Default	09/12/2022	100.0	100.0	0.0	3	3	9	4
	17. PHYSICAL / BUILDING SECURITY	To prevent unauthorised physical access, damage and interference with the organisation's information systems and services.	17.1 Access Control 17.2 Internal Security	Default	09/12/2022	83.3	66.7	6.8	3	3	9	4
							Average indicative Risk	3.5	Average current risk		9.0	

Agenda Item 9.1

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 4 March 2025

INTERNAL AUDIT

9.1 - STAFF DEVELOPMENT PAPER F

LEVEL OF ASSURANCE
Good

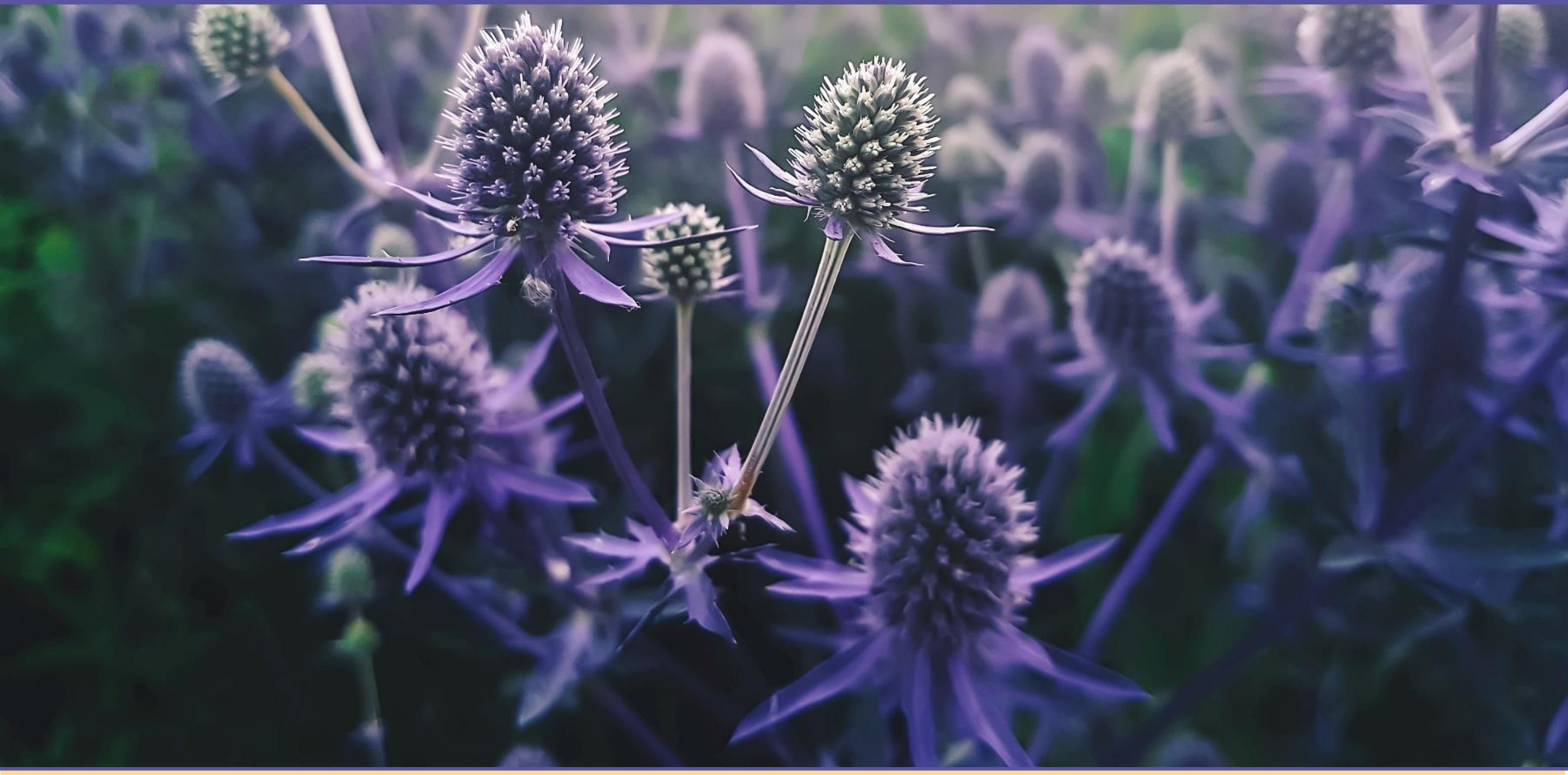
Dundee & Angus College

Staff Development

Internal Audit report No: 2025/02

Draft issued: 4 February 2025

Final issued: 7 February 2025



Henderson Loggie

Contents

Level of Assurance

In addition to the grading of individual recommendations in the action plan, audit findings are assessed and graded on an overall basis to denote the level of assurance that can be taken from the report. Risk and materiality levels are considered in the assessment and grading process as well as the general quality of the procedures in place.

Gradings are defined as follows:

Good	System meets control objectives.
Satisfactory	System meets control objectives with some weaknesses present.
Requires improvement	System has weaknesses that could prevent it achieving control objectives.
Unacceptable	System cannot meet control objectives.

Action Grades

Priority 1	Issue subjecting the organisation to material risk and which requires to be brought to the attention of management and the Audit and Risk Committee.
Priority 2	Issue subjecting the organisation to significant risk and which should be addressed by management.
Priority 3	Matters subjecting the organisation to minor risk or which, if addressed, will enhance efficiency and effectiveness.

Management Summary

Overall Level of Assurance

Good	System meets control objectives.

Risk Assessment

This review focused on the controls in place to mitigate the following risks on the Dundee & Angus College (‘the College’) Strategic Risk Register (as at November 2024):

- Risk 3.1 - Failure to reach aspirational standards in learning, teaching, and service delivery (Residual Risk Score: 6, Minor);
- Risk 3.4 - Failure to meet the aspirational standards in respect of the health, safety, wellbeing and development of staff and students (Residual Risk Score: 6, Minor);
- Risk 3.7 - Industrial relations problems (including industrial action) (Residual Risk Score: 8, Minor); and
- Risk 3.12 - Failure to attract, engage, retain or develop appropriately qualified staff (Residual Risk Score: 4, Minor).

Background

As part of the Internal Audit programme at the College for 2024/25 we carried out a review of the systems in place for Staff Development. The Audit Needs Assessment identified this as an area where risk can arise and where Internal Audit can assist in providing assurances to the Principal and the Audit and Risk Committee that the related control environment is operating effectively, ensuring risk is maintained at an acceptable level.

Oversight of the staff development processes at the College is the responsibility of all managers across both the academic and support functions within the College. Operational management of the resourcing and training needs of staff is the responsibility of the Vice Principal Support Services and Operations, supported by the Head of People and Organisational Development (OD), who oversees the OD and Human Resources (HR) teams. The OD and HR teams work in conjunction with line managers across the College to determine any learning and development opportunities, and to ensure that the College has sufficient capacity and capability going forward.

The College has in place a People Strategy, with the most recent iteration issued in May 2024. This Strategy is built around eight principles of high performing culture each of which has key strategic objectives linking to delivery of the strategic vision and driving operational activities and priorities.

The College has an annual Development Review process in place, which is completed for all staff. This process captures areas of development need to inform future training provision. The College also undertakes staff development days, where any College wide training needs are addressed through protected time for training provision, in addition to themed training weeks / months where courses are offered to all staff to improve and develop their skills in a specific area.

Scope, Objectives and Overall Findings

This audit considered whether the College is making best use of its staff and incorporated a review of workforce planning; training; the personal development plan system; and succession planning.

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

Objective	Findings				
The objective of our audit was to obtain reasonable assurance that:		**1**	**2**	**3**	**Action already in progress**
		No. of Agreed Actions			
1. The College has a systematic approach for ensuring that its staff resources match need in order to deliver planned commitments. Where gaps are identified, timely action is taken to close these	**Good**	0	0	0	✓
2. The College's approach to training, including induction training, is clearly informed by an assessment of where there are skills / knowledge / performance gaps	**Good**	0	0	0	✓
3. The College has a systematic approach to the evaluation of its training to ensure that it is achieving the desired impact	**Good**	0	0	0	✓
4. There is a systematic approach for translating business objectives into actions / tasks for members of staff and a systematic approach is used for communicating objectives and performance expectations to staff	**Good**	0	0	0	
5. A systematic process is used for providing feedback to staff on performance and agreeing action to improve performance	**Good**	0	0	0	
6. Appropriate succession planning strategies, action plans and monitoring arrangements are in place within the College	**Good**	0	0	0	
Overall Level of Assurance	**Good**	**0**	**0**	**0**	
		System meets control objectives.			

Audit Approach

The Head of People and Organisational Development, the HR Manager, and a sample of senior managers were interviewed, and the College's policies, procedures and structure were reviewed, to assess compliance with the above objectives.

Summary of Main Findings

Strengths

- There is a Workforce Plan in place which sets out the long-term strategic focus for workforce development.
- Curriculum planning and utilisation reporting is used to inform decisions relating to staffing and recruitment to ensure that staff resources match planned commitments and aims.
- There are processes in place to support successful recruitment, and the development and promotion of staff where staff have ambition to progress within the College.
- There is a set induction programme to support new employees. This includes 12-month roadmaps for both academic and support staff, set training modules, and probationary meetings at three and six months to assess progress.
- All staff take part in annual Development Reviews with their line manager. There is a set template to ensure consistency in reviews and a number of supporting guidance documents to ensure a focus on development needs. Staff set a number of targets which are revisited throughout the year to assess progress and support needed for achievement of goals.
- An academic training pathway has been developed to support academic staff in obtaining the required qualifications to register with the General Teaching Council (Scotland) (GTCS).
- Two all-staff development days are held each year to engage staff with training and development opportunities.
- There is a large internal Continuing Professional Development (CPD) programme available to all staff across a wide range of topics. While certain training will be mandatory dependent on role, staff are invited to engage with any training they feel is of interest to them or will assist in their development.
- The iTrent system is used to record all training and development undertaken by each member of staff to ensure an accurate record is available.
- Staff are asked to complete evaluations upon completion of training or participation in staff development days. This allows OD staff to assess the impact of the training and whether development needs are being met.
- While there is no formal succession planning document in place, there are numerous processes that feed into succession planning. This includes identification of potential single points of failure, ongoing training of staff to support progression and early recruitment where gaps are identified.

Actions Already in Progress

- The Workforce Plan was due to undergo review in January 2024. However, this review did not take place at that time due to competing priorities. During our discussions with the Head of People and Organisational Development it was noted that this is currently undergoing review.
- A Communications project is due to take place in 2025, targeting digital skills with a focus on building confidence, encouraging an open minded approach, and honing competencies and the ability to problem solve without the reliance on key member of staff with a strong understanding of digital skills. It is expected this will be completed by august 2026.
- The College have been exploring options to improve the iTrent system, having identified that there is a learning management system module which can be added to the system. A demonstration for this module was delivered in November 2024 and consideration is being given to implementing this functionality ahead of the 2025/26 academic year

Weaknesses

- No significant weaknesses were identified during our review. However, as highlighted above, there are several areas where work is still progressing.

Acknowledgments

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

Main Findings

Objective 1 - The College has a systematic approach for ensuring that its staff resources match need in order to deliver planned commitments. Where gaps are identified, timely action is taken to close these

The College has a Workforce Plan in place covering the period 2022 – 2024. The plan was first published in January 2022 and was due to undergo review in January 2024. During our discussions with the Head of People and Organisational Development (OD) it was noted that this Plan is currently undergoing review.

The Workforce Plan sets out a long-term strategic focus on the College's workforce, taking an agile approach, allowing for planning against future challenges. The College is focused on delivering educational, organisational and financial priorities and effective workforce planning ensures that focused decisions are being made to deliver targets and enhance services offered. The People Team has overall responsibility for delivery of the plan which includes effective recruitment and development of staff.

From discussion with key staff including the Head of People and OD, it was established that a post request system is in place to ensure that posts cannot be added without appropriate consideration and approval. Posts must be approved by all three members of the Executive Leadership Team to give appropriate overview and ensure the posts are necessary and within budget. For academic staffing, the Vice Principal Curriculum and Partnerships reviews the curriculum plan, timetable information, and utilisation reports on a regular basis to identify areas of under or over provision. Where this may arise, consideration will be given to staffing levels and identifying opportunities to upskill other staff to help in areas of under provision.

The Vice Principal Support Services and Operations oversees resourcing for support staff, identifying whether staff with appropriate skills are in place. The College has seen an increasing need in relation to student support, both in volume and complexity of support needed, which can create increased pressures for support staff. The College has identified mental health support for both staff and students as a key area of development and this has helped to identify requirements for training and development.

Objective 2 - The College's approach to training, including induction training, is clearly informed by an assessment of where there are skills / knowledge / performance gaps

As part of the Workforce Plan (January 2022), the College has undertaken a mapping exercise, considering how the Workforce Plan connects with other key strategies including the Digital Strategy, Estates Strategy, People Strategy, Learner Experience Strategy and Financial Strategy. This sets out the ways in which working has and will continue to evolve, and the skills and experiences that will be required to ensure the progression and success of strategies across the College.

Upon joining the College, all staff are enrolled into an induction process to support and guide their first 12 months of employment with the College. Human Resources (HR) is notified when an employee is added to the system and a welcome email is sent to the employee with a link to access the induction hub. This shows what mandatory training must be completed, with additional optional training available should an employee be interested in any particular area. The mandatory training for all staff is made up on eight key modules which consist of training in key areas such as the UK General Data Protection Regulation and Health and Safety. The hub is also home to other induction paperwork such as the induction checklists that must be completed by the employee and line manager, and four-to-six-week plan. This is used to identify any gaps in the employee's skill set or where training may be beneficial.

All new starts undergo probation reviews at both three and six months in the role. This is used as an opportunity to assess an employee's skills and competencies within the role, identifying any areas where further training may be needed to support the employee, although employees are encouraged to discuss development and training needs with their line managers at any stage with no need to wait until a formal review. It should be noted that upon progressing beyond the six-month probation review, induction may continue but this is dependent on the specific role and the employees previous experience. This means that they will continue to engage in training and development for as long as deemed appropriate.

Induction road maps have been created for both academic and support staff which clearly set out the journey staff will undertake from first day, three-month review, six-month review, and completion of first year of employment. There are supporting checklists for the roadmap documents which must be completed by the new member of staff and their line manager. It is the responsibility of the line manager to ensure that the new staff member progresses through the induction process and the checklist is completed.

All members of staff undergo annual a Development Review with their line manager which are described in more detail under Objective 4. As part of these reviews, discussions are held about employees' performance and if any additional support, training, or development is required for the staff member to fulfil their role. Staff are encouraged to also discuss ambitions, training and development opportunities with their line manager at any stage during the year as opposed to waiting for their formal Development Review.

During our discussion with the Academic Development Lead, it was noted that a key consideration in relation to academic staff is the contractual requirement for lecturers to be registered with the General Teaching Council (Scotland) (GTCS) from November 2028, in line with National Bargaining arrangements. As a result of this requirement, the Academic Development Team and OD staff have developed a teacher training pathway to ensure that all academic staff will have appropriate qualifications. Due to the nature of some academic roles, many staff are employed by the College who have significant experience in industry, but this is not always supported by the required teaching qualifications. The academic pathway considers the experience and qualifications which members of staff already have and considers the available pathways available to support each member of staff in meeting qualification and training requirements. There is also an academic team leader forum in place, which meets three times a year to discuss training needs and upcoming areas for development.

Objective 2 - The College’s approach to training, including induction training, is clearly informed by an assessment of where there are skills / knowledge / performance gaps (Continued)

From our discussions with managers, it was established that many members of staff may hold specialist qualifications to support their role. This varies widely across the College and includes industry qualifications in specific trades such as plumping, veterinary qualifications, or accounting qualifications. These qualifications typically have mandatory training and Continuing Professional Development (CPD) requirements in order to maintain the professional designation. While it is the responsibility of each staff member to ensure that these requirements are met, the College provide support for staff by giving access to a range of in-house CPD training and staff are encouraged to engage with industry experts and external CPD resources, as required. This may include attendance at a conference, enrolment on a specific industry training course, or inviting an industry expert to the College to provide training to a group of staff.

In addition to the upskilling of academic staff it has been identified, as part of the Workforce Plan, that there is a need to focus on other development areas which will support both staff and students. These areas include:

- Digital Literacies;
- Wellbeing and Resilience; and
- Industry Standard Skills.

General training needs are also identified through consultation with staff, consideration of feedback from training and staff development sessions, and horizon scanning for upcoming topics of interest within the industry. For example, as established through conversations with staff, current focuses include Equality, Diversity and Inclusion, attendance, neurodiversity, and mental health. Topics may also be driven by College data collection such as sickness absence which may identify common issues such as stress or mental health, or issues such as an increased number of difficult conversations taking place within teams.

There is a programme of mandatory training in place which all staff must undertake - both at induction and again as refresher training - on a cyclical basis. Completion rates of mandatory training are monitored on an ongoing basis and are reported to the Human Resources and Development Committee. From our review of the minutes of the November 2024 committee meeting, it was determined that all training from the 2022/23 mandatory training programme had a 100% completion rate. Completion rates from the 2023/24 training programme were reported at 86%, 93% and 91%. The training programme for the 2024/25 mandatory training list is currently still in progress, and at November 2024 was recorded at 43% and 44%. These rates will continue to be monitored and where mandatory training has not been completed, will be raised with the relevant manager for discussion as part of the individual staff members development review.

Objective 2 - The College’s approach to training, including induction training, is clearly informed by an assessment of where there are skills / knowledge / performance gaps (Continued)

From discussion with staff and the Director of Curriculum and Partnerships, and as identified in the Workforce Plan, it was established that a key area for development relates to digital skills. Since COVID-19, there has been a rapid change in the uptake of and the way in which technology is used by staff in all areas of the College. However, this has led to a skills gap for some staff that may previously not have been reliant on technology but whose role now have large elements which require digital skills. As a result of this, a Communications project is due to start in 2025, targeting digital skills with a focus on building confidence, encouraging an open-minded approach, and honing competencies and the ability to problem solve without the reliance on key members of staff with a strong understanding of digital skills. The purpose of the project will be to ‘baseline’ all staff and develop core competencies, to ensure that everyone has the same base level of digital understanding and skills. A project brief is due to be reported to the Senior Leadership Team in early 2025, and the project is expected to last for approximately 18-months with completion for the 2026/27 academic year.

Finally, the College operates two all-staff development days each year where the College is closed to students to allow staff to take part in training and development opportunities. The most recent development day took place in November 2024, with activities taking place over all three campus buildings. Staff were invited to sign up to training and development sessions which were of interest to them and varied across a wide range of areas including technical skills, health and wellbeing, and opportunities to complete core CPD and training they may otherwise have not had time to complete. Feedback received has been hugely positive with staff praising the range of development opportunities, the dedicated time in which to take part in training, and the opportunity to engage with colleagues from across all areas of the College.

Objective 3 - The College has a systematic approach to the evaluation of its training to ensure that it is achieving the desired impact

The College operates a large internal CPD programme available to all members of staff. On completion of any CPD courses, employees are asked to complete an evaluation, which helps to ensure that the desired impact is being achieved and to consider where changes may be required. Any training delivered in-house by the College or training courses that are logged via the iTrent system undergo an online evaluation shortly after completion of the training to assess the content and output of the training. This is used to gather feedback about how staff found the session, what they enjoyed, or thought could be improved, and how they would apply anything that they learnt moving forward.

During our discussions with the Head of People and Organisational Development and other managers, it was established that the College currently uses the iTrent system to track and record training and development activities, following a number of years using a variety of self-developed in-house systems. The intention was to encourage consistency in the way that training and development was recorded and ensure accuracy of data. However, there have been a number of difficulties for staff using the system which currently requires a significant amount of manual input and administration and does not report information in the desired manner. From discussion with the Head of HR and OD it was noted that the College has been exploring solutions and there is a learning management module that can be added to the system. A demo for this was delivered in November 2024 and consideration is being given to implementing this ahead of the 2025/26 academic year.

As noted previously, the College also runs two all staff development days each year, which provides the opportunity for staff take part in various training and development activities. A survey is sent to all staff following the staff development days, the findings of which are collated by HR and OD to allow consideration and to determine the overall staff opinion, positive outcomes, whether the days had the desired impact for staff, and to identify any specific future College-wide training needs. Feedback is also utilised to support development and changes to the development days to align with the needs of staff.

Objective 4 - There is a systematic approach for translating business objectives into actions / tasks for members of staff and a systematic approach is used for communicating objectives and performance expectations to staff

Through discussions with the Head of People and OD, it was identified that the College has an annual Development Review process which involves a direct translation from the College's operational plans, which set out actions to support the delivery of the strategic objectives. A strategy for 2025 is currently in development and once established, any key messages will be used to shape the Development Review process.

The Development Review process takes place annually for all members of staff with their line manager. This is on a rolling basis, meaning that there is not a fixed point in the year at which these will take place for all members of staff. The Development Review cycle is made up of four main stages – planning, discussion, act, and reflection, which means that all members of staff will always be at one of the four stages. A Development Review template is in place to ensure consistency in the process for all members of staff and managers. The template is split into three main sections – Review of the Year, Planning for Next Year, and Setting Priorities and Goals. The review of the year encourages staff to reflect on events, activities, wellbeing, responsibilities and development from the previous 12 months with suggested areas they may consider such as progress against goals, successes, development and CPD, and personal reflections. Planning for next the upcoming year takes into consideration the events, activities and responsibilities that are expected within the next 12 months, with a specific emphasis on the College values of 'Innovation, Inspiration, Trust, Respect and Success'. Consideration is also given to priorities at an individual and team level, including the support that may be needed, areas for development, and changes that may be needed. The final section is where specific goals are set, using 'SMART' targets (Specific, Measurable, Achievable, Realistic, and Time Bound). The form is then completed by the staff member to highlight any areas of good performance in the year, and then this is signed off by their line manager and passed to HR and OD to review the information for any emerging trends and training gaps. The process then commences again, with the form updated to note any changes to the operational plan within the relevant department, to ensure the College's strategic objectives are consistently reflected in the process.

The College has detailed guidance to support the process which sets out what happens at each stage of the Development Review cycle, responsibilities for both staff and management, and links to resources including the review template and specific guidance documents. Other guidance documents include:

- Clean Language Questions;
- Having Crucial Conversations;
- Identifying Individual Objectives;
- D4 Feedback Model; and
- Purpose of Development Reviews.

Completion rates of Development Reviews are tracked on an ongoing basis and are reported to the HR Committee. From review of the minutes from the November 2024 committee meeting, we confirmed that completion rates of development reviews to date for 2024/25 were at 62%. It should be noted that Development Reviews are part of an ongoing cycle, with staff members completing reviews throughout the year, rather than a set time by which these must be completed meaning that 100% completion would not be expected until the end of the academic and financial year.

Staff Development

Objective 5 - A systematic process is used for providing feedback to staff on performance and agreeing action to improve performance

As noted under Objective 4, above, the College has a formal Development Review process in place, which is completed annually, with ongoing monitoring throughout the year. Objectives are set for each member of staff and are agreed between them and their line manager during the review process. The objectives are connected to the College's operational plans, which in turn link back to the strategic objectives and to the identified professional development needs specific to the individual member of staff. Progress on these objectives is monitored throughout the year during the regular one-to-one meetings between the staff member and their line manager, with proactive steps taken to help the staff member achieve their objectives, which may include taking part in specific training or qualifications.

The Development Review form for teaching staff is structured using the GTCS standards to shape the development needs. There is no assessment of staff members' 'performance', but instead a review and identification of areas of further professional development priorities for the coming 12-month period.

As the Development Review process is operated on an annual cycle, including a review of objectives from the previous year and goal setting for the coming year, opportunities for both formal and informal feedback are utilised by managers to communicate any areas to be addressed by the member of staff. An example of this, as noted above, is the informal one-to-one meetings between the member of staff and their line manager, which provides an opportunity for discussions around specific events within the staff member's area of the College, but also for the line manager to obtain updates on the progress of the staff member's achievement of their Development Review objectives. From discussions with management across the College, it was established that this process is consistently applied, and that any areas of focus can also be elevated through the hierarchy within each department via one-to-one meetings held between staff and their line managers.

Objective 6 - Appropriate succession planning strategies, action plans and monitoring arrangements are in place within the College

Through our discussions with the Head of People and OD, it was established that there is no formal succession planning document in place, however there are several processes which feed into succession planning. The College links its succession planning processes into its recruitment and other internal processes to help ensure suitable candidates within the College are encouraged and equipped to apply. A number of senior staff have progressed through various levels within the College demonstrating the effectiveness of identifying opportunities for development and supporting staff with ambition of promotion. It was noted that as part of this the College incorporates a culture of encouraging growth and development within, and as such it aims to upskill and support people even if it means them moving on to new opportunities out with the College.

From discussions it was identified that the College supports staff to progress internally, as part of its culture, with the motivation being the retention of quality staff. However, we did establish that the requirement to publicly advertise roles and follow an open and fair recruitment process is followed to ensure that the most suitable candidate, either internal or external, will be selected.

It was noted for recruitment exercises, that the recruiting manager receives advice and support from HR colleagues on the approach to be taken in advertising the role and in ensuring that the job descriptions are accurate. As part of the internal development processes, staff with aspirations for career progression are encouraged to take part in development activities that may support promotion into a more senior role. Succession planning is also built into the Development Review process as all staff are invited to note their goals in relation to career progression, and line managers review the training for those who aspire to progress to a more senior role within the College. The structure of the form is also aligned to GTCS standards and the College's operational priorities.

During our discussion with the Head of People and OD, it was noted that some areas have been identified as having a single person dependency, where absence of that staff member may cause significant operational issues for the area in which they work. Where dependencies have been identified, arrangements have been made to train other staff should a succession need be identified. This can include leadership development of junior members of staff, early recruitment where there may be identified gaps, and extending the handover process where a member of staff is leaving their role (either for a different role within the College or leaving the College entirely).

It was also established that a leadership development programme was previously in place at the College and there are ambitions to reintroduce this. At present leadership development is delivered through CPD and training opportunities, as well as through resources provided by College sector groups and the College Development Network (CDN).

Henderson Loggie

Agenda Item 9.2

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 4 March 2025

INTERNAL AUDIT

9.2 – PROGRESS REPORT PAPER G

Dundee & Angus College

Internal Audit Progress Report

Audit & Risk Committee – 4 March 2025

Issued: 24 February 2025

Henderson Loggie

Internal Audit Progress Report
March 2025

Progress with the annual plan for 2024/25 is shown below.

Audit Area	Planned reporting date	Report status	Report Number	Overall Conclusion	Audit Committee	Comments
Annual Plan 2024/25	September 2024	Draft: 12/07/24 2nd Draft: 15/07/24 3rd Draft: 03/09/24 Final:	2025/01	N/A	17/09/24	
Payroll	March 2025					Management requested that the audit fieldwork be deferred until March 2025. Agreed start date 25 March 2025.
Budgetary Control	June 2025					Agreed start date for fieldwork 14 April 2025.
Staff Development	March 2025	Draft: 04/02/25 Final: 07/02/25	2025/02	**Good**	04/03/25	
Digital Strategy Implementation	June 2025					Agreed start date for fieldwork 24 March 2025.
Credits	December 2025					Agreed start date for fieldwork 18 August 2025.
Bursary, Childcare and Hardship Funds	December 2025					Agreed start date for fieldwork 11 August 2025.

Audit Area	Planned reporting date	Report status	Report Number	Overall Conclusion	Audit Committee	Comments
EMA	December 2025					Agreed start date for fieldwork 11 August 2025.
Follow Up Reviews	September 2025					Agreed start date for fieldwork 7 July 2025.

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

Agenda Item 9.3

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 4 March 2025

INTERNAL AUDIT

9.3 - PROCUREMENT & CREDITORS AUDIT PROGRESS

PAPER H

BOARD OF MANAGEMENT

Finance & Property Committee 25 February 2025 and Audit & Risk Committee 4 March 2025

Progress Report - Procurement and Creditors Internal Audit Recommendations

Paper for information

1. Introduction

Procurement and Creditors was selected for review in our 2023/24 Internal Audit Plan and Audit and Risk Committee considered the Auditor's Report on 4 June 2024.

The overall report level of assurance was 'Requires Improvement' meaning the system has weaknesses that could prevent it fully achieving control objectives.

The auditors made six recommendations which were all accepted by management. The Finance and Property Committee requested an update on progress with actions at its meeting on Tuesday 25th February 2025. Audit and Risk Committee also requested an update on actions arising from the Procurement and Creditors Report at its meeting on Tuesday 4 March 2025.

2. Recommendations

Members are asked to note the progress below.

3. Progress to February 2025

The following provides a summary of progress in respect of creditors and procurement audit recommendations up to 14 February 2025.

Recommendation 1

Priority Action Grade	Report Grade	Recommended Action	Responsible Officer	Deadline
3	Requires improvement	R1 Although the College's Procurement Policy and Procurement Authorisation Process documents are comprehensive, clear, and are in line with extant Act and Regulations, they should be updated in line with the agreed review frequency to ensure that they accurately reflect any changes in relevant legislation, emerging procurement best practice, staff responsibilities, and the College's procurement values, aims, and approach.	Head of Procurement APUC	31 December 2024 **Complete**

Progress

The Procurement Policy and Procurement Authorisation Process were approved by Finance and Property Committee on 3 December 2024 and have been issued to staff via the staff portal. This recommendation is complete.

Recommendation 2

Priority Action Grade	Report Grade	Recommended Action	Responsible Officer	Deadline
3	Requires improvement	R2 The College should conduct a cost/benefit analysis to assess the impact of changing the approach for ordering of catering supplies and repairs in order to create additional opportunities for smaller, local suppliers to bid for the provision of goods and services related to catering. This could involve establishing the College's own purchasing framework (similar to the Minor Works and Building Maintenance framework currently being worked on) or comparing quotes from local suppliers for select categories of catering spend.	Head of Procurement APUC	31 August 2025

Progress

Audit and Risk Committee agreed a revised deadline of 31 August 2015 for implementation of this recommendation to enable collaboration between APUC and the catering team. This work is expected to be complete by 31 August 2025.

Recommendation 3

Priority Action Grade	Report Grade	Recommended Action	Responsible Officer	Deadline
2	Requires improvement	R3 The College should improve enforcement of compliance in regard to raising Purchase Orders for relevant transactions. The College should clearly communicate to staff that it is against the College's policy to arrange for the supply of goods or services without an appropriately approved Purchase Order and explain to staff how the process helps maintain value for money and minimise supplier risk. Consideration should be given to establishing a more robust "No PO, No Pay" policy, with exclusions explicitly defined and adequately explained to staff members.	Director of Finance	End September 2024 **Complete**

Progress

We have reiterated to staff that it is against the College's policy to arrange for supply of goods or services without an appropriately authorised Purchase Order. We have explained how this maintains value for money and minimises risk.

The College's existing Purchase Order Requisition Procedure (PP1) requires POs to be raised for all purchases, with the exception of utilities (e.g. telephony, electricity, rates, rent) and emergency purchases, e.g. urgent estates repairs. The Purchase Order Requisition Procedure (PP1) ensures we comply with our financial governance requirements and in particular, Financial Regulations and Procurement Regulations.

Since we received this audit recommendation in May 2024, we have focussed efforts on increasing purchase order usage and visible control in our highest spend areas. Estates comprises 30% (£1.9m) and Digital 19% (£1.3m) of our budgeted procurement related expenditure.

We are still working closely with Estates colleagues to consolidate invoices on a weekly/monthly basis for suppliers with high volume/low value expenditure. We are raising purchase orders with these suppliers for the expected spend for the week/month ahead, eliminating a significant amount of processing time, but increasing the overall value of purchase order compliance.

PO compliance was 23% in 2023/34. In December we reported an increase of 6% and as at 14th February compliance since August 2024 has increased to 36%.

Next steps:

1. We will continue to support the Estates team to identify ways to increase purchase order usage and minimise processing time **(on-going)**
2. We will work with other prioritised areas in the College to consolidate purchase order and invoice activity. **(on-going)**
3. We are monitoring PO usage on a monthly basis and will work with individual areas to improve Purchase Order usage across the College **(on-going)**

There is always a balance to be struck between the control arrangements in place and the efficient and pragmatic operation of our activities. The Senior Leadership Team has considered implementing a strict 100% No PO, No Pay Policy. This policy is increasingly in use by some public sector bodies to support financial control and compliance and is a desired way forward from a financial compliance perspective.

In practice, the No PO, no pay policy means invoices that do not contain a PO number will not be paid, potentially creating significant issues with suppliers and budget holders and impacting adversely on College operations, given that most transactions still do not have purchase orders.

As this work progresses we will implement the No PO, No Pay Policy for all activities and budgets where this is possible for the 2025/26 financial year.

Recommendation 4

Priority Action Grade	Report Grade	Recommended Action	Responsible Officer	Deadline
2	Requires improvement	R4(i) The College should conduct a review of existing procurement arrangements, to ensure that external procurement support is structured in a way which will effectively contribute to the delivery of value for money and minimisation of risk at the College. This should involve a specific focus on the future role and responsibility of the TRPT given the existing resource constraints.	Director of Finance	End Sept 2024 **Complete**
2	Requires improvement	R4(ii) The College should communicate to all staff the purpose, importance, and added value of appropriately conducted procurement activity. Staff members should be reminded of the Procurement Policy and procedures in place, and of TRPT's strategic and operational role in managing and assisting with procurement activity. The need for compliance with the established procurement arrangements should be emphasised, and any repeated non-adherence by individuals or departments should be monitored and corrective action taken. A rationale should be given by the purchasing department in any instance where procurement activity has not been conducted in line with the College's guidance.	Director of Finance	~~End September 2024~~ **Revised deadline:** 31 January 2025 **Complete**

Progress

Alongside the introduction of revised operational arrangements, we have reinforced with staff the purpose, importance and added value of procurement activity and the need to follow financial governance requirements. We are actively monitoring compliance, and corrective action will be taken where required. We require a written rationale where departments have not complied fully with procurement guidance.

Recommendation 5

Priority Action Grade	Report Grade	Recommended Action	Responsible Officer	Deadline
2	Requires improvement	R5 The College should consider re-establishing induction and refresher training for non-procurement staff involved in purchasing and procurement activity. This would help staff to understand the legislative background and enhance their knowledge of business processes and internal governance, as well as familiarising them with TRPT and ensuring that they are aware of the team's strategic and operational role in relation to procurement activity	Head of Procurement APUC	End Sept 2024 **Revised deadline:** 31 March 2025

Progress

Procurement training is currently being developed by APUC and we plan to have delivered the training by the end of March 2025.

Recommendation 6

Priority Action Grade	Report Grade	Recommended Action	Responsible Officer	Deadline
2	Requires improvement	R6 The College should examine the following elements of the process to amend standing supplier data: R6 (i) It should be ensured that the process utilised in practice is in line with the documented Bank Account Changes Procedures.	Director of Finance	30 June 2024 **Complete**
2	Requires improvement	R6 (ii) It should be ensured that evidence of processing the changes is appropriately retained in a shared location available to the Finance Team. This should capture all requests received, details of the changes made, how they were verified as bona fide, and evidence of any subsequent independent checks and approvals conducted. The establishment of a central record, available to the Finance Team, containing all amendments made to supplier standing data, such as a spreadsheet, should be considered.	Director of Finance	30 June 2024 **Complete**
2	Requires improvement	R6 (iii) The introduction of built-in system controls in the Sun / P2P systems should be considered, which would require authorisation by an appropriately senior member of the Finance Team prior to any changes to supplier bank details going live and the account being enabled for payment. This would ensure that review and approval is not retrospective, and segregation of duties cannot be circumvented.	Director of Finance	30 June 2024 **Request approval for revised deadline:** 31 December 2024 **Complete**

Progress

R6(i) The documented Supplier Bank Account Changes procedure has been revised and re-issued to finance staff.

R6(ii) Evidence of supplier bank account changes processed, verification and approval is retained in a central location accessible to the finance team.

R6(iii) We have consulted our supplier and it is not possible to build authorisation system controls into the P2P system to ensure segregation of duties controls cannot be circumvented. We are content that the existing internal controls provide adequate assurance.

4. 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 a range of risks identified within the Strategic Risk Register namely:

2.4 – Financial fraud
3.2 – Failure to achieve/maintain compliance arrangements, e.g. contracts, awarding bodies, audit.

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

Agenda Item 9.4

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 4 March 2025

INTERNAL AUDIT

9.4 - FOLLOW UP SUMMARY PAPER I

BOARD OF MANAGEMENT

Audit & Risk Committee
Tuesday 4 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 21 February 2025.

Audit Area	Rec. priority	Considered, but not agreed	Number agreed	Number fully implemented	Number partially implemented	Behind original implementation date	On target
Procurement & Creditors May 2024	2	-	9	7	-	1*	1
2023/24 Student Activity	3	-	3	-	-	-	3
2023/24 Student Support Funds	2	-	1	-	-	-	1
Sports Centre Review	NA	-	7	2			5
Staff Development	🟩	-	-	-	-	-	-
Total		**0**	**20**	**9**	**0**	**1**	**10**

* In line with revised deadline

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 21 February 2025

Six recommendations are fully implemented, Nine on target in line with the original date and two on target in line with the revised implementation dates agreed at the September 2024 meeting.

The current audit recommendations with the respective progress updates are detailed in Appendix 1 below.

5. Procurement and Creditors Action Point Update

A report providing more detail on the implementation of the Procurement and Creditors recommendations is provided elsewhere on this agenda (Paper H).

6. 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
Andy Ross, Director of Infrastructure
Nicky Anderson, Director of Finance
Executive Sponsor: Steve Taylor, Vice Principal Support Services and Operations

Appendix A

Outstanding Recommendations Update 4 March 2025

Year	Audit Area Report Title	Priority Action Grade	Report Grade	Action	Responsible Officer	Deadline	Progress (as at 21 February 2025)
2024/03	Procurement & Creditors	3	Requires Improvement	R2 The College should conduct a cost/benefit analysis to assess the impact of changing the approach for ordering of catering supplies and repairs in order to create additional opportunities for smaller, local suppliers to bid for the provision of goods and services related to catering. This could involve establishing the College's own purchasing framework (similar to the Minor Works and Building Maintenance framework currently being worked on) or comparing quotes from local suppliers for select categories of catering spend.	Head of Procurement APUC	~~End Nov 2024~~ 31 August 2025	**On track** **Revised deadline agreed**
2024/03	Procurement & Creditors	2	Requires Improvement	R3 The College should improve enforcement of compliance in regard to raising POs for relevant transactions. The College should clearly communicate to staff that it is against the College's policy to arrange for the supply of goods or services without an appropriately approved PO and explain to staff how the process helps maintain value for money and minimise supplier risk. Consideration should be given to establishing a more robust "No PO, No Pay" policy, with exclusions explicitly defined and adequately explained to staff members.	Director of Finance	End Sept 2024	**Complete**

Appendix A

Year	Audit Area Report Title	Priority Action Grade	Report Grade	Action	Responsible Officer	Deadline	Progress (as at 21 February 2025)
2024/03	Procurement & Creditors	2	Requires Improvement	R4(ii) The College should communicate to all staff the purpose, importance, and added value of appropriately conducted procurement activity. Staff members should be reminded of the Procurement Policy and procedures in place, and of TRPT's strategic and operational role in managing and assisting with procurement activity. The need for compliance with the established procurement arrangements should be emphasised, and any repeated non-adherence by individuals or departments should be monitored and corrective action taken. A rationale should be given by the purchasing department in any instance where procurement activity has not been conducted in line with the College's guidance.		31 January 2025	**Complete**
2024/03	Procurement & Creditors	2	Requires Improvement	R5 The College should consider re-establishing induction and refresher training for non-procurement staff involved in purchasing and procurement activity. This would help staff to understand the legislative background and enhance their knowledge of business processes and internal governance, as well as familiarising them with TRPT and ensuring that they are aware of the team's strategic and operational role in relation to procurement activity	Head of Procurement APUC	~~End Sept 2024~~ 31 March 2025	**On track** **Revised deadline agreed**

Appendix A

Year	Audit Area Report Title	Priority Action Grade	Report Grade	Action	Responsible Officer	Deadline	Progress (as at 21 February 2025)
2024/03	Procurement & Creditors	2	Requires Improvement	R6(iii) The introduction of built-in system controls in the Sun / P2P systems should be considered, which would require authorisation by an appropriately senior member of the Finance Team prior to any changes to supplier bank details going live and the account being enabled for payment. This would ensure that review and approval is not retrospective, and segregation of duties cannot be circumvented.	Director of Finance	~~End June 2024~~ 31 December 2024	**Complete**
2024/06	2023/24 Student Activity Data	3	NA	**R1** Where academic staff agree that students can defer their studies to the next academic session, confirmation of deferment should be communicated to MIS staff and students flagged as deferred in UNIT-e to ensure that the Credits claim is adjusted for the current year.	Administration Project Manager, and Data Management Team Leader	30 June 2025	**On track**
2024/06	2023/24 Student Activity Data	3	NA	**R2** For students who withdraw from their courses, ensure that the withdrawal date recorded in UNIT-e reflects the last date of physical attendance or engagement	Administration Project Manager, and Data Management Team Leader	30 June 2025	**On track**
2024/06	2023/24 Student Activity Data	3	NA	**R**3 Ensure that Credits claimed for students are based upon the value of the units listed on the student course record, which reflect the activity delivered in the year, and not based upon a default tariff.	Administration Project Manager, and Data Management Team Leader	30 June 2025	**On track**

Appendix A

Year	Audit Area Report Title	Priority Action Grade	Report Grade	Action	Responsible Officer	Deadline	Progress (as at 21 February 2025)
2024/07	2023/24 Student Support Funds	2	NA	**R1** The College should ensure that final checks are performed on the accuracy of the FES data prior to submitting to SFC. As the FES data contains both Credits and support funds data, any changes made to Credits data should be reviewed to ensure that any impact on support funds data is accurate.	Administration Project Manager	30 June 2025	**On track**
2024/08	Sports Centre Business Process Review	High	NA	Arrangements to update systems to conclude on the costs and viability of introducing photo membership cards are under review.	Sports Centre Manager	31 January 2025	**Complete**
2024/08	Sports Centre Business Process Review	High	NA	The potential of conflict between sports centre operations and the wider College first-aid rota are noted and further review (and action as necessary) will be undertaken.	Sports Centre Manager	31 January 2025	**Complete**
2024/08	Sports Centre Business Process Review	Medium	NA	An analysis should be conducted, which includes benchmarking against local competition and stakeholder engagement, in order to allow a revised charging structure to be introduced, which may potentially require a change to exiting conditions for commercial lets.	Business Partnership Manager	30 June 2025	**On track**

Appendix A

Year	Audit Area Report Title	Priority Action Grade	Report Grade	Action	Responsible Officer	Deadline	Progress (as at 21 February 2025)
2024/08	Sports Centre Business Process Review	Medium	NA	A review should be conducted to examine the feasibility of leasing new equipment or outright purchase, depending on whole life costs. This should be informed by a review of the condition of the existing equipment and an estimate of the remaining useful life. It should also be informed by stakeholder consultation with academic staff, students and external users to make sure that any investment in equipment is aligned with identified need. Thereafter a rolling replacement programme should be put in place to ensure that future investment in equipment is built into the budget going forward.	Business Partnership Manager	30 June 2025	**On track**
2024/08	Sports Centre Business Process Review	Medium	NA	As part of the budget setting process, a review of current staffing requirements should be conducted to allow a FTE calculation to be calculated for the delivery of business as usual and seasonal activity (such as the camps run in April and October) and to identify any changes which are required to staff contracts, in collaboration with HR and Finance colleagues (and potentially trade unions), to ensure that there is sufficient clarity for staff around the hours they will work to meet the needs of the sports centre and its internal and external customers(for example a minimum number of contracted hours), whilst providing the flexibility required to ensure that an effective “on call” list can be operated to maintain safe staffing levels (which is akin to the Dundee Leisure model of “support and supply”). This review should also examine the rates of pay for hours worked after 9pm and on Sundays.	Business Partnership Manager	30 June 2025	**On track**

Appendix A

Year	Audit Area Report Title	Priority Action Grade	Report Grade	Action	Responsible Officer	Deadline	Progress (as at 21 February 2025)
2024/08	Sports Centre Business Process Review	Medium	NA	A review should be commissioned which quantifies the investment required to maintain a commercially viable sports centre at Gardyne in order to build a case for future SFC capital funding and partnership funding, in order to protect the ongoing future of the pool and the sports hall facilities.	Business Partnership Manager	30 June 2025	**On track**
2024/08	Sports Centre Business Process Review	Low	NA	We would recommend that a review be conducted to compare the outcomes achieved from the Clubwise system against the outcomes described in the original business case. In addition, we would recommend that the possibility of providing read only access to academic staff to the pool booking system be explored to provide improved visibility	Business Partnership Manager	30 June 2025	**On track**

Agenda Item 10.0

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 4 March 2025

RISK MANAGEMENT POLICY PAPER J

BOARD OF MANAGEMENT

Audit and Risk Committee

Tuesday 4 March 2025

Review of Risk Management Policy

Paper for approval

1. Introduction

The College's Risk Management Policy is subject to rolling review to ensure that it remains up to date and reflective of good practice in risk management. The most recent review reflects the outcomes of the Risk Management training and Risk Appetite setting session undertaken in October 2024.

2. Recommendation

The Audit & Risk Committee is asked to review and approve the revised Risk Management Policy as outlined as Appendix A.

3. Summary of amendments

In line with the outcomes of the risk training and risk appetite work undertaken, it is proposed that an additional section (3.2) be added to the policy as follows:

> 3.2 Board of Management Risk Appetite
>
> The Board of Management will review its risk appetite on an on-going basis in line with the arrangements in place through the Government HM Treasury 'Orange book' arrangements. This appetite will be used to establish the level at which specific risks become of most concern and are then subject to more detailed review and scrutiny at each subsequent meeting.
>
> This will be determined relative to the following guidance linking the risk appetite for a specific group of risks to the post mitigation score and categorisation of that risk.

Risk Classification	Post Mitigation Risk Score	Colour	Risk Appetite
Minor	1 - 3	🟦	1 Avoid
Moderate	4 - 8	🟩	2 Averse
Significant	9 - 15	🟧	3 Moderate
Major	16 - 20	🟥	4 Open
Fundamental	21 - 25	🟪	5 High

> Using this approach, where the post mitigation of a specific risk is 16, which places it in the MAJOR band, but the risk appetite level set by the Board was 3 – Moderate, this would require the risk to be subject to a focused review and update at each subsequent meeting of the Board of Management Audit & Risk Committee.
>
> Conversely, where the post mitigation risk was 16, which places it in the MAJOR band, but the risk appetite level set by the Board was 4 – Open, the risk would still be subject to normal regular review but would not require a focused review and update at each subsequent meeting of the Board of Management Audit & Risk Committee.

Irrespective of the above, in all cases where a post-mitigation risk is highlighted as purple, this will be subject to review on a daily or weekly basis as appropriate and regular updates and engagement enacted with the Board of Management. Formal updates will be subject to review at each subsequent meeting of the Board of Management Audit & Risk Committee and/or full Board as determined by the Principal and Board Chair.

Alongside this additional section, the references noted in the policy will be amended to include reference to the HM Treasury Orange book.

4. Link to Strategic Risk Register

Consideration of the options suggested in this report will support the identification and mitigation of risk across all College activities

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

Dundee & Angus College

Summary of outputs from the Risk Appetite session conducted with the Board and senior managers

January 2025

Henderson Loggie

Contents

Risk Appetite Session

Background

At the request of the Vice Principal Support Services and Operations, a face to face session was arranged at the Kingsway Campus on 22 October 2024, to be delivered by David Archibald, Partner and Head of Internal Audit in Henderson Loggie. The purpose of the session was to deliver a facilitated risk appetite session with the College Board, which would also be attended by the College Executive Team.

Approach

In advance of the risk appetite session on 22 October 2024, an extract from the updated Government Finance Function 'Risk Appetite Guidance Note' August 2021 was issued for consideration by the Vice Principal Support Services and Operations. This document sets out 13 potential risk categories, which can be scored from a risk appetite perspective, on a five-point scale from Averse to Eager. These are drawn from the HM Treasury Orange Book 2020.

The Orange Book – Management of Risk, Principles and Concepts (2020) advises that '*the Board should determine and continuously assess the nature and extent of the principal risks that the organisation is exposed to and is willing to take to achieve its objectives – its risk appetite – and ensure that planning and decision-making reflects this assessment. Effective risk management should support informed decision-making in line with this risk appetite, ensure confidence in the response to risks, transparency over the principal risks faced and how these are managed'.*

The Risk Appetite Guidance Note was developed by risk practitioners in the public sector to support colleagues in implementing effective risk management arrangements, aligned with the Orange Book principles. The guidance note defines risk appetite as "*a concept is often referenced in organisations, without clearly defining what it is. Similarly, the terms risk appetite and risk tolerance are often used interchangeably. It is equally true that many organisations already apply the principles contained in this guidance without necessarily fully acknowledging them as part of a risk management framework where risk appetite is actively considered in decision-making*".

Risk appetite provides a framework which enables an organisation to make informed management decisions. By defining both optimal and tolerable positions, an organisation clearly sets out both the target and acceptable position in the pursuit of its strategic objectives. The benefits of adopting a risk appetite include:

- Supporting informed decision-making
- Reducing uncertainty
- Improving consistency across governance mechanisms and decision-making;
- Supporting performance improvement
- Focusing on priority areas within an organisation
- Informing spending review and resource prioritisation processes.

It was agreed that a total of 8 risk categories would be scored at the session on 22 October 2024. These are summarised in Appendix 1, below.

The example appetite levels, as defined by the risk categories set out in the Orange Book (for the 8 risk categories selected – see Appendix 1), were assessed in Groups and then discussed in a plenary session by those attending the 22 October 2024 risk appetite session (either in-person or joining online). The plenary session contained both Board members and senior managers. Each risk category was discussed in turn, with positive engagement evident from all attendees, in order to arrive at a shared consensus for the risk appetite level for each of the 8 risk categories scored. These are summarised in the table below.

Risk Appetite Session

Summary of Risk Appetite scores agreed

Risk Category	Risk Score
1. Strategy	4 - Open
2. Operations	4 - Open
3. Financial	4 - Open
4. Commercial	4 - Open
5. People	4 - Open
6. Technology	4 - Open
7. Project / Programme	4 - Open
8. Reputational	4 - Open but verging to 3 – Cautious

Actions

Action Point 1 - As part of the discussion it was agreed that a review of delegated authority limits and reports / information provided to inform the Board of around outcomes and risks associated with activities delegated through the Scheme of Delegation.

Action Point 2 – As part of the plenary discussion on the Reputational risk category it was agreed that further work was required to define precisely what this category means to Dundee & Angus College to better inform the risk management, mitigation and reporting arrangements in this area.

Linking the risk appetite to individual risk scores

As highlighted during the session on 22 October 2024, one of the key challenges when setting a risk appetite is how to connect this assessment across into routine risk reporting. From our perspective, one of the ways to achieve this is by subdividing your risk matrix into five sections, rather than your current four sections, with thresholds set to differentiate between various risk scores from 1 to 25.

The current categorisation of individual risks on your Strategic Risk Register is as follows:

Green (1-8) = Minor Risk;
Amber (9-15) = Significant Risk
Red (16-20) = Major Risk
Purple, (>21 - 25) = Fundamental Risk

Risk Appetite Session

We connected the risk appetite scoring to your individual risk scoring matrix by sub dividing your current **MINOR** risk band into two distinct bands (MODERATE and MINOR). The remaining bands remain unchanged. One of the benefits of this approach is that it allows senior managers to identify any risks where the residual (or net) risk score, after mitigation, is above the risk appetite level set by the Board. An example table which shows how you could connect the risk matrix (scored from 1 to 25) with your risk appetite (scored from Averse to Eager – or 1 to 5) is shown below.

Risk Classification	Risk Score	Colour	Risk Appetite Score
FUNDAMENTAL	Risks with a score of 21 and above	🟪	5 – High
MAJOR	**Risks with a score of between 16 and 20**	🟥	4 - Open
SIGNIFICANT	Risks with a score of between 9 and 15	🟨	**3 - Moderate**
MODERATE	Risk with a score of between 4 and 8	🟦	2 - Averse
MINOR	Risks with a score of 3 or lower	🟩	1 - Avoid

So, in the table above we have a scenario where the net (or residual) risk score after mitigation for a Financial risk is **16**, which places it in the **MAJOR** band. But the risk appetite level set by the Board is **3 - Moderate** for this category of risk (Financial risks)**,** which equates to the **SIGNIFICANT** band**.** So, for this financial risk there is a mismatch between the residual risk score set by management (a score of 16 on the 5 x 5 scale for the risk register) and the risk appetite level set by the Board (3 – Cautious), which should drive a discussion around potential mitigations at future Board meetings.

Acknowledgement

We would like to take this opportunity to thank all the College Board members and Executive Team who attended the risk appetite session on 22 October 2024.

Appendix 1 - Orange Book Example Risk Categories

The Orange Book recommends risks should be organised by taxonomies or categories of risk. Grouping risks in this way supports the development of an integrated and holistic view of risks. These are not intended to be exhaustive. Failure to manage risks in any of these categories may lead to financial, reputational, legal, regulatory, safety, security, environmental, employee, customer and operational consequences.

Strategy risks – Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment (e.g. political, economic, social, technological, environment and legislative change).

Operations risks – Risks arising from inadequate, poorly designed or ineffective/inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money.

Financial risks – Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.

Commercial risks – Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and /or failure to meet business requirements/objectives.

People risks – Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.

Technology risks – Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience. Information risks – Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.

Project/Programme risks – Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.

Reputational risks – Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations.

Henderson
Loggie

Appendix A

RISK MANAGEMENT POLICY

College Policy No	**PP06**
Approved by	**Audit & Risk Committee**
Original Issue Date	**30/09/2015**
Current Issue Date	**06/03/2025**
Review Date	**01/04/2028**

CONTENTS

1 PURPOSE

The purpose of this policy and related arrangements is to:

- outline approaches and arrangements in respect of the management, oversight, control, mitigation, evaluation and reporting of risks associated with College operations and activities;
- ensure that significant risks are monitored and managed more closely; and
- confirm the roles and responsibilities of the Board of Management, Senior Leadership team and others in the effective management of risks.

2 SCOPE

This policy covers the management of financial, strategic, operational, reputational and project-based risks related to all aspects of College activities and operations, including those where the College is operating in partnership with others.

This policy is approved by the Audit & Risk Committee of the Board of Management and will be subject to regular review by the Committee in line with College document control and review procedures.

It should be noted that this policy is does not cover arrangements in respect of health and safety risk assessment which is managed under the terms of the College Health and Safety Policy.

3 IDENTIFICATION AND MANAGEMENT OF RISKS

The development of effective risk management arrangements are essential to control and manage the risks that may otherwise threaten the ability of the College to meet its objectives.

Risk management is bound inextricably within the system of internal control that operates across the College. This system encompasses a number of elements that together ensure that effective and efficient outcomes are achieved, allowing the College to respond to strategic and operational risks. These elements include the following.

3.1 Strategic Risk Framework

High level strategic risks are outlined within a clear risk register that links directly to the College Strategy and key outcomes as outlined through Outcome Agreements and strategic priorities. These risks are discussed and approved by the full Board of Management two times per year. This framework is integrated with strategic planning arrangements and relates directly to strategic developments and detailed analysis of the regional operating context for the College.

Within these arrangements, the Executive Leadership Team undertake the ongoing monitoring and mitigation of risks significant to the College. The strategic risk register is formally reviewed and updated quarterly through the Board of Management Audit & Risk Committee.

Risks are managed based on a series of risk factors determined by assessment of the likelihood multiplied by the impact of each specific risk using a scale of 1 (low) to 5 (high).

Guidance on the scoring of risks is as follows and is indicative rather than prescriptive, with judgement required in respect of the assessment of differing types of risk (operational, financial, reputational etc):

Score	Likelihood Description (assessed likelihood over a rolling 5 year period)	Impact Description
1	Highly Unlikely. The likelihood of the risk arising is minimal (<5% likelihood of arising).	Minimal: If the risk does arise the impact of this is not felt to be significant in respect of the operation of the College and would be managed through normal arrangements.
2	Unlikely. Risks at this level are unlikely to arise but are possible (>5% but <25% likelihood of arising).	Minor: If the risk does arise it would cause slight disruption or impact on College operations requiring management input to resolve but not impacting on significant whole services, projects or activities. Impact could be mitigated without significant difficulty and/or would exist for a short period of time. Resolution would be achieved through normal work arrangements and budgets.
3	Possible. The likelihood of the risk arising is possible and instances would not be unexpected. (>26% but <50% likelihood of arising).	Moderate. Risk would have a noticeable impact or disruption to the operation of large scale functions (or multiple smaller functions) of the College and would require specific focused management input to resolve. This may require allocation of specialist input and reallocation or re-prioritisation of budget.
4	Likely. Risks in this category are probably and it is anticipated that these will arise (>50% but <75% likelihood of arising)	Major. Risk would have a substantial impact on the ability of the College to operate, covering multiple large functions or activities for a prolonged period. Major risks are likely to require the enactment of specific remedial measures and/or business continuity responses. It would be expected that this may require allocation of specialist input and additional (unplanned) budget.
5	Almost certain. The likelihood of the risk arising is almost certain. (>75% likelihood of arising).	Critical/Catastrophic. Risk would have a severe impact on the ability of the college to operate covering all operations (or multiple large functions or activities) for a prolonged period. Major risks are likely to require the enactment of specific remedial measures and/or business continuity responses. It would be expected that this would require allocation of specialist input and significant additional (unplanned) budget.

Each risk factor is then colour coded as follows:

Colour Code	Description	Scoring Range
Blue	**(Low risk factor - Minor risk)** Risks in this category are considered very minor and unlikely to cause any disruption. They are managed through routine procedures and do not require special attention.	1 - 3
Green	**(Low risk factor - Moderate risk)** Risks in this category are considered minor and unlikely to cause significant disruption. They are typically managed through routine procedures and review and do not require special attention.	4 - 8
Amber	**(Medium risk factor - Significant risk) 9 - 15**: These risks are more significant and could potentially impact operations or objectives. They require active management and monitoring to ensure they do not escalate.	9 - 15
Red	**(High risk factor - Major risk) 16 - 20**: High-risk factors are likely to have a substantial impact on the organisation. They demand immediate and robust mitigation strategies and are closely monitored by senior management and the Audit & Risk Committee.	16 -20
Purple	**(Very High risk factor - Fundamental risk) 21 and above**: Risks in this category are critical and pose a fundamental threat to the organisation's viability. They require urgent and comprehensive action plans and are subject to continuous review at the highest levels of management and through the Board of Management.	21 and above

Each risk is assessed and categorised prior to the actions taken to manage the risk and again following assessment of the mitigating actions in place.

3.2 Board of Management Risk Appetite

The Board of Management will review its risk appetite on an on-going basis in line with the arrangements in place through the Government HM Treasury 'Orange book' arrangements. This appetite will be used to establish the level at which specific risks become of most concern and are then subject to more detailed review and scrutiny at each subsequent meeting.

This will be determined relative to the following guidance linking the risk appetite for a specific group of risks to the post mitigation score and categorisation of that risk.

Risk Classification	Post Mitigation Risk Score	Colour	Risk Appetite
Minor	1 - 3	🟦	1 Avoid
Moderate	4 - 8	🟩	2 Averse
Significant	9 - 15	🟧	3 Moderate
Major	16 - 20	🟥	4 Open
Fundamental	21 - 25	🟪	5 High

Using this approach, where the post mitigation of a specific risk is 16, which places it in the MAJOR band, but the risk appetite level set by the Board was 3 – Moderate, this would require the risk to be subject to a focused review and update at each subsequent meeting of the Board of Management Audit & Risk Committee.

Conversely, where the post mitigation risk was 16, which places it in the MAJOR band, but the risk appetite level set by the Board was 4 – Open, the risk would still be subject to normal regular review but would not require a focused review and update at each subsequent meeting of the Board of Management Audit & Risk Committee.

Irrespective of the above, in all cases where a post-mitigation risk is highlighted as purple, this will be subject to review on a daily or weekly basis as appropriate and regular updates and engagement enacted with the Board of Management. Formal updates will be subject to review at each subsequent meeting of the Board of Management Audit & Risk Committee and/or full Board as determined by the Principal and Board Chair.

3.2 Outcome Agreement and Assurance (OA) Planning

The national measurement planning arrangements linked to the Outcome Agreement and Assurance models are used to set outcome targets and objectives, inform budget plans, and identify risks associated with many College activities. Progress towards meeting OA activity plans is reviewed through the use of the National Assurance Model arrangements and is monitored on a rolling basis throughout the year and reported through the annual OA self-evaluation report.

3.3 Quality Management System

The College operates a documented quality management system based around ISO9001 principles. This system provides a clear structure of policies, procedures, quality processes and other documentation that underpin the control and review of key College processes and their related risks.

All sections of the quality management system are approved at Executive Leadership Team level, with reference to the Board of Management where appropriate.

3.4 Operational Risk Framework

Managers ensure that significant risks related to the outcomes, activities and operational objectives of their area of responsibility are identified, assessed and monitored. Operational risks are appraised on a rolling basis through team/service/project meetings and emerging risks are communicated and managed as required. Where necessary, the impact of risks in respect of the achievement of operational outcomes is detailed within operational plans and self-evaluation records.

3.5 Determination and Management of Project-Based Risks

Approval of capital and revenue projects where College contribution is in excess of £500k in value will include the requirement to create and manage a specific risk register in relation to the project or activity. This determination and rating of risk must include the following.

- Risks impacting on project/College objectives.
- Significant financial and other operational risks.
- Reputational or other risks

Project based risk registers may be necessary in other circumstances where the nature of the project or the level of non-financial risk involved warrants this.

3.6 Financial Risks

The quarterly management accounts and outturn forecast reports provided to the Finance & Property Committee highlight the key risks and sensitivities underpinning the financial monitoring and planning being undertaken. These risks are reviewed at each Finance & Property Committee meeting, with this information shared with the full board to enhance awareness of the ongoing financial position and risks associated with this.

3.7 Internal Audit Arrangements

The Board of Management Audit & Risk Committee determines and approves a rolling annual schedule of internal audit activities designed to check and test internal control and risk management arrangements. Analysis and feedback in respect of risk and control issues is used to inform development and prioritisation of this schedule. The schedule includes the internal audit review of risk management approaches, arrangements, and effectiveness.

3.8 External Audit Arrangements

External audit provides feedback to the Audit & Risk Committee on the operation of the internal controls reviewed as part of the annual audit requirements specified by the Scottish Government and Scottish Funding Council.

3.9 Quality and Third-Party Monitoring

Internal and external reviews and reports in respect of the achievement of required outcomes and compliance with systems are used to inform potential risks and to strengthen internal control systems as appropriate.

3.10 Management Reporting Arrangements

Regular reporting through a range of management channels including Executive and Senior Leadership Team meetings; team and service meetings; Stop and Review activities; and project and system planning groups is designed to monitor key risks and their controls.

Decisions to address changes in the risk profile are made through these regular reporting activities and priorities, impacts or concerns are reported to the Senior Leadership Team and/or the Board, as necessary.

To underpin these arrangements extensive use is made of clear and comprehensive data through real-time reporting from College systems and the development and review of a broad range of business intelligence dashboards and reports.

3.11 Annual Report Arrangements

The Board of Management is responsible for reviewing annually the effectiveness of risk management arrangements and outcomes, based on information provided by the independent auditors (internal and external) and the Executive Leadership Team.

To inform this the Audit & Risk Committee will consider annually a report produced by the internal auditors that summarises the outcomes of audit activities and provides a clear opinion in respect of the robustness of the internal controls in place and any other significant factors found.

Detailed evaluation reports in respect of the achievement of key College outcomes and on the quality of learning, teaching and services will be discussed and approved annually by the full Board (or relevant Committee). These will be considered alongside financial performance and other metrics as considered appropriate.

3.12 Business Continuity Planning and Disaster Recovery

The College maintains a business continuity plan providing a framework within which serious incidents or other significant events that may impact on business continuity are managed.

Business continuity and disaster recovery arrangements are scenario tested on a regular basis by the Senior Leadership Team. The outcomes of scenario testing will be used to improve arrangements as appropriate.

Business continuity testing will include testing against unquantifiable ‘black swan risks’ to ensure that plans and approaches are as resilient as they can be in respect of unexpected and unconsidered high impact risks.

4 RESPONSIBILITIES

4.1 Role of the Board of Management

The Board of Management has responsibility to provide leadership within a framework of effective controls which enable risk to be assessed and managed. The Board of Management has responsibility through the operation of the Board and each Board Committee to monitor, challenge and overseeing risk management within the College as a whole.

Within all of these arrangements it is the responsibility of the Board of Management to:

- Establish the overall culture and ethos in respect of risk and opportunity management within the College.
- Determine the appropriate risk appetite (the level of exposure with which the Board is comfortable) for the College that balances risk with opportunity.
- Approve major decisions affecting the College risk profile or exposure in accordance with appropriate financial strategy and procedures and agreed delegation limits
- Ensure that risk management is integrated in strategic planning activities and outcome agreements.
- Monitor the management of key risks (those rated in excess of the risk appetite) to reduce their probability and impact.
- Satisfy itself that the less significant risks are managed, and that risk controls are in place and working effectively.
- Annually review the College approach to risk management and approve changes or improvements as necessary.

Each Board Committee reviews the strategic risks allocated to its area of responsibility on a quarterly basis, making recommendations on change to the Audit & Risk Committee as appropriate.

4.2 Role of the Audit & Risk Committee

The Board of Management has delegated responsibility for risk management to the Audit & Risk Committee.

The Audit & Risk Committee will monitor and report to the Board on internal controls and alert Board members to any significant emerging issues. In addition, the Committee oversees internal audit, external audit and management as required in its review of internal controls.

The Audit & Risk Committee will report to the Board annually on the effectiveness of the internal control system, including the College system for the management of risk.

4.3 Role of the Senior Leadership Team

As the senior management group of the College, the Senior Leadership Team have overall operational responsibility for the identification, management and mitigation of risk in line with Board objectives and risk appetite.

It is the role of the Senior Leadership Team to provide advice and guidance to the Board in respect of potential and actual risk issues and to implement appropriate risk management and internal controls on an on-going basis. Senior Leadership Team members will also be asked to provide accurate, timely and clear information to the Board of Management and its Committees to support board members in understanding and evaluating the status of risks and controls.

Within these responsibilities, the Vice Principal Support Services and Operations and the Audit & Risk Committee will review annually the effectiveness of the system of internal control and provide a report on this to the Board of Management through the Audit & Risk Committee.

4.4 Role of Managers

All staff with a management or team leadership role are responsible for ensuring that good risk management practices are developed and adopted within their area of responsibility.

5 IMPLEMENTATION

To support implementation of this policy all staff with responsibilities under the terms of the policy will receive appropriate guidance, support and training in relation to these responsibilities.

6 REFERENCES

- Board of Management Articles and Committee Remits
- Code of Good Governance for Scotland’s Colleges
- Strategic risk register
- Regional Outcome Agreement
- Quality Manual
- Finance Procedures
- Internal audit schedule and reporting
- Business Continuity Plan
- UK Treasury ‘Orange Book’

7 REVIEW DETAILS

Next Review Scheduled for:	1 April 2028
Responsibility for Review:	Audit Committee and Vice Principal (Support Services & Operations)
Union Consultation Required:	No

Agenda Item 11.0

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 4 March 2025

STRATEGIC RISK REGISTER PAPER K

BOARD OF MANAGEMENT
Audit and Risk Committee
Tuesday 4 March 2025

Strategic Risk Register Update

Paper for approval

1. Strategic Risk Register

A copy of the March 2025 draft Strategic Risk Register is enclosed. This is noted for approval.

2. Board of Management Risk Scoring and Risk Appetite Outcomes

Board members undertook an awareness raising and risk appetite review session as part of the Board Development workshop on 22 October 2024. A summary report outlining the outcomes of this session was considered under the previous item.

Work was also progressed following the spring 2004 Risk Management audit to create clearer guidance in respect of the scoring of risk likelihood and impact (pre and post mitigation). Following this change it was agreed that the Strategic Risk Register be reviewed in line with the more detailed guidance to revise and better align scoring.

These tasks have been completed and the scoring (pre and/or post mitigation of risks has been amended in sixteen instances. In fourteen of these cases the change has resulted in a reduced risk score due to application of the revised scoring methodology rather than any change in respect of the actual risk itself. Changes in respect of the two increased risks due to changes in the college environment are noted below.

3. 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 cuts in sector funding, 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 the More Successful and Sustainable College plans and updates shared with all Board members since initial publication in April 2023.

The appropriate curriculum, HR and financial plans and approaches underpinning the paper and progress around the proposals it contained have been discussed at each meeting of the Learning, Teaching and Quality; Human Resource & Development; and Finance & Property Committee over the past year.

The 2023/24 annual accounts and financial statements confirm that the College has achieved a cash backed surplus for 2023/24, with this supporting the overall cash position. Whilst this is a positive outcome, it is recognised that the current year position has deteriorated against budget and that action will need to be taken over the remainder of the year to rectify this position.

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.

The changes planned to risk management practice outlined earlier in the agenda will reduce the requirement for detailed reporting at every meeting, although it is still recommended that updates on the most significant risks continue to be reflected at future Audit and Risk Committees.

4. Reinforced Autoclaved Aerated Concrete (RAAC) Risk

An update on the most up to date picture regarding the RAAC present within the Kingsway Campus was shared with the Board in December, with the additional RAAC discovered in parts of the Kingsway tower representing a significant increase in concern. All required mitigations remain in place relative to the specialist structural engineering advice received and outline plans are in place should any subsequent change in advice limit the use of accommodation.

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. A further update will be provided at the next Board meeting.

5. Review of Strategic Risk Register

The draft March 2025 Strategic Risk Register is enclosed with the following changes recommended in respect of Strategic risks.

In addition to the fourteen risks amended in respect of either the pre and/or post mitigation scoring, the further amended risks have increased and are highlighted for approval:

No	Risk	Change Proposed
2.6	Demands of capital developments / maintenance impacts on financial sustainability or delivery of learning and/or services	Pre and post mitigation risk increased to reflect the increasing demands placed on maintenance requirements given the age and condition of campuses and campus infrastructure
4.5	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	Pre and post mitigation risk increased in line with the above assessment and as a result of the increased presence of RAAC within the Kingsway campus.

6. 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

2024 - 2025

As at March 2025

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 2	4 ↓ 8	• 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 3	8 ↓ 12	• 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	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
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 4	3 4	9 ↓ 16	• Negotiation/influence at national level • Review of activities/ projects and response to new opportunities	3 4	1	3 ↓ 4	• 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 4	2	6 ↓ 8	• 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	ELT	Executive Leadership Team	Prin	Principal	**Score**	**Impact**	**Likelihood**
	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&P**	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 3	8 ↓ 9	• 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&P**	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	ELT	Executive Leadership Team	Prin	Principal	Score	Impact	Likelihood
	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**
2	**Financial (cont)**									
2.3 **F&P**	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 4	3	9 12	• Strong financial controls: segregation of duties and review of transactions. • Review of impact of any changes in structure or duties • Whistleblowing arrangements	2 3	2	4 ↓ 6	• Continuous review of financial controls • Internal Audit programme	VPSO
2.5 **F&P**	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&P**	Demands of capital developments / maintenance impacts on financial sustainability or delivery of learning and/or services	4 3	4 2	16 ↑ 6	• Multi-year estates strategy and capital planning • Lobbying of SFC on capital and backlog maintenance funding • Planning for D&A Foundation bids	4 2	3 2	12 ↑ 4	• 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

	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 3	2	4 ↓ 6	• 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 5	16 ↓ 20	• 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	ELT	Executive Leadership Team	Prin	Principal	Score	Impact	Likelihood
	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 (cont.)									
3.4 HR&D	Failure to meet the aspirational standards in respect of the health, safety, wellbeing and development of staff and students	4 3	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 3	8 ↓ 12	• Marketing strategy • Reputation plan • Positive marketing approaches	3 4	2 3	6 ↓ 12	• Stakeholder engagement • Social media monitoring arrangements	VPCP, DirC&A
3.6 HR&D	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	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			

	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 (cont.)**									
3.7 **HR&D**	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 **HR&D**	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

	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 (cont.)**									
3.10 **HR&D**	College arrangements do not minimise risk associated with Modern Slavery	4	2 3	8 ↓ 12	• Clear and compliant procurement arrangements and procedures • Staff identity checking arrangements and use of PVG.	3 4	1	3 ↓ 4	• 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 4	15 ↓ 20	• 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	ELT	Executive Leadership Team	Prin	Principal	**Score**	**Impact**	**Likelihood**
	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 (cont.)**									
3.12 **HR&D**	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	ELT	Executive Leadership Team	Prin	Principal	**Score**	**Impact**	**Likelihood**
	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**
4	**Infrastructure**									
4.1 **A&R**	Major Disasters – eg Fire, MIS Failure, Failure of Emergency Procedures, RAAC or similar infrastructure failure	5	3 4	15 ↓ 20	• 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&P**	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 4	2	6 ↓ 8	• 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	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	Responsibility
4	**Infrastructure**									
4.5 **F&P**	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 4	20 ↑ 16	• 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 3	4	16 ↑ 12	• Lobbying of SG and SFC on campus vision and needs • Prioritization 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.

Strategic Risk Framework

High level strategic risks are outlined within a clear risk register that links directly to the College Strategy and key outcomes as outlined through Outcome Agreements and strategic priorities. These risks are discussed and approved by the full Board of Management two times per year. This framework is integrated with strategic planning arrangements and relates directly to strategic developments and detailed analysis of the regional operating context for the College.

Within these arrangements, the Executive Leadership Team undertake the ongoing monitoring and mitigation of risks significant to the College. The strategic risk register is formally reviewed and updated quarterly through the Board of Management Audit & Risk Committee.

Risks are managed based on a series of risk factors determined by assessment of the likelihood multiplied by the impact of each specific risk using a scale of 1 (low) to 5 (high).

Guidance on the scoring of risks is as follows and is indicative rather than prescriptive, with judgement required in respect of the assessment of differing types of risk (operational, financial, reputational etc):

Score	Likelihood Description (assessed likelihood over a rolling 5 year period)	Impact Description
1	Highly Unlikely. The likelihood of the risk arising is minimal (<5% likelihood of arising).	Minimal: If the risk does arise the impact of this is not felt to be significant in respect of the operation of the College and would be managed through normal arrangements.
2	Unlikely. Risks at this level are unlikely to arise but are possible (>5% but <25% likelihood of arising).	Minor: If the risk does arise it would cause slight disruption or impact on College operations requiring management input to resolve but not impacting on significant whole services, projects or activities. Impact could be mitigated without significant difficulty and/or would exist for a short period of time. Resolution would be achieved through normal work arrangements and budgets.
3	Possible. The likelihood of the risk arising is possible and instances would not be unexpected. (>26% but <50% likelihood of arising).	Moderate. Risk would have a noticeable impact or disruption to the operation of large scale functions (or multiple smaller functions) of the College and would require specific focused management input to resolve. This may require allocation of specialist input and reallocation or re-prioritisation of budget.
4	Likely. Risks in this category are probably and it is anticipated that these will arise (>50% but <75% likelihood of arising)	Major. Risk would have a substantial impact on the ability of the College to operate, covering multiple large functions or activities for a prolonged period. Major risks are likely to require the enactment of specific remedial measures and/or business continuity responses. It would be expected that this may require allocation of specialist input and additional (unplanned) budget.

Score	Likelihood Description (assessed likelihood over a rolling 5 year period)	Impact Description
5	Almost certain. The likelihood of the risk arising is almost certain. (>75% likelihood of arising).	Critical/Catastrophic. Risk would have a severe impact on the ability of the college to operate covering all operations (or multiple large functions or activities) for a prolonged period. Major risks are likely to require the enactment of specific remedial measures and/or business continuity responses. It would be expected that this would require allocation of specialist input and significant additional (unplanned) budget.

Each risk factor is then colour coded as follows:

Colour Code	Description	Scoring Range
Blue	**(Low risk factor - Minor risk)** Risks in this category are considered very minor and unlikely to cause any disruption. They are managed through routine procedures and do not require special attention.	1 - 3
Green	**(Low risk factor - Moderate risk)** Risks in this category are considered minor and unlikely to cause significant disruption. They are typically managed through routine procedures and review and do not require special attention.	4 - 8
Amber	**(Medium risk factor - Significant risk) 9 - 15**: These risks are more significant and could potentially impact operations or objectives. They require active management and monitoring to ensure they do not escalate.	9 - 15
Red	**(High risk factor - Major risk) 16 - 20**: High-risk factors are likely to have a substantial impact on the organisation. They demand immediate and robust mitigation strategies and are closely monitored by senior management and the Audit & Risk Committee.	16 -20
Purple	**(Very High risk factor - Fundamental risk) 21 and above**: Risks in this category are critical and pose a fundamental threat to the organisation's viability. They require urgent and comprehensive action plans and are subject to continuous review at the highest levels of management and through the Board of Management.	21 and above

Each risk is assessed and categorised prior to the actions taken to manage the risk and again following assessment of the mitigating actions in place.

Board of Management Risk Appetite

The Board of Management will review its risk appetite on an on-going basis in line with the arrangements in place through the Government HM Treasury 'Orange book' arrangements. This appetite will be used to establish the level at which specific risks become of most concern and are then subject to more detailed review and scrutiny at each subsequent meeting.

This will be determined relative to the following guidance linking the risk appetite for a specific group of risks to the post mitigation score and categorisation of that risk.

Risk Classification	Post Mitigation Risk Score	Colour	Risk Appetite
Minor	1 - 3	🟦	1 Avoid
Moderate	4 - 8	🟩	2 Averse
Significant	9 - 15	🟧	3 Moderate
Major	16 - 20	🟥	4 Open
Fundamental	21 - 25	🟪	5 High

Using this approach, where the post mitigation of a specific risk is 16, which places it in the MAJOR band, but the risk appetite level set by the Board was 3 – Moderate, this would require the risk to be subject to a focused review and update at each subsequent meeting of the Board of Management Audit & Risk Committee.

Conversely, where the post mitigation risk was 16, which places it in the MAJOR band, but the risk appetite level set by the Board was 4 – Open, the risk would still be subject to normal regular review but would not require a focused review and update at each subsequent meeting of the Board of Management Audit & Risk Committee.

The Board of Management determined in October 2024 that its risk appetite was Open across the following factors:

- Strategy
- Operations
- Financial
- Commercial
- People
- Technology
- Project/Programme Management
- Reputational*

*Reputational was subject to significant discussion between Open and Cautious.

Irrespective of the above, in all cases where a post-mitigation risk is highlighted as purple, this will be subject to review on a daily or weekly basis as appropriate and regular updates and engagement enacted with the Board of Management. Formal updates will be subject to review at each subsequent meeting of the Board of Management Audit & Risk Committee and/or full Board as determined by the Principal and Board Chair.

Agenda Item 13.0

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 4 March 2025

DATE OF NEXT MEETING

Tuesday 3 June 2025 at 5:00pm in Room K-TO-624, Kingsway Campus