BOARD OF MANAGEMENT

Audit and Risk Committee

Tuesday 5 March 2024 at 5.00pm **Room A625, Kingsway Campus** (MS Teams option available)

AGENDA

1.	**WELCOME**		
2.	**APOLOGIES** Welcome to David Robertson from the Higher Education/Further education Shared Technology and Information Service (HEFESTIS) Welcome to Nicky Anderson, Director of Finance and Andy Ross, Director of Infrastructure		
3.	**DECLARATIONS OF CONNECTION & INTEREST**		
4.	**MINUTE OF THE PREVIOUS A&R AND JOINT A&R / F&P MEETINGS** – 5 December 2024	Paper A & B for approval	
5.	**MATTERS ARISING**	Paper C for noting	
6.	**HEFESTIS ANNUAL CYBER SECURITY RISK & MATURITY REPORT**	Paper D for information	DR/AR
7.	**INTERNAL AUDIT**		
	6.1. Risk Management & Business Continuity	Paper E for approval	HL
	6.2. 2023/24 Progress Report	Paper F for information	HL
	6.3. Follow Up Summary	Paper G for information	ST
8.	**STRATEGIC RISK REGISTER**		
	(i) Risk Register Update (ii) Strategic Risk Register	Paper H for approval	ST
9.	**EXTERNAL AUDIT**	Verbal update	MS
10.	**DATE OF NEXT MEETING** – Tuesday 4 June 2024 at 5.00pm in Room A625, Kingsway Campus		

Agenda Item 4.0

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 5 March 2024

MINUTE OF THE PREVIOUS A&R AND JOINT A&R/F&P MEETINGS

PAPER A & B

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 5 December 2023

Minute of the Audit & Risk Committee meeting held on Tuesday 5 December 2023 at 4.30pm in Room A605 Kingsway Campus and via Microsoft Teams

PRESENT:	H Honeyman (Chair Audit) L O'Donnell (observing)	S Middleton
IN ATTENDANCE:	S Taylor (Vice Principal) M Speight (Mazars) R Holland (Mazars)	P Muir (Board Administrator) S Macnaught (Henderson Loggie)

1. **WELCOME**

   H Honeyman welcomed members of the Audit & Risk Committee and welcomed 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 K Ditcham, M Williamson, R McLellan, J Buchanan and D Archibald.

3. **DECLARATIONS OF INTEREST OR CONNECTION**

   There were no declarations.

4. **MINUTE OF THE PREVIOUS MEETING** – 19 September 2023

   The minutes of the Audit and Risk Committee meeting held on 19 September 2023 were approved as an accurate record.

5. **MATTERS ARISING**

   Matters arising from previous meetings were closed with one remaining open in respect of the meeting between the Committee chair and M Speight from Mazars. H Honeyman noted that she would contact M Speight to arrange to catch up.

6. **AUDIT & RISK COMMITTEE ANNUAL REPORT TO THE BOARD**

   S Taylor summarised the report drafted for submission to the board.

   S Taylor confirmed that the points highlighted within the report are now complete and approved with no concerns regarding any internal matters.

The Committee reviewed the Annual Audit Report and related work and expressed satisfaction with the assessment provided. In terms of the contribution from the External Auditor, the Committee were pleased with the support provided by the external audit team, the process and the performance and effectiveness of the External Audit team throughout the financial year.

The annual report was approved for circulation to the Board of Management on 12th December 2023. **H Honeyman to progress.**

7. INTERNAL AUDIT

7.1. Student Activity

S Macnaught 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 Macnaught highlighted one recommendation related to credits claimed. This was to ensure any significant change to the credits claimed after audit sampling were brought to auditors' attention on a timely basis to be considered for testing prior to conclusion of the audit fieldwork stage. The second recommendation highlighted the importance of attendance reports which should be maintained on CELCAT to support the actual hours completed and credits claimed.

H Honeyman and S Middleton queried the credit claim procedure and the procedures in place to prove students' attendance and to prevent any reoccurrence. S Taylor highlighted that the student activity in question was affected by their employers and work schedules, so was complex to plan and record.

The report was approved.

7.2. Student Support Funds

S Macnaught summarised the report on the discretionary, hardship, bursary, childcare, and EMA funds highlighting that the testing and audit work undertaken had highlighted that the national policies were being followed and there were no issues to be brought to the Committee.

A couple of observations were noted around the small EMA overclaim of £30 which had been adjusted by the College in the monthly return for August 2023.

In addition to this, another point noted during the audit was the acknowledgment of award letters. It was highlighted there were occasions where re-award letters were not issued. Requirements have been reiterated to all staff involved in the re-assessment of awards, and sample checks to be conducted as part of on-going inspections. S Middleton highlighted the importance of a paper trail of award letters issued and received. S Taylor stated he was happy to reinforce recommendations to improve the student award letter process, and noted that arrangements for many students could be complex.

The report was welcomed and approved by the committee.

7.3. Infrastructure Strategy/Capital Projects

S McNaught highlighted the positive report with minor opportunities of improvement. Following a previous review of capital projects, a recommendation for project appraisal procedures for projects below a specific threshold was implemented, but had been discontinued through various staff changes. S Taylor confirmed that these would be reintroduced.

H Honeyman noted that this was an excellent report and noted thanks to the Team for the management of audit outcomes and actions.

7.4. Follow Up Summary

S Taylor presented the summary and noted that work was progressing well in terms of audit recommendations, with these being closed out as per the update. The remaining action outstanding is Student Invoicing and Debt Management which will be closed at the new revised date of January 2024. S Middleton asked how realistic this date it to achieving the outcome. S Taylor stated that this date has been identified for a reasonable period and the Finance team have been working towards this deadline and an update on progress would be reported at the next meeting.

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

8. DATA REPORTING

S Taylor noted that there had been no reportable data breaches. The annual report on cyber security and resilience would be considered at the next meeting.

9. STRATEGIC RISK REGISTER UPDATE

S Taylor summarised the Strategic Risk Register, highlighting the changes arising from September 2023 Board meeting.

Following on from previous updates in respect of the reduction in full-time student recruitment in 2021/22 and in 2022/23, discussions remain on-going between Colleges Scotland, the Scottish Government, and the Scottish Funding Council around a range of sector wide flexibilities and rule changes to better support the sector.

Feedback from SFC appears to be more supportive of the sector and that colleges should not be overly concerned around the risk of significant financial clawback for 2022/23.

As a major risk, the financial sustainability risk was discussed, and the significant on-going action in respect of this noted.

H Honeyman asked if the post-mitigation risk was high enough given the financial picture in the public sector. S Taylor stated increasing the risk was likely to signify that the board felt that the College was not financially sustainable which would then require a different set of actions to be undertaken. S Taylor noted that a balanced budget had been achieved for 2023/24 and that work was progressing to identify and realise further savings for 2024/25. S Middleton highlighted concern that the clawback of funds was not within the SFC remit and that this was a concern. The Committee requested that the post-mitigation risk be reviewed by the Executive and be brought back to the next meeting. **S Taylor to progress.**

Following discussion at the Board of Management meeting on 28 September 2023 the potential estates risk surrounding Reinforced Autoclaved Aerated Concrete (RAAC) had been updated. S Taylor highlighted that the condition of the RAAC remained good with recommended work carried out and completed, with annual inspections in place. Additional structural engineer recommendations have been received identifying the potential need to replace RAAC panels within a 3-5 year timeframe. S Taylor stated that this did impact on future infrastructure planning for the Kingsway campus, which was currently being considered and would come to the Board in the near future.

H Honeyman asked if there were any Health & Safety concerns attached to this RAAC risk of the College. S Taylor reassured the Committee that all work for RAAC had been completed with the risk remaining low/medium with no immediate concerns.

S Middleton expressed her concern and questioned if the correct colour code (green) for the post-mitigation RAAC risk was sufficient, as she felt this risk could deteriorate if not correctly managed. S Taylor assured the Committee that the risk register was reviewed on a regular basis, he highlighted that the RAAC issue may cause potential issues in the future and that the risk scoring would change if this was the case.

The wider impact of the condition of the Kingsway campus in particular was discussed and it was proposed that a risk around the ability of the College to fund or progress future large infrastructure plans be reviewed for the next meeting. **S Taylor to progress.**

10. **DATE OF NEXT MEETING** – Tuesday 5 March 2024, Kingsway Campus, Room A625 Committee

Action Point Summary

Action	Responsibility	Date
Annual Audit Committee Report to be presented to the Board	H Honeyman	12 December 23
Risk Register to be reviewed and amendment recommendations brought forward on financial sustainability and major infrastructure condition/renewal risks.	S Taylor	5 March 2024

BOARD OF MANAGEMENT

Joint Audit & Risk and Finance & Property Committee

Tuesday 5 December 2023

Minute of the Joint Audit & Risk and Finance & Property Committee meeting held on Tuesday 5 December 2023 at 4.30pm in Room A605 Kingsway Campus and via Microsoft Teams

PRESENT:	H Honeyman (Chair)	S Middleton
	L O'Donnell	D Fordyce
	B Lawrie	S Hewitt
	C Cusick	D Smith
	M Beattie	
IN ATTENDANCE:	S Taylor (Vice Principal)	Penny Muir (Board Administrator)
	J Grace (Vice Principal)	B Ferguson (Vice Principal)
	A Ross (Director of Infrastructure)	B Grace (Head of Estates)
	M Speight (Mazars)	S Macnaught (Henderson Loggie)
	R Holland (Mazars)	

1. WELCOME

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

2. APOLOGIES

Apologies were noted from K Ditcham, M Williamson, R McLellan, J Buchanan, D Rosie, D Mackenzie and D Archibald.

3. DECLARATIONS OF INTEREST OR CONNECTION

There were no declarations.

4. INTERNAL AUDIT ANNUAL REPORT

S Macnaught noted the Internal Audit report concluded for 2022/23 was positive and highlighted that audit outcomes had been graded as good or satisfactory with only minor recommendations made. S Macnaught stated that all audit work had been undertaken in accordance with the audit standards required for public bodies and that all work was independent of the College. It was confirmed that the audit plan had been fulfilled and that the internal auditors were comfortable with the controls in place.

B Lawrie asked about the outcomes of the recent Partnership Audit and S Macnaught stated the overall objective of the audit was to establish whether the College's arrangements for partnership working are effective. The commitment to partnership working was enshrined within the 2025 – Strategy – 'More Successful Students'. The discussions with college management and external partners also highlighted a clear commitment around raising attainment, which was demonstrated by the ongoing involvement of the Director of Curriculum – Partnerships and Projects. The report showed great strengths and no weaknesses arising from this fieldwork.

B Lawrie asked about the legal liability of the College across a range of partnerships and it was reinforced that all legal partnerships are signed off through the college's solicitors, with various significant projects which have already gone through legal support such as Tay City Deals and Dundee Football Club.

The annual report was approved.

5. ANNUAL AUDIT COVERING LETTER AND REPORT

M Speight introduced the covering letter included within the report, noting that provided a clean and unqualified audit opinion with minor comments in respect of some items, and an overall positive conclusion in respect of effective financial management and value for money of the College. M Speight stated that their engagement with the College and finance team had been very positive and productive, which had assisted in the smooth operation and completion of audit requirements.

M Speight noted that the audit outcome was positive and unqualified, representing a good audit outcome for the College with no significant concerns highlighted. The scope of Mazars work were outlined in the Annual Audit Plan which was presented to the Audit & Risk Committee in May 2023. Mazars reviewed the Annual Audit Plan and concluded that the significant audit risks and other areas of management judgement documented remain appropriate.

M Speight identified and raised two internal control recommendations in section 3 which relates to findings from the audit work carried out. One expectation- only a minor point outstanding, was the impact of RAAC and the carrying value of building assets. B Ferguson stated there were no changes to the risk identified, with sufficient work already carried out.

M Speight highlighted his concern with the valuation of land and buildings, stating that the College's property, plant, and equipment (PPE) portfolio totals over £77.3 million of assets (2022: £68.7million) M Speight highlighted that in line with the requirements of the Government Financial Reporting Manual, the College adopted a formal revaluation policy of an external valuation every five years. For the 2023 year-end, Graham & Sibbald Chartered Surveyors provided the College with an interim valuation which will be used to update the remaining carrying values. Given the significance of the value of fixed assets held a misstatement in the valuation could be material to the financial statements. M Speight assured the committee that satisfactory assurance has been gained in respect of the valuation risk in relation to land and buildings and as part of the review and it was identified the financial statements were updated to reflect the change (allowing for the impact of RAAC on the valuation).

It was confirmed that the final report could not be issued until this revised valuation was known, but that this was expected imminently and did not impact on the other elements of the financial statements or audit outcomes.

B Ferguson thanked Mazars for their input and echoed the sentiment around the effort put in by the Finance team and others to achieve an excellent audit outcome. S Hewitt endorsed this comment.

The Committee noted the positive audit outcome.

6. FINANCIAL STATEMENTS FOR THE YEAR ENDED 31 JULY 2023

B Ferguson summarised the financial statements highlighting that despite the excellent outcomes that the College consistently achieved, and the fantastic opportunities developing within the D&A region, there are significant challenges to be faced.

The ‘flat cash’ funding settlement for colleges for 2023/24 at a time of high inflation and significant wage pressures has represented a further significant funding reduction for the sector as a whole. He thanked Mazars for the approach taken to the audit and for their work in understanding the College and its operating context.

B Ferguson summarized the differences between the tables presented within the statutory accounts and how these related back to the quarterly management accounts considered by the Finance and Property Committee. Movements in non-cash items such as the land, buildings and pension valuations were highlighted.

B Ferguson stated that Mazars summarised the results in their report, emphasising that the college is operating with a £2.5m deficit expenditure which has been adjusted and made up of some non-cash related items. The underlying position was a small operating deficit.

D Fordyce stated this was a comprehensive report and queried if the revenue year was correct within the pay award table on page 171. B Ferguson highlight that this was correct and related to Scottish Government policy applied at that time.

D Fordyce thanked B Ferguson and the Finance team for their hard work in preparing the financial statements and undertaking such a positive audit.

The Financial Statement for the year ended 31 July 2023 were approved (subject to amendment) for submission to the Board of Management meeting on 12 December 2023.

7. DATE OF NEXT MEETING – tbc

Action Point Summary

Action	Responsibility	Date
Financial Statement for the year ended 31 July 2023 and external audit report to be presented to the Board	B Ferguson	12 December 23

Agenda Item 5.0

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 5 March 2024

MATTERS ARISING PAPER C

BOARD OF MANAGEMENT
Audit & Risk Committee
Tuesday 5 March 2024

Matters Arising

Paper C for information

The following actions were noted from the Tuesday 5 December 2023 Audit & Risk Committee meeting.

Agenda Item No	Action	Current status	Open / Closed
6.0	Annual Audit Committee Report to be presented to the Board. **H Honeyman**	Reported on 12th December 2023	Closed
9.0	Risk Register to be reviewed and amendment recommendations brought forward on financial sustainability and major infrastructure condition/renewal risks. **S Taylor**	Included in March update	Closed

The following actions were noted from the Tuesday 6 June 2023 Audit & Risk Committee meeting.

Agenda Item No	Action	Current status	Open / Closed
11.0	Meeting to be arranged between the Committee Chair and M Speight (Mazars) **S Taylor**	Discussion on arrangements and contact made as needed	Closed

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

Agenda Item 6.0

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 5 March 2024

HEFESTIS ANNUAL CYBER SECURITY RISK & MATURITY REPORT

PAPER D

Information security and access controls

2022

HEFESTIS

Dundee and Angus College: Annual Information and Cyber Security Risk and Maturity Report 2023

NOVEMBER 2023

DAVID ROBERTSON

HEFESTIS | HIGHER EDUCATION/FURTHER EDUCATION SHARED TECHNOLOGY AND INFORMATION SERVICES STIRLING BUSINESS CENTRE, WELLGREEN, STIRLING, FK8 2DZ

Information and Cyber Security (ICS) Risk and Maturity Report

The following report is generated from review of the Dundee and Angus College information and cyber security maturity and RAID log including ongoing information and cyber security management activity over a period of 1 year. The reporting period is October 2022 to November 2023 and includes reference to previous improvements recorded from October 2020.

Contents

EXECUTIVE SUMMARY

Over the reporting period October 2022 to November 2023 the cyber security activities performed at Dundee and Angus College have significantly strengthened **information and cyber security (ICS)** maturity and risk management. However, the threat level to the HE/FE sector is still high to very high. This report summarises the ongoing cyber security risk and maturity position and is calculated against Dundee and Angus College risk appetite, the public sector action plan and industry maturity standards.

Of exceptional note is the risk mitigation and maturity improvement recorded at strategic, tactical and operational levels throughout the college in relation to embedding of technical security controls across the entire digital estate (Microsoft 365: Defender, Azure, Sentinel, CISCO: TALOS, Vulnerability scanning: Nessus) which have raised scoring to the highest possible levels of advanced maturity (4 to 5) with significant improvement of risk and maturity posture over the reporting period in all technical control areas.

Key Performance Indicators

Risk Mitigation: Progress Towards Minimising Cyber Security Risk

Over the reporting period the college has maintained a **100%** mitigation level to presenting critical risks (KPI #1) **100%** compliance with risk appetite minimum (KPI#2) and **achievement of 100% towards** optimal risk appetite levels (KPI#3) – **significant and substantial** overall improvement. See **risk summary** and **RAID Log** (appendix1) for details.

Security Maturity Improvement Is Significant

Areas of excellence were demonstrated at all levels in relation to operational security, information and cyber security management.

Progress in technical policy development plus embedding of cloud-based controls and services have further contributed to reduced risk and a strengthening of the security posture - **significant improvement**. See Maturity Assessment (appendix 2).

Transition Towards National Standards (PSCRF Version 1 to Version 2)

The previous version of the of the Public Sector Action Plan (PSCRF Version 1) is now out of date and nearing end of life. To ensure the college is abreast of the latest tools for maintaining cyber security resilience criteria at national level, a Public Sector Action Plan Assessment using the latest (PSCRF Version 2) version of the Cyber Resilience Framework self-assessment tool has been initiated and is in the early stages of being completed.

* National release of the updated **Public Sector Cyber Resilience Framework Version 2 has been delayed over 2023** and is now due for piloting and implementation over 2024 to 5, replacing current versions of the framework. Early adoption of the new standards has begun and, where available and appropriate, outputs from this activity have been included within this report.

Conclusion

Dundee and Angus college have reached a position of advanced information and cyber security resilience by applying resource, technology and communications in a risk prioritised and controlled manner over 2020 to 2023. Recommendations to maintain and enhance this position follow in the recommendations section on the next page.

Justifications, illustrations and more detailed analysis constitute the remainder of this report and its appendices.

Recommendations

It is important to note that continuous improvement and application of best practice are the most effective countermeasures against the threat of significant cyber security incident to the HE/FE sector which continues to rise and significantly evolve year on year. Effective ICS mitigation and protection is best approached as a continuous improvement programme of managed activity providing countermeasures against improved or invigorated cyber-criminal activity. This approach is strongly demonstrated at Dundee and Angus college and is recommended for continuance. The following recommendations are included to provide continued systematic management of ICS threats and activities.

Continuation of good practice in priority order (ongoing)

1. Continuance of existing best practice in all areas in order to maintain the security posture and continuously address ICS risk throughout the organisation and for all stakeholders

Management response	We will be performing against the new PSCRF v2 during the year and this should ensure best practice continues to be followed
Timescale for completion/continuance	Ongoing

2. Direct focus on completion of activities to embed best practice in ICS across the organisation in order to replicate the success and clarity of improvements in information and cyber security namely
    - continued update of technical activity, policy and standards documentation

Management response	All policies and standards are reviewed on a regular basis as per the College's policy. This will include all ICS documentation
Timescale for completion/continuance	Ongoing

3. Transition to alignment with the **Public Sector Cyber Resilience Framework version 2** which is due for release early next year as a more complex, granular benchmark for maturity and risk management in greater depth and alignment of internal/external auditing procedures is recommended.

Management response	The PSCRF v2 will be the basis of all future auditing of the controls we have in place
Timescale for completion/continuance	Ongoing

4. Measures to include in transition: annual/ongoing review and reporting of information and cyber security progress and activity for purposes of ongoing quantification and management of risk and security posture against existing auditable standards and assessment *including the 2023 Public Sector Action Plan/cyber resilience framework over the course of 2024 and beyond.

Management response	Controls and process we have in place will continue
Timescale for completion/continuance	Ongoing

5. Focus be applied in future reporting cycles to maintain continuous improvement and more widely embed improved security practice, procedures and systems as business as usual

Management response	As security posture matures further, we will see continuous improvement in this regard
Timescale for completion/continuance	Ongoing

Areas for improvement

There are two areas identified that would benefit from further attention. However those areas are not directly IT related – in priority order.

1. Physical security (although not a high cyber security risk) is the lowest scoring maturity area and may benefit from strengthening in partnership with the estates teams.

Management response	By the very nature of colleges, it is difficult to put in place physical security barriers without having a negative impact on our students. However, looking to put in place campus access strategy and cctv strategy. On top of this review of access to the comms cabinets will be carried out
Timescale for completion	October 2024

2. There is an **opportunity for improvement** in ensuring that best practice and technical controls are applied to the supply chain and third party management procedures.

Management response	We will ensure that Cyber Security is seen as a key factor when procuring systems and services from third-party suppliers
Timescale for completion	Ongoing

3. Classification scheme embedding could be improved in partnership with the governance team

Management response	We will put in place classification and retention policies for key College data
Timescale for completion	December 2024

Justification from maturity modelling and update.

Area 1 – there was **1 significant** gap identified in organisational maturity over the reporting period. The gap relates to physical security where areas for follow up by means of audit against the control standards have been identified.

Area 2 – there were **2 improvement** gaps identified in organisational maturity over the reporting period. These relate to supplier security and organisation of information security. It may be useful to look more closely into improvements which might be made in the securing and management of third parties and suppliers to the organisation to ensure that improvements that

have been made to the technical security infrastructure are embedded horizontally across the supply chain. Organisation of information security should be enabled organically as the upgrades and policy updates to technical controls are captured and shared beyond systems and the IT service more broadly across the organisation. (*See also Area 3).

Area 3 – relates substantially to completion of policy and documentation to the point of sign off and review following significant digital upgrades and an element of bedding in of new technologies – which can be managed as business as usual. It is noted that adoption of data classification policies and retention scheduling should only be included as and when determinant criteria are agreed and authorised at corporate governance level.

ICS Risk and Maturity Analysis

The most recent annual risk profile is illustrated within this section.

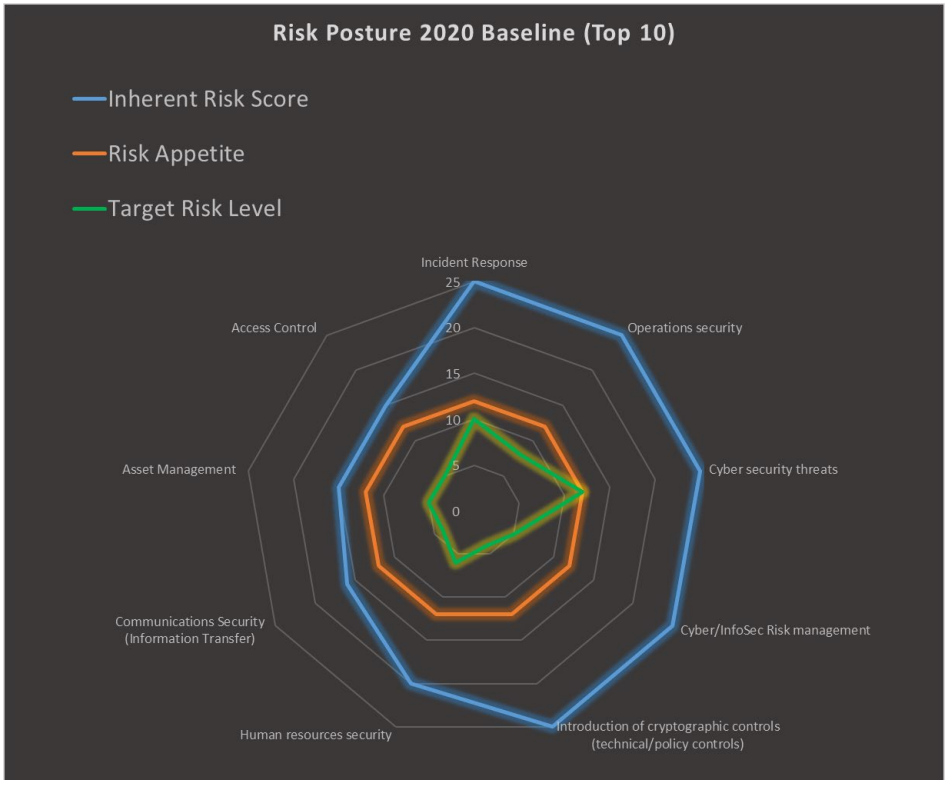
Risk Posture and KPI's

The three risk posture diagrams illustrate change in risk levels over the reporting period. Baseline scores from the beginning of the reporting period are on the left, current scores in the middle and, on the right, combined scores showing where change in risk level has been recorded. The report illustrates progress towards the "green area" in the centre of each chart which indicates the optimal "target level" for ICS risk as defined by the organisation.

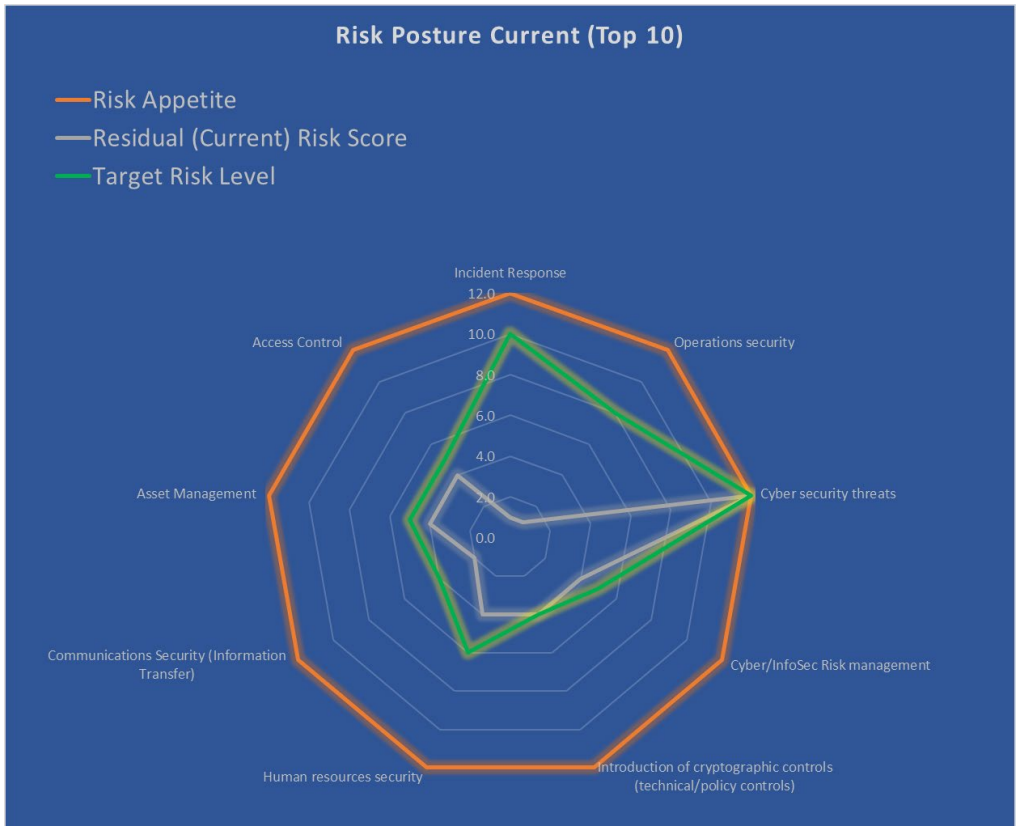
- the **blue** line (baseline) in the "baseline" and "combined" risk posture diagrams illustrates the levels of risk recorded at the assessment starting period used as a baseline for mapping progress against inherited levels of ICS risk – reflecting the risk report initial or starting posture.
- the **orange** line (maximum appetite) shows the maximum risk appetite as a minimum standard of acceptable ICS risk - better than half out of maximum scoring of 25 = 12 (defined by the organisation - adjustable) *excludes external threat level
- the **green** line (target appetite) displays the preferred target levels of risk as an aspirational level of risk to the organisation for each risk category *optimum acceptable levels of risk
- the **grey** line (current risk level) represents the current ICS risk level as recorded at the end of the reporting period.

Risk improvement is displayed as the gap between the **blue** line (baseline) and the grey line (current) risk posture scorings and is used to generate ICS risk key performance indicators.

October 2020 (Baseline) Risk Where D & A College were **(Blue)**



November 2022 (Current) Risk Where D & A College are (Grey)



October 2020 to November 23 (Combined) Risk Measured Improvement

Key Risk Management Performance Indicators

Key Performance Indicator 1: Reduction In Number Of Critical Risks = 100%

Over the reporting period the cyber security mitigations and actions applied by this institution have maintained critical risk instance mitigation by 100% with 0 critical risks recorded. There are currently no critical level ICS risks recorded against industry appetite levels. Best practice.

Key Performance Indicator 2: Reduction Of Risk Towards Minimum Compliance Levels = 100%

Markedly the figures represent 100% achievement and maintenance of a minimum compliance position within the initial risk tolerance threshold. *Minimum threshold = 12 or below commensurate with baseline to target levels of security compliance against Public Sector Action Plan criteria for all recorded ICS risks over the 12-month reporting period. Best practice.

Key Performance Indicator 3: Reduction Of Risk Towards Target (Advanced/Optimal) Levels = 100%

Over the reporting period the recorded level of reduction to presenting ICS risk represents a further 10% progress to 100% mitigation towards the advanced target levels of risk appetite. Significant improvement and best practice.

Risk management reporting therefore indicates significant improvement of the ICS risk position over 2023 to a best practice model and builds on successful implementation of technical risk controls over 2020 to 2022.

ICS Maturity and Posture Summary

The cybersecurity posture for the institution refers to its overall cybersecurity resilience, articulated in terms of continuous improvement. The ICS security maturity posture expresses the relative levels of mitigation, countermeasures, procedures and application security to the IT and wider security estate, particularly relative to the internet and vulnerability to cyber-threat. Baselining and ongoing measurement of security maturity is performed to articulate and put in place measures with KPI's to illustrate and monitor information and cyber security resilience within and across the organisation.

Justification

Security Maturity Summary: By Section (Average Score)

Control Description	Control: Maturity Score Baseline	Current Maturity Score	Target Maturity Score	Maturity Gap	Improvement
A.17 Information security aspects of business continuity management	1.8	5.0	4.0	-1.0	3.3
A.16 Information security incident management	2.0	5.0	4.0	-1.0	3.0
A.13 Communications security	2.1	4.3	4.0	-0.3	2.1
A.7 Human resources security	3.3	4.0	4.0	0.0	0.7
A.18 Compliance	2.9	3.8	4.0	0.3	0.9
A.6 Organisation of information security	2.1	2.7	4.0	1.3	0.6
A.14 System acquisition, development and maintenance	2.5	3.6	4.0	0.4	1.2
A.1 Security Strategy	3.0	4.0	4.0	0.0	1.0
A.9 Access control	2.9	3.4	4.0	0.6	0.5
A.11 Physical and environmental security	1.7	1.7	4.0	2.3	0.0
A.8 Asset management	3.1	3.6	4.0	0.4	0.5
A.12 Operations security	3.7	5.0	4.0	-1.0	1.3
A.2 Terms and Definitions	2.0	4.0	4.0	0.0	2.0
A.3 Structure of information security standards	3.0	4.0	4.0	0.0	1.0
A.4 Risk Management	4.0	4.0	4.0	0.0	0.0
A.5 Information security policy management	3.0	4.0	4.0	0.0	1.0
A.10 Cryptography	4.0	4.0	4.0	0.0	0.0
A.15 Supplier relationships	2.2	2.2	4.0	1.8	0.0
Average score/improvement	2.7	3.8	4.0	0.2	1.1

Maturity improvement summary

Strong maturity with high levels of improvement is indicated by the ICS maturity summary – the right hand "improvement" column indicates by how much ICS posture has strengthened over the reporting period.

Improvement is very good (dark green) in two areas due to a strong culture of cybersecurity awareness and progression of planned technical infrastructure upgrade and managed cloud-based migration from network dependent services.

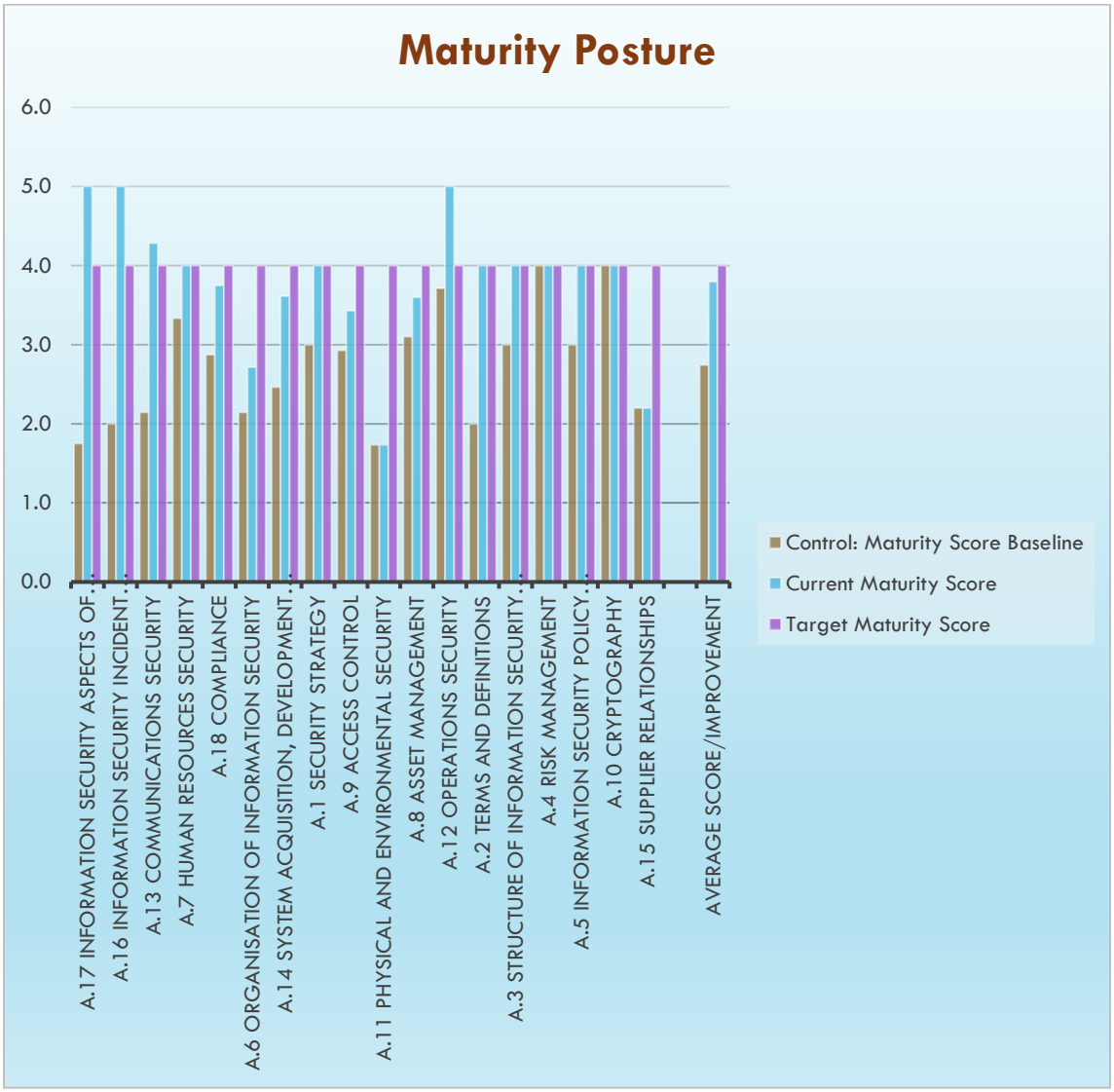
Improvement is good (medium green) in the main body of the summary reflecting embedding of updated technical security controls across the digital estate.

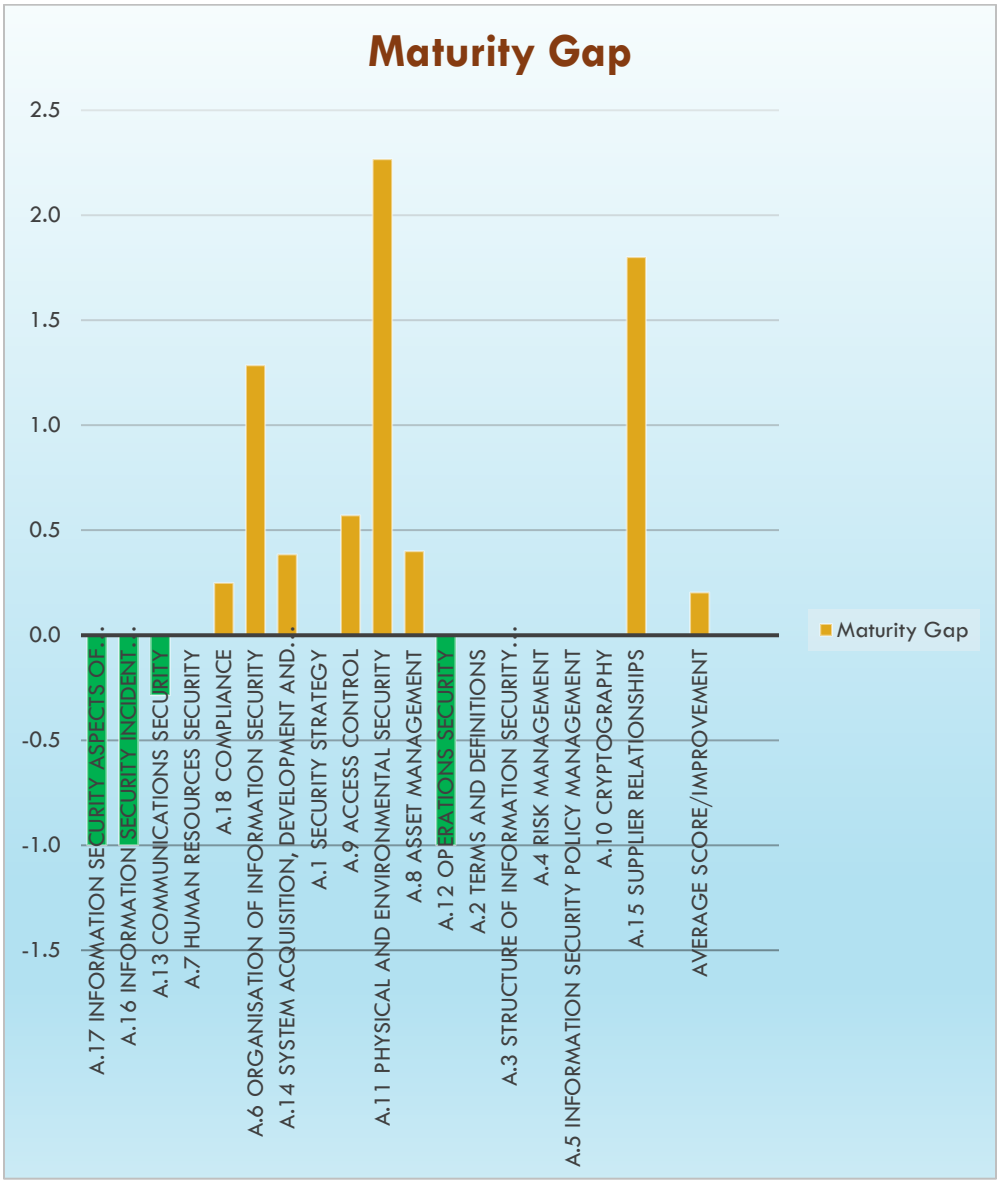
Posture has been maintained (light green) in 4 other areas indicating stability, but the opportunity to adopt cyber security improvements which have been gained more widely across the organisation beyond the IT and technical sphere of influence.

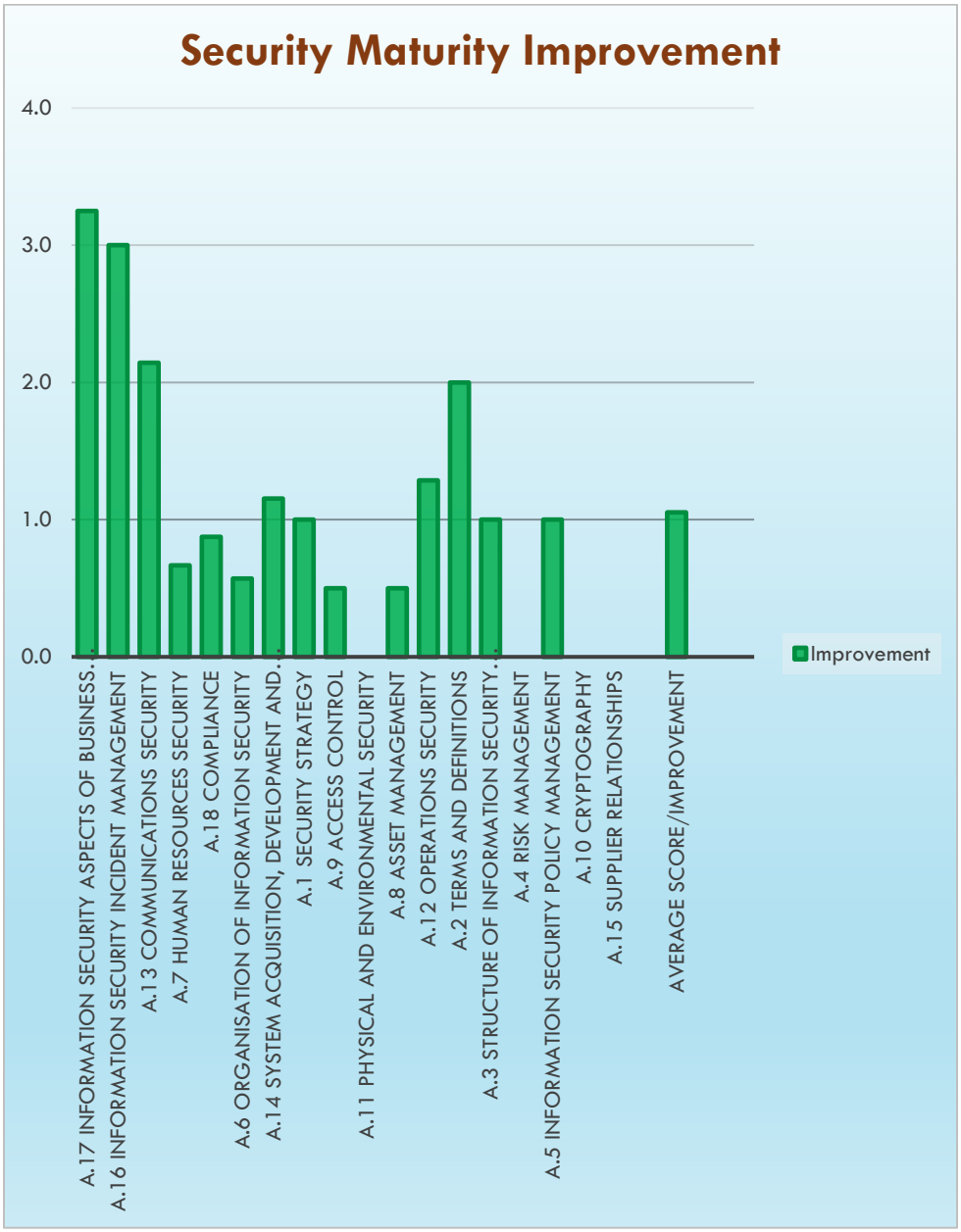
Improvements in the organisation of cyber and information security and a wide range of security applications and controls underpin high levels of overall improvement.

Maturity Gap Improvement

The change between Baseline and current ICS maturity levels over the reporting period is illustrated in the following set of charts.




Maturity Gap
2.5
2.0
1.5
1.0
0.5
0.0
-0.5
-1.0
-1.5
A.17 INFORMATION SECURITY ASPECTS OF...
A.16 INFORMATION SECURITY INCIDENT...
A.13 COMMUNICATIONS SECURITY
A.7 HUMAN RESOURCES SECURITY
A.18 COMPLIANCE
A.6 ORGANISATION OF INFORMATION SECURITY
A.14 SYSTEM ACQUISITION, DEVELOPMENT AND...
A.1 SECURITY STRATEGY
A.9 ACCESS CONTROL
A.11 PHYSICAL AND ENVIRONMENTAL SECURITY
A.8 ASSET MANAGEMENT
A.12 OPERATIONS SECURITY
A.2 TERMS AND DEFINITIONS
A.3 STRUCTURE OF INFORMATION SECURITY...
A.4 RISK MANAGEMENT
A.5 INFORMATION SECURITY POLICY MANAGEMENT
A.10 CRYPTOGRAPHY
A.15 SUPPLIER RELATIONSHIPS
AVERAGE SCORE/IMPROVEMENT
Maturity Gap



The charts above display the ICS maturity areas using gap analysis - Current vs Baseline. (**Green**) bars in the maturity posture and improvement charts indicate where improvement has been made as detailed in the previous section.

Maturity Gap Quantification

Focus is given to the **Orange** areas in the Maturity Gap chart (middle) where further improvement opportunity has been identified and may be considered for prioritisation.

1. A gap score greater than 2 indicates significant maturity improvement is required (one area)
2. A gap score of between 1 and 2 indicates maturity improvement is recommended (no areas)
3. A gap score of 1or less indicates incremental improvements may be gained (5 areas)
4. A gap score of zero or lower indicates that ICS maturity is high and should be maintained (12 areas)

Area 1 – there was **1 significant** gap identified in organisational maturity at the end of the reporting period. The gap relates to physical security where areas for follow up by means of audit against the control standards have been identified.

Area 2 – there were **2 improvement** gaps identified in organisational maturity at the end of the reporting period. These relate to supplier security and organisation of information security. It may be useful to look more closely into improvements which might be made in the securing and management of third parties and suppliers to the organisation to ensure that improvements that have been made to the technical security infrastructure are embedded horizontally across the supply chain. Organisation of information security should be enabled organically as the upgrades and policy updates to technical controls are captured and shared beyond systems and the IT service more broadly across the organisation. (*See also Area 3).

Area 3 – relates substantially to completion of policy and documentation to the point of sign off and review following significant digital upgrades and an element of bedding in of new technologies – which can be managed as business as usual. It is noted that adoption of classification scheme and retention scheduling should be included as and when determinant criteria are agreed and authorised at corporate governance level.

Area 4 - the report indicates that ICS risk is currently applicably mitigated in all other areas i.e. action plans have been successfully completed and identified improvements have been made.

Areas of Significant Improvement

Areas of excellence were demonstrated at all levels in relation to information and cyber security management.

Progress, not only in implementation of technical cybersecurity mechanisms and applications but also to cloud-based controls and services have strongly contributed to reduced risk and a strengthening of the security posture - **significant improvement**. See Maturity Assessment (appendix 2).

It should be noted that although there was a significant increase in external risk and threat level due to Covid related change and heightened threat actor activity, there were no areas of maturity regression recorded over the reporting period despite increased pressure on remote service and device usage which, consequently, had minimal impact on overall security posture.

Appendices

Appendix 1: RAID log (current)

RAID Log (D&A - 2023).xlsx

Appendix 2: Maturity Posture (current)

Information Security Maturity Tool (D&A -

Appendix 3: Calculating Risk and Maturity Improvement

Calculating Risk and Maturity Improvement

Following ongoing review of information and cyber security services conducted for Dundee and Angus College over 2023, an updated report on information and cyber security (ICS) risk management has been provided. The purpose of this annual report is to articulate measures with KPI's (Key Performance Indicators) put in place to monitor and improve cyber security risk and maturity management within the organisation.

All risk scoring is from 0 to 25 with a score of 25 (Likelihood 5 x Impact 5 = 25 critical) being the maximum possible value for risk facing the organisation. Maturity scoring is from 0 to 5 with 0 being low to no maturity and 5 being advanced maturity levels.

Improvement is rated by percentage of maximum possible scoring

0%	= no change
0 to 5 %	= minor improvement
5 to 10 %	= good improvement
15 to 20%	= substantial improvement
> 20%	= significant improvement

Agenda Item 7.0

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 5 March 2024

INTERNAL AUDIT

7.1- RISK MANAGEMENT & BUSINESS CONTINUITY

PAPER E

LEVEL OF ASSURANCE
Satisfactory

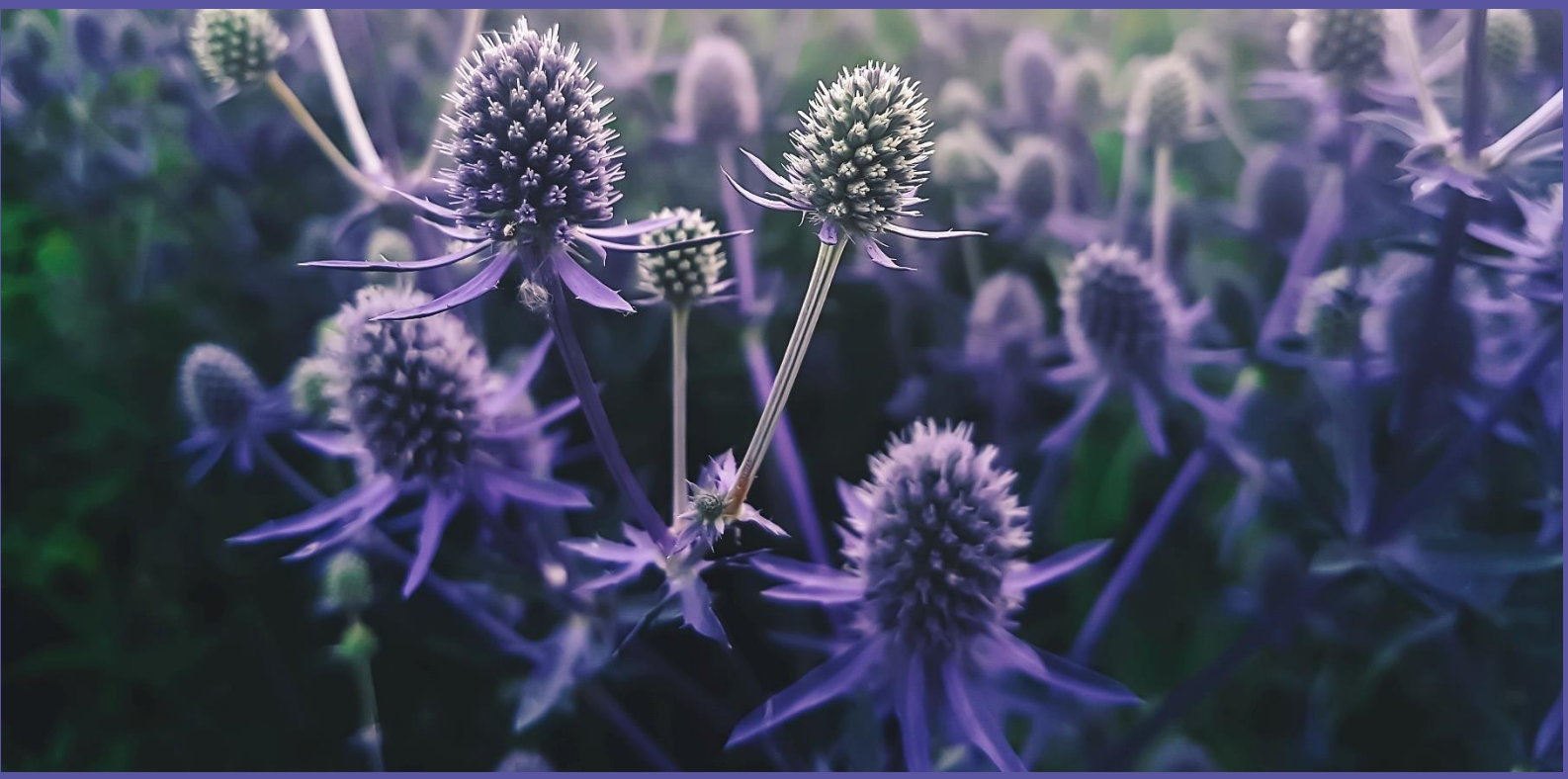
Dundee & Angus College

Risk Management and Business Continuity / Disaster Recovery Planning

Internal Audit report No: 2024/02

Draft issued: 6 February 2024

Final issued: 7 February 2024



Henderson Loggie

Level of Assurance

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

Gradings are defined as follows:

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

Action Grades

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

Management Summary

Overall Level of Assurance

Satisfactory	System meets control objectives with some weaknesses present.

Risk Assessment

This review focused on the controls in place to mitigate all risks on Dundee & Angus College ('the College') Strategic Risk Register:

Background

As part of the Internal Audit programme at the College for 2023/24 we carried out a review of the College's risk management and business continuity / disaster recovery arrangements. Our 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 (ARC) that the related control environment is operating effectively, ensuring risk is maintained at an acceptable level.

The Scottish Public Finance Manual (SPFM) requires that each public sector organisation's internal control systems should include embedded arrangements for identifying, assessing, addressing, reviewing and reporting their risks. This should be integrated into normal management systems and closely linked to the business planning process. Each organisation's governing body should make a considered choice about its desired risk profile, taking account of its legal obligations, ministers' policy decisions, its business objectives, and public expectations of what it should deliver.

Good risk management includes a range of matters including:

- Creating a formal risk management framework, including identifying risk appetite;
- Risk identification;
- Risk assessment (likelihood and impact);
- Risk mitigation;
- Risk reporting and escalation; and
- Risk review and feedback.

In addition, an effective Business Continuity Plan is essential to ensure that the College can, in response to a disaster or threat, continue to operate key activities and ensure that the interests of key stakeholders continue to be met.

Scope, Objectives and Overall Findings

Risk Management
The scope of this aspect of the audit, which was the main focus of the review, was to consider whether there are corporate procedures in place to adequately assess risk and minimise the possibility of unexpected and unplanned situations developing, which are in line with good practice.

Scope, Objectives and Overall Findings (Continued)

Business Continuity / Disaster Recovery Planning
We also undertook a high-level review of business continuity / disaster recovery planning arrangements to consider whether there are adequate plans in place to minimise disruption to College's operations following loss of life, buildings or equipment and restore business processes.

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

Objective	Findings			
The objective of our audit was to ensure that:		**1**	**2**	**3**
		No. of Agreed Actions		
Risk Management 1. Key risks have been identified and are being appropriately controlled, mitigated, reported and discussed at appropriate levels of management and the Board of Management.	**Good**	-	-	1
2. The processes in place reflect good practice in risk management.	**Satisfactory**	-	-	3
Business Continuity / Disaster Recovery Planning 3. Business Continuity / Disaster Recovery Plans are in place covering all of the College's activities and locations.	**Satisfactory**	-	-	-
4. The Business Continuity / Disaster Recovery Plans are workable, properly communicated to members of staff, and have been adequately tested.	**Good**	-	-	-
5. The processes and procedures in place follow recommended good practice	**Satisfactory**	-	-	-
Overall Level of Assurance	**Satisfactory**	**-**	**-**	**4**
		System meets control objectives with some weaknesses present.		

Audit Approach

Risk Management
We obtained and reviewed a copy of the College's risk management policies, procedures, Strategic Risk Register (SRR), and other risk registers, and discussed the risk management arrangements in place with the Vice Principal Support Services and Operations, Director of Infrastructure, Head of Estates, Vice Principal Curriculum and Attainment, Director of Student Experience, and Director of Curriculum and Attainment.

The College's risk management arrangements were then benchmarked against relevant good practice guidance (as defined within the SPFM and the UK Government Orange Book).

Audit Approach (Continued)

Risk Management (continued)
We considered whether all relevant key risks have been identified and included on the SRR and ensured that these are monitored and adequately reported on.

Business Continuity / Disaster Recovery Planning
We obtained copies of Business Continuity / Disaster Recovery Plans in place and considered whether they cover all of the College's activities and locations.

We discussed the College's approach with the Vice Principal Support Services and Operations, Director of Infrastructure, Head of Estates, Vice Principal Curriculum and Attainment, Director of Student Experience and Director of Curriculum and Attainment, and reviewed evidence of how plans have been communicated to staff and the extent to which plans have been tested.

An assessment of the key processes and internal controls was performed with reference to relevant good practice guidance as defined in the UK Government Business Continuity Management toolkit and ISO 22301 Business Continuity Management System (BCMS) guidance.

Summary of Main Findings

Strengths

Risk Management

- The College's Risk Management Policy sets out the framework for risk management within the College and the responsibilities of the Board of Management, Board Committees and management;
- High level strategic risks are outlined within the SRR. These risks are discussed and approved by the full Board of Management two times per year;
- The Board has delegated responsibility for risk management to the ARC although each Board Committee reviews the strategic risks allocated to its area of responsibility on a quarterly basis, making recommendations on change to the ARC as appropriate;
- The Executive Leadership Team (ELT) and Senior Leadership Team (SLT) undertake the ongoing monitoring and mitigation of risks significant to the College;
- The Vice Principal Support Services and Operations prepares a SRR Update paper for discussion at the ARC and this paper is also now provided to the full Board when the SRR is presented. Similar papers are prepared for the other Board Committees;
- Operational risks are appraised on a rolling basis through team / service / project meetings and emerging risks are communicated and managed as required; and
- There is a Cyber risk register and an Annual Information and Cyber Security Risk and Maturity Report is prepared for the College by HEFESTIS (Higher Education / Further Education Shared Technology and Information Services).

Business Continuity / Disaster Recovery Planning

- The College has a Business Continuity Policy in place which provides a framework for the effective management of the response to any major incident affecting the College;
- The Business Continuity Policy is supported by a Business Continuity Plan (BCP). The BCP sets out how the policy would be operationalised in the event of a major incident;
- Within the BCP, a number of lists have been created as a guide to the actions which may be required by all staff, the Business Continuity Team, Principal, Head of Estates, Head of ICT, Student Services Team, People Team and Finance Team;
- Relevant contact details for staff, suppliers, radio stations etc. are maintained on Teams;
- There is a separate Cyber Incident Response Procedure and a BCP – Pandemics;

Summary of Main Findings (Continued)

Strengths (continued)

Business Continuity / Disaster Recovery Planning (Continued)

- The College has successful responded to a number of incidents in recent years including the cyber-attack and COVID-19 pandemic. Key elements of the College's response to any incident include: the ability to switch to online learning; resilience / duplication of provision between campuses; good links with Local Authorities and other organisations; and the enacting of a Cloud first ICT policy.
- The College's Business Continuity Policy and BCP have been widely circulated and are available on Microsoft Teams and the College Staff Portal, and appropriate communication channels are available in the event of an incident; and
- A major incident desk top exercise was facilitated by the College's insurers in 2019 and another one is to be programmed in the next 12 months. A desk top exercise, facilitated by HEFESTIS, was also carried out in 2022 to test the Cyber Incident Response Procedure and another is planned for later this year.

Weaknesses / Opportunities for Improvement

Risk Management

- There is scope to add monitoring of activity targets to the list of monitoring reports on the SRR for risk 2.2 'Failure to achieve institutional sustainability' and also scope to consider adding a further strategic risk in relation to attracting, engaging, retaining, and developing appropriately qualified staff;
- Risks on the SRR are scored on a 5x5 scale. While there is some guidance to support the assessment of likelihood of the adverse events occurring, and the impact to the College should the risk occur, further clarity would be useful on the factors to be considered when making this assessment;
- In line with good practice, the Risk Management Policy states that it is the Board's responsibility to determine the appropriate risk appetite for the College that balances risk with opportunity. This has not however been clearly documented to allow residual risks on the SRR to be formally considered for compatibility with the Board's stated risk appetite;
- There is a live action from the Board to undertake risk training, which was last carried out in 2019. There has also been no recent risk management training for the ELT, SLT, and other relevant managers and staff;

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 and Action Plan

Objective 1: Key risks have been identified and are being appropriately controlled, mitigated, reported and discussed at appropriate levels of management and the Board of Management.

The College's Risk Management Policy (current issue date 14 March 2023) and related arrangements:

- 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 (SLT) and others in the effective management of risks.

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; and
- Annually review the College approach to risk management and approve changes or improvements as necessary.

The Board of Management has delegated responsibility for risk management to the Audit & Risk Committee (ARC). Each Board Committee reviews the strategic risks allocated to its area of responsibility (as indicated on the Strategic Risk Register (SRR)) on a quarterly basis, making recommendations on change to the ARC as appropriate. The ARC monitors and reports to the Board on internal controls and alerts Board members to any significant emerging issues. The ARC reports to the Board annually on the effectiveness of the internal control system, including the College system for the management of risk.

The SLT has overall operational responsibility for the identification, management and mitigation of risk in line with Board objectives and risk appetite, with the Vice Principal Support Services and Operations taking a lead role. It is the role of the SLT 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.

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.

Objective 1: Key risks have been identified and are being appropriately controlled, mitigated, reported and discussed at appropriate levels of management and the Board of Management (Continued).

High level strategic risks are outlined within the SRR. 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 (ELT) and SLT undertake the ongoing monitoring and mitigation of risks significant to the College. The SRR is formally reviewed and updated quarterly through the ARC. The Vice Principal Support Services and Operations prepares a SRR Update paper for discussion at the ARC and this paper is also now provided to the full Board when the SRR is presented. Similar SRR Update papers are prepared by the Vice Principal Support Services and Operations for the Finance and Property Committee and Human Resources and Development Committee. The Vice Principal Curriculum and Partnerships Report to the Learning, Teaching and Quality Committee aims to provide members with reassurance that actions and activities are being progressed and addressed that support the mitigation of relevant risks identified within the SRR.

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). 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. Where a post mitigation risk is highlighted as 'red' (High risk factor – Major risk – score 16-20) or above this will be subject to review at each subsequent meeting of the ARC. Monitoring arrangements for each risk are set out on the SRR together with the lead responsible officer(s), which is mainly the Principal and / or Vice Principals.

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. An example team operational plan was reviewed as part of our audit. Although we noted that there is no specific section for risk, the Team Curriculum and Quality Priorities for the year linked in with the College's key strategic risks. Team risk registers are not maintained although there is a separate Cyber risk register and an Annual Information and Cyber Security Risk and Maturity Report is prepared for the College by HEFESTIS (Higher Education / Further Education Shared Technology and Information Services). A COVID-19 specific risk register was maintained during the pandemic.

The Risk Management Policy notes that the approval of capital and revenue projects where the 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; and
- Reputational or other risks.

Objective 1: Key risks have been identified and are being appropriately controlled, mitigated, reported and discussed at appropriate levels of management and the Board of Management (Continued).

The Policy also notes that 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.

Following a recommendation made in a recent internal audit of Infrastructure Strategy / Capital Projects (report 2023/09, issued November 2023) College management is currently revisiting the thresholds above which recognised risk management processes such as project risk registers are utilised. It is proposed that projects above £100k will have a Project Manager and risk register, with projects above £500k adopting full project management arrangements.

We reviewed the College SRR as at November 2023 against a sample of three other college strategic risk registers and considered whether all relevant key risks had been identified and included. The following common risks were found to be not specifically included on the College SRR, although it was noted that the Credit Target Risk is included as a standing item on the SRR Update paper:

- Failure to manage strategic risks associated with subsidiary company;
- Failure to attract, engage, retain and develop appropriately qualified staff;
- Failure of Corporate Governance;
- Failure to maximise income via diversification / achieve improved business development;
- Fail to recruit or retain sufficient students or learners / meet planned activity targets; and
- Financial pressures causing reduced curriculum range, choice and opportunity / continued staff reductions negatively impacting on training provision; quality assurance; assessing.

Objective 1: Key risks have been identified and are being appropriately controlled, mitigated, reported and discussed at appropriate levels of management and the Board of Management (Continued).

Observation	Risk	Recommendation	Management Response	
The above common risks were discussed with the Vice Principal Support Services and Operations. In most cases it was confirmed that the risks were more broadly covered by risks already on the SRR such as 2.2 'Failure to achieve institutional sustainability' or had already been considered following a detailed review of the SRR by the Board Chair in Autumn 2022 and subsequent discussion by the SLT, ARC and Board. It was agreed that there is scope to add monitoring of activity (credit) targets to the list of monitoring reports on the SRR for risk 2.2 and also scope to consider adding a further strategic risk to those already monitored by the Human Resources and Development Committee in relation to attracting, engaging, retaining and developing appropriately qualified staff.	Key risks are not all formally identified on the SRR along with the monitoring arrangements in place.	**R1 -** The following amendments to the SRR should be considered: • adding monitoring of activity targets to the list of monitoring reports on the SRR for risk 2.2 'Failure to achieve institutional sustainability'; and • adding a further strategic risk in relation to attracting, engaging, retaining and developing appropriately qualified staff.	Agreed. **To be actioned by:** Vice Principal Support Services and Operations **No later than:** 31 March 2024	
			Grade	**3**

Objective 2: The processes in place reflect good practice in risk management.

A comparison of the College's risk management arrangements was made against a best practice checklist developed from relevant guidance including the Scottish Public Finance Manual (SPFM) and UK Government Orange Book. This noted many areas where the College's arrangements aligned with good practice. However, there were a small number of areas where they did not fully align, and further improvement could be made.

Linkage to strategic objectives
Although the College Risk Management Policy notes that the SRR links directly to the College Strategy and key outcomes as outlined through the Regional Outcome Agreement (ROA) there is no specific cross referencing on the SRR. A recommendation was made following our previous review of risk management in 2019 (report 2019/06, issued May 2019) that the SRR should be amended to make explicit reference to the relevant section of the ROA / Strategic Plan. Although this was accepted at the time, the ARC accepted a management recommendation to remove this action due to changes in ROA format by the Scottish Funding Council. For example, the ROA no longer includes a Finance or Estates section and therefore many risks on the SRR could not be cross-referred to the ROA.

Identification of risks outside the key risks
As noted under Objective 1, with the exception of the Cyber risk register and project risk registers, a formal risk register is only maintained for strategic risks. As previously noted, operational risks are embedded within management operations and are appraised on a rolling basis through team / service / project meetings and emerging risks are communicated and managed as required.

While the current approach does provide substantial assurance, there is potential to expand the risk management arrangements with the introduction of risk registers at an operational level. However, we confirmed with management that the work required to create and maintain operational risk registers, and the benefits which would accrue from this work, have already been considered and it is not deemed appropriate for the College to pursue this option given the current level of management and staff resources available. It was noted that operational risk registers have been prepared in the past and discussions with senior management confirmed that risk management is embedded into day-to-day operations. Therefore, we do not feel that a separate recommendation on this point is necessary.

Objective 2: The processes in place reflect good practice in risk management (Continued).

Observation	Risk	Recommendation	Management Response	
Risk prioritisation Risks on the SRR are scored on a 5x5 scale, with scores defined as follows: **Score / Impact / Likelihood** 1 / Routine / Remote 2 / Minor / Unlikely 3 / Significant / Possible 4 / Major / Probable 5 / Critical / Very Likely While this provides some guidance to support the assessment of likelihood of the adverse events occurring, and the impact to the College should the risk occur, further clarity would be useful on the factors to be considered when making this assessment. This could include for example, when assessing impact, the financial value of any loss or the number of days a service / building would be lost. For likelihood, the percentage chance or number of instances of the risk occurring could be defined.	Without more detailed guidance, there may be a lack of consistency in assessing the impact and likelihood scores.	**R2 -** The College should develop a framework to provide further guidance on how to assess the impact and likelihood of identified risks, ensuring a consistent approach for risk assessment.	Agreed. **To be actioned by:** Vice Principal Support Services and Operations **No later than:** 30 September 2024	
			Grade	**3**

Objective 2: The processes in place reflect good practice in risk management (Continued).

Risk appetite
The UK Government Orange Book includes a guidance note on risk appetite. This provides useful guidance on the development, application and documenting risk appetite.

This guidance includes example appetite levels defined by risk categories. An extract is shown below for the Strategy risk category.

Averse	Minimal	Cautious	Open	Eager
Guiding principles or rules in place that limit risk in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 5+ year intervals	Guiding principles or rules in place that minimise risk in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 4-5 year intervals	Guiding principles or rules in place that allow considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 3-4 year intervals	Guiding principles or rules in place that are receptive to considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 2-3 year intervals	Guiding principles or rules in place that welcome considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 1-2 year intervals

Observation	Risk	Recommendation	Management Response	
In line with best practice, the Risk Management Policy states that it is the Board's responsibility to determine the appropriate risk appetite for the College that balances risk with opportunity. This has not however been clearly documented to allow residual risks on the SRR to be formally considered for compatibility with the Board's stated risk appetite. A Board Development Session was held in June 2019 on risk culture; Board members personal responsibility; and the tone from the top. It was hoped that the session would give members a better understanding of the College's risk maturity level and risk appetite. The session took place pre-cyber-attack, and no output was now available from this.	Residual risks are not formally considered for compatibility with the Board's stated risk appetite.	**R3 -** The Board should consider and establish what the College's high-level risk appetite is for each defined risk category, and residual risks on the SRR should be formally considered for compatibility with this stated risk appetite. The UK Government Orange Book guidance note on risk appetite can be used for reference, particularly in relation to documenting the risk appetite.	Agreed. **To be actioned by:** Board of Management **No later than:** 30 September 2024	
			Grade	**3**

Objective 2: The processes in place reflect good practice in risk management (Continued).

Observation	Risk	Recommendation	Management Response
Training It is important to ensure that staff and Board members understand, in a way appropriate to their role, what the College's risk strategy is, what the risk priorities are, and how their particular responsibilities in the organisation fit into that framework. There is a live action from the Board to undertake risk training, which was last carried out in 2019. There has also been no recent training for the ELT, SLT and other relevant managers and staff.	Appropriate and consistent embedding of risk management will not be achieved and risk priorities may not be consistently addressed.	**R4 -** A plan should be implemented to ensure that periodic risk management training is provided for Board members, senior managers and other relevant College managers and staff.	Agreed. **Board of Management Training to be actioned by:** Board Chair / Board Governance Professional **No later than:** 30 September 2024 **ELT, SLT and Manager training to be actioned by:** Vice Principal Support Services and Operations **No later than:** 31 December 2024
			Grade **3**

Objective 3: Business Continuity / Disaster Recovery Plans are in place covering all of the College's activities and locations.

The College has a Business Continuity Policy (current issue date 6 June 2023) in place, which provides a framework for the effective management of the response to any major incident affecting the College. This includes providing leadership and guidance to co-ordinate the response to a major incident in the College, to minimise the effect of the incident, prepare for 'business as usual' as quickly as possible and to reassure staff, students and the community that an effective process for the full restoration of all services is in place.

The Policy applies to all activities undertaken within the control of the Board of Management of the College. This is primarily focused on activities which take place within the confines of the three main College campuses in Arbroath, Gardyne and Kingsway, along with any outreach centres currently in use. It should also be referred to if a major incident were to arise outwith the College, for instance on partner premises or during staff / student trips.

The Policy comes into effect whenever a serious and / or sustained incident or event (or the potential of such an incident / event) significantly threatens any valuable assets.

The Policy includes guidance on the notification of an incident and Business Continuity Team membership, role and responsibilities. Responsibility for declaring a major incident and invoking the Business Continuity Policy lies with any member of the ELT.

The Business Continuity Policy is supported by a Business Continuity Plan (BCP). The BCP sets out how the policy would be operationalised in the event of a major incident. It is designed to ensure the continuation of vital services and functions that support the running of the College in the event that any form of business interruption occurs.

The aim of the BCP is to enable the business of the College to effectively manage a situation and the effects of service disruption. This will be achieved through delivery of the following objectives:

- Effectively managing the response to the event, limiting the injury / damage to critical assets;
- Definition and prioritisation of the critical functions within the services;
- Analysis of risks to the service;
- Determination of critical resource requirements;
- Documented response to the incident;
- Effective communications with students, staff, stakeholders, emergency services and media throughout the incident; and
- Enabling the rapid transfer of business operations to possible pre-determined recovery site(s). These may or may not be at the same location depending on the scale of the incident.

The BCP includes further guidance on incident identification and notification and incident management. A number of lists have been created as a guide to the actions which may be required by all staff, the Business Continuity Team, Principal, Head of Estates, Head of ICT, Student Services Team, People Team and Finance Team. Relevant contact details for staff, suppliers, radio stations etc. are maintained on Teams.

Objective 3: Business Continuity / Disaster Recovery Plans are in place covering all of the College's activities and locations (Continued).

The BCP notes that key departments and functions have produced Disaster Recovery Plans, with the intention that the combination of the BCP and the Disaster Recovery Plans would represent a comprehensive plan for each particular Campus / Department / Building.

In practice, the only other formal documented plans in place are a Cyber Incident Response Procedure (current issue date 18 March 2022) and a BCP – Pandemics (current issue date 6 June 2023).

Although discussions with the members of the ELT and SLT interviewed indicated that the College would be able to respond to any incident, as has been proved in recent years by the College's successful response to the cyber-attack and COVID-19 pandemic, and smaller incidents such as Storm Babet, there are no formal documented Disaster Recovery Plans in place for key departments and functions.

The following were noted as key elements of the College's response to any incident:

- As a result of the pandemic, systems are in place to switch to online learning;
- There is resilience / duplication of provision between campuses therefore in the event of the loss of a building on one campus students on many courses would be able to be transported to another campus to continue with their studies. If required, there could be evening and weekend classes;
- There are good links with the Local Authorities, other colleges and universities, commercial and other organisations, who would be able to provide assistance following an incident. This may include the sourcing of alternative accommodation, provision of IT or other staff to help in recovery and access to learning materials and equipment;
- Post-cyber-attack the College has enacted a Cloud first ICT policy which provides significant resilience and business continuity benefits;
- Student work is stored on Office 365 / Teams rather than being mainly paper or campus server based;
- All major ICT systems are no longer hosted on campus; and
- Student funding (and payroll) payments can be made based on previous BACS files.

Further discussion with the Vice Principal Support Services and Operations indicated that the College does not have the management or staff resources to prepare and maintain detailed department Disaster Recovery Plans and keep these up to date, and the plans may be well out of date by the time of any incident.

Risk Management and Business Continuity / Disaster Recovery Planning

Objective 4: the Business Continuity / Disaster Recovery Plans are workable, properly communicated to members of staff, and have been adequately tested.

The College's Business Continuity Policy and BCP have been widely circulated to the ELT, SLT, other College managers and staff, including the Caretaker Team Leaders and Help / Point Reception at each campus. In addition, the documents are available on Microsoft Teams and the College Staff Portal.

During an incident, official communication channels such as the College social media accounts are used, and a media communication strategy put in place. A closed WhatsApp group, which was instigated as a result of network outage in 2017, has been retained as an effective way to communicate information quickly in a secure environment and Microsoft Teams and a SharePoint portal are also used as a mechanism to communicate.

The Business Continuity Policy states that scenario exercises will be conducted at appropriate intervals to test the College's response to a range of potential major incidents, in order to identify any gaps or weaknesses in the Business Continuity Policy and Plan or ability of key personnel to respond. The BCP notes that it should be re-tested when there has been any major revision of College procedures or if there is any significant change to the general environment or personnel.

A major incident desk top exercise was facilitated by the College's insurers, Zurich, in September 2019. This was attended by members of the College ELT and SLT. The scenario was an explosion and fire at the Arbroath Campus CALC building.

The objectives of the workshop were to:

- Rehearse the response of the College to a major incident, including:
  - Roles & responsibilities for decision making;
  - The immediate Incident Management response;
  - Resuming normal operations;
  - Communication with all key stakeholders throughout the incident & subsequent disruption;
- Identify gaps or updates required to current plans; and
- Identify actions required to improve the College's response to major incidents.

The Vice Principal Support Services and Operations advised that a further desk top exercise with Zurich will be programmed in the next 12 months.

A desk top exercise was also carried out in 2022 to test the Cyber Incident Response Procedure. This was facilitated by HEFESTIS. Another exercise is planned for later this year, following the planned update of the Procedure.

In addition, the BCP has been 'live' tested during the cyber-attack and COVID-19 pandemic, and smaller incidents such as Storm Babet.

Objective 5: The processes and procedures in place follow recommended good practice.

A comparison of the College's business continuity management arrangements was made against an ISO Business Continuity Management System (BCMS) self-assessment questionnaire. This noted many areas where the College's arrangements aligned with good practice however there were a small number of areas where they did not fully align, which can be summarised under three headings (as described in the UK Government Business Continuity Management Toolkit).

Business Impact Analysis (BIA)
A BIA identifies and documents an organisation's key products and services; the critical activities required to deliver these; the impact that a disruption of these activities would have on the organisation; and the resources required to resume the activities. This includes setting the point in time at which each of the key products and services would need to be resumed in the event of a disruption (this is often referred to as the Recovery Time Objective or RTO).

This would also include an analysis of the threats to any outsourced processes and their impact on achieving BCMS and RTOs.

Risk Assessment
In the context of business continuity management, a risk assessment looks at the likelihood and impact of a variety of risks that could cause a business interruption. By assessing these, organisations will be able to prioritise their risk reduction activities. Organisations should focus their risk assessment on the critical activities and supporting resources identified in the BIA stage. For this reason, a risk assessment can only take place once a BIA has been completed.

Determining Business Continuity Management Strategy
This stage of the business continuity management process is about identifying the action that an organisation can take to maintain the critical activities that underpin the delivery of the organisation's products and services. Having previously determined the RTO for each critical activity, the organisation now needs to develop a strategy for meeting it. This involves taking appropriate action to mitigate the loss of the resources identified at the BIA stage.

The performance of the BIA, risk assessment and determination of strategy would link in with the preparation of Disaster Recovery Plans for key departments and functions as referred to under Objective 3 above. As previously noted, discussion with the Vice Principal Support Services and Operations indicated that the College does not have the management or staff resources to prepare department Disaster Recovery Plans and keep these up to date.

A recommendation was made following our previous review of business continuity in 2019 to reflect the new requirements of ISO 22301 in the next iteration of the BCP, specially around setting measurable objectives and performance evaluation. Although this was accepted at the time, the ARC accepted a management recommendation that this not be implemented as, following the cyber-attack, the College undertook an analysis and evaluation of the performance and effectiveness of its business continuity management, and it was not found to be deficient. Management do not believe that the lack of reference to ISO 22301, nor the individual and extensive elements required by the standard, has impacted on the effectiveness of the plans enacted as a result of 'real life' business continuity issues. Therefore, we have not raised a recommendation on this point.

Henderson Loggie

Aberdeen 45 Queen's Road AB15 4ZN
Dundee The Vision Building, 20 Greenmarket DD1 4QB
Edinburgh Ground Floor, 11-15 Thistle Street EH2 1DF
Glasgow 100 West George Street, G2 1PP

T: 01224 322 100
T: 01382 200 055
T: 0131 226 0200
T: 0141 471 9870

F: 01224 327 911
F: 01382 221 240
F: 0131 220 3269

Agenda Item 7.2

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 5 March 2024

INTERNAL AUDIT

7.2- 2022/23 PROGRESS REPORT PAPER F

Dundee & Angus College

Internal Audit Progress Report

Audit & Risk Committee – 5 March 2024

Issued: 26 February 2024

Henderson Loggie

Internal Audit Progress Report
March 2024

Progress in delivering the annual plan for 2023/24 is shown below.

Audit Area	Planned reporting date	Report status	Report Number	Overall Conclusion	Audit & Risk Committee	Comments
Annual Plan 2023/24	September 2023	Draft: 29/08/23 2nd Draft: 07/09/23 Final:	2024/01	N/A	19/09/23	
Procurement and Creditors / Purchasing – Sustainable Procurement	June 2024					Fieldwork scheduled for w/c 18/03/24
Sports Centre Operations BPR	December 2023					Fieldwork commenced 19/02/24 and this review will now be reported at the ARC meeting on 04/06/24.
Risk Management and Business Continuity / Disaster Recovery Planning	March 2024	Draft: 06/02/24 Final: 07/02/24	2024/02	**Satisfactory**	05/03/24	
Environmental Sustainability	June 2024					Fieldwork scheduled for w/c 25/03/24
Credits	December 2024					Fieldwork scheduled for w/c 19/08/24

Audit Area	Planned reporting date	Report status	Report Number	Overall Conclusion	Audit & Risk Committee	Comments
Bursary, Childcare and Hardship Funds	December 2024					Fieldwork scheduled for w/c 12/08/24
EMA	December 2024					Fieldwork scheduled for w/c 12/08/24
Follow Up Reviews	September 2024					Fieldwork scheduled for w/c 08/07/24

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

info@hlca.co.uk
hlca.co.uk

Aberdeen 45 Queen's Road AB15 4ZN **T:** 01224 322 100 **F:** 01224 327 911
Dundee The Vision Building, 20 Greenmarket DD1 4QB **T:** 01382 200 055 **F:** 01382 221 240
Edinburgh Ground Floor, 11–15 Thistle Street EH2 1DF **T:** 0131 226 0200 **F:** 0131 220 3269
Glasgow 100 West George Street, G2 1PP **T:** 0141 471 9870

Agenda Item 7.3

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 5 March 2024

INTERNAL AUDIT

7.3- FOLLOW UP SUMMARY

PAPER G

BOARD OF MANAGEMENT

Audit & Risk Committee
Tuesday 5 March 2024

Audit Recommendations Follow-up Summary

Paper F 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.

3. Background

The following provides a summary of current progress in respect of audit recommendations up to February 2024.

Audit Area	Rec. priority	Considered, but not agreed	Number agreed	Number fully implemented	Number partially implemented	Behind original implementation date	On target	Implementation date (month end)
Student invoicing & debt management April 2022	3	-	1	-	-	1	-	Jan 2024
Distance/workbased learning July 2023	3	-	1	-	-	-	1	Mar 2024
Credits claimed	2	-	1	-	-	-	1	June 2024
July 2023	3	-	1	-	-	-	1	June 2024
Award letters August 2023	3	-	1	-	-	-	1	May 2024
Capital projects Sept 2023	3	-	3	-	-	-	3	June 2024
Annual accounts – deficiencies in internal control December 2023	2	-	2	-	-	-	2	July 2024
Risk Management February 2024	3	-	4	1	-	-	3	Sept 2024
Total		**-**	**14**	**1**	**-**	**1**	**12**	

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

Progress to February 2024

The final sign off in terms of the recommendation to review our student invoicing and debt management policy has been recorded as delayed because we are now carrying out a more significant review of all arrangements surrounding student debt alongside the implementation of the REMS student management and revised payments system project. This work is expected to be completed by 31 August 2024.

The audit recommendation of 2022 related only to an update of the existing procedure (which has not been a priority) and it is proposed that this recommendation be removed from future reporting as it has been overtaken by the introduction of the new system and new ways of working.

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

4. 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
Billy Grace, Head of Estates
Nicky Anderson, Director of Finance
Executive Sponsor: Steve Taylor, Vice Principal Support services and operations

Outstanding Recommendations Update March 2024 Appendix 1

Year	Audit Area Report Title	Priority Action Grade	Report Grade	Action	Responsible Officer	Deadline	Progress (as at March 2024)
2022/04	R3 – Student Invoicing and Debt Management	3	Satisfactory	A review of the College's written debt management procedures should be conducted, and the document should be updated to reflect the changes in working practices which have been brought in as a result of remote working and the impact of the COVID-19 pandemic.	Head of Finance	~~August 2022~~ ~~January 2023~~ ~~January 2024~~ Revised actions and deadline August 2024	Behind schedule The current Financial Procedure remains valid and collection has been augmented by additional methods of reaching out to students such as Teams and texts. A review of all arrangements surrounding the management of student debt is underway with arrangements linking into the implementation of the REMS student management system and revised payment systems. **Action is recommended for deletion from the list**
2023/07	R1 – Distance / Workbased Learning	3		The College should ensure evidence of progression and participation / engagement is retained to evidence eligibility of the Credits claimed for workbased learning students. Where curriculum staff identify that no evidence is available, or that students are no longer engaging, this should be notified to the Student Records team to ensure that the Credits are removed from the Credits claim	Administration Manager and Directors of Curriculum & Attainment	End March 2024	On target

Year	Audit Area Report Title	Priority Action Grade	Report Grade	Action	Responsible Officer	Deadline	Progress (as at March 2024)
2023/07	Credits Claimed	2		R2 Ensure that any significant changes to the Credits claimed after audit sampling are brought to auditor's attention on a timely basis so that these can be considered for testing prior to conclusion of the audit fieldwork stage.	Data Management Team Leader	End June 2024	On target
2023/07	Credits Claimed	3		R3 Attendance records should be maintained on CELCAT to support the actual hours completed, and Credits claimed, for infill deferrals.	Data Management Team Leader and Directors of Curriculum & Attainment	End June 2024	On target
2023/08	Award Letters	3		R1 Ensure that revised award letters are always issued, and copies retained, where reassessment of student awards is made during the year.	Student Funding Team Leader and Student Services Manager	End May 2024	On target
2023/09	Capital projects	3	Satisfactory	R1 – Reinstate the formal project appraisal procedures detailing the circumstances and threshold for the requirement to provide a strategic business case, and the level of appraisal required for projects below this threshold.	Director of Infrastructure	End June 2024	On target
2023/09	Capital projects	3	Satisfactory	R2 – For projects above an appropriate cost threshold ensure that recognised risk management processes such as project risk registers are utilised.	Director of Infrastructure	End June 2024	On target

Year	Audit Area Report Title	Priority Action Grade	Report Grade	Action	Responsible Officer	Deadline	Progress (as at March 2024)
2023/09	Capital projects	3	Satisfactory	R3 – It is recommended that a procedure be implemented which requires that all selection documentation for projects above a defined financial threshold which are not processed in conjunction with the Procurement Team (or compliant equivalent such as the SCAPE framework) be documented in a common format to support high level review to ensure that procedures are followed in line with the relevant regulations	Director of Infrastructure	End June 2024	On target
2023/12	External Audit Annual Report – deficiencies in internal control	Level 2 (medium)	--	It is recommended an asset revaluation or at least an indexation estimate from an appropriately qualified property valuation expert is carried out annually	Director of Finance	31 July 2024	On target
2023/12	External Audit Annual Report – deficiencies in internal control	Level 2 (medium)	--	It is recommended that management perform an annual review of the fixed asset register and ensure all assets being reported still exist and are in use. Any assets which are no longer in use or cannot be located should be accounted for as disposals.	Director of Finance	31 July 2024	On target

Year	Audit Area Report Title	Priority Action Grade	Report Grade	Action	Responsible Officer	Deadline	Progress (as at March 2024)
2024/02	Risk Management	3	Satisfactory	R1 - The following amendments to the SRR should be considered: • adding monitoring of activity targets to the list of monitoring reports on the SRR for risk 2.2 'Failure to achieve institutional sustainability'; and • adding a further strategic risk in relation to attracting, engaging, retaining and developing appropriately qualified staff.	Vice Principal Support Services & Operations	End March 2024	Completed
2024/02	Risk Management	3	Satisfactory	R2 - The College should develop a framework to provide further guidance on how to assess the impact and likelihood of identified risks, ensuring a consistent approach for risk assessment.	Vice Principal Support Services & Operations	End Sept 2024	On target
2024/02	Risk Management	3	Satisfactory	R3 - The Board should consider and establish what the College's high-level risk appetite is for each defined risk category, and residual risks on the SRR should be formally considered for compatibility with this stated risk appetite. The UK Government Orange Book guidance note on risk appetite can be used for reference, particularly in relation to documenting the risk appetite.	Board of Management	End Sept 2024	On target

Year	Audit Area Report Title	Priority Action Grade	Report Grade	Action	Responsible Officer	Deadline	Progress (as at March 2024)
2024/02	Risk Management	3	Satisfactory	R4 - A plan should be implemented to ensure that periodic risk management training is provided for Board members, senior managers and other relevant College managers and staff.	Vice Principal Support Services & Operations and Board of Management	End Sept 2024	On target

Agenda Item 8.0

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 5 March 2024

STRATEGIC RISK REGISTER

(i) RISK REGISTER UPDATE — PAPER H
(ii) STRATEGIC RISK REGISTER

BOARD OF MANAGEMENT
Audit and Risk Committee
Tuesday 5 March 2024

Strategic Risk Register Update

Paper G for approval

1. Strategic Risk Register

A copy of the March 2024 draft Strategic Risk Register is enclosed. This is noted for approval and incorporates the changes arising from discussion at the December 2023 Audit & Risk Committee meeting and recommendations arising from the recent internal audit on Risk Management.

2. Credit Target/Funding Risks

Following on from previous updates in respect of the reduction in full-time student recruitment in 2021/22 and in 2022/23, discussions have progressed well between Colleges Scotland, the Scottish Government, and the Scottish Funding Council around a range of sector wide flexibilities and rule changes to better support the sector.

These discussions have resulted in the removal of any risk associated with clawback of income in respect of the 2022/23 activity target. This has been confirmed in writing by SFC.

National discussions are progressing in respect of 2024/25 and beyond, with discussion around greater sector engagement and advance warning of future changes being welcomed.

In respect of D&A, activity levels in 2023/24 will mean that there is no risk in respect of the clawback of funding as activity targets will be achieved.

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. A final update on progress through these savings plan was discussed at the September 2023 Board meeting.

The most recent management accounts and budget monitoring reports considered by the Finance and Property committee confirm that the College is on track to achieve a better than break even position for 2023/24 and initial discussions on the budget for 2024/25 are pointing to this being developed on a sustainable basis.

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.

4. Cost of Living Crisis

Significant activities were reported in respect of the Thrive with D&A project to support students and staff with the challenges faced by the cost of living crisis. Following review of the impact of this work it was agreed that this would continue throughout 2023/24, including provision of the free food offer for students and staff.

5. Reinforced Autoclaved Aerated Concrete (RAAC) Risk

Following discussion at the Board of Management and Audit & Risk Committee the risks surrounding RAAC were included as an example within risk 4.1.

In respect of RAAC itself, there is no change in respect of the needs or arrangements associated with the monitoring of condition. Updates have, however, been provided to the Finance and Property Committee on initial steps towards the next infrastructure vision for the whole College estate, including potential phasing of future developments to remove RAAC from our estate.

On a practical level, a business continuity plan has been created to address the continuation of curriculum and service should there be a need to vacate either of the current areas that have RAAC present.

6. Review of Strategic Risk Register

The draft March 2024 Strategic Risk Register is enclosed.

This has been subject to review following discussion at the December 2023 Audit & Risk Committee, and as a result of the recent Risk Management audit as follows.

Risk		Changes Made
2.1	Change in SFC Funding Methodology and Allocation – Reduction in Funding	Wording amended to reflect potential new funding body and/or funding arrangements arising from sector reform (Withers report)
2.2	Failure to achieve institutional sustainability	Additional mitigations identified to reflect national discussions and changes (flexibilities) emerging through the Tripartite group. Additional monitoring identified to reflect change to mitigations and to clarify link between strategy and funding. Additional monitoring point identified to reflect recommendation arising from Risk Management audit in respect of activity (credit) targets.

Risk		Changes Made
3.12	Failure to attract, engage, retain or develop appropriately qualified staff.	Additional risk with mitigation and monitoring actions created following discussion with Henderson Loggie as part of the recent audit on Risk Management
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	Additional risk with mitigation and monitoring actions created following discussion with Audit & Risk Committee

7. Approvals

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

- 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

2023 - 2024

As at March 2024

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	4	Major	Probable
	DirInf	Director of Infrastructure	Chair	Chair of the Board of Management	5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS: Risks	Impact	Likelihood	Score	TREATMENT: Mitigation Actions	Impact	Likelihood	Score	POST MITIGATION EVALUATION: Monitoring	Lead Responsibility
1 Strategic and Structural										
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	2	8 ↔	• Robust monitoring via ROA • 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	3	12 ↔	• Review of changes and amendment of strategic direction/plans • Financial strategy sensitivities	Principal & Chair

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

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

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS: Risks	Impact	Likelihood	Score	TREATMENT: Mitigation Actions	Impact	Likelihood	Score	POST MITIGATION EVALUATION: Monitoring	Lead Responsibility
1 Strategic and Structural										
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
1.4 Board	College disadvantaged as a result of changes arising from major national educational body reviews: SFC, SQA, EdS	4	4	16	• Negotiation/influence at national level • Review of activities/ projects and response to new opportunities	4	1	4 ↔	• Robust monitoring via ROA • Amendment of strategic direction/ plans • Rolling curriculum review	Principal

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

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

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS: Risks	Impact	Likelihood	Score	TREATMENT: Mitigation Actions	POST MITIGATION EVALUATION: Impact	Likelihood	Score	Monitoring	Lead Responsibility
1 Strategic and Structural										
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	4	2	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: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

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

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility
2 Financial										
2.1 **F&P**	Change in Funding Body and/or Funding Methodology and Allocation – Reduction or restriction in Funding **Amended Wording to reflect potential new funding body/arrangements**	3	4	12	• Negotiation/influence at national level • **Contingency plans for amended funding levels or requirements**	3	3	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 **Additional mitigation and monitoring actions noted**	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	VPSO
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

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

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

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Lead Responsibility
2 Financial (cont)										
2.4 **A&R**	Financial Fraud	4	3	12	• Strong financial controls: segregation of duties and review of transactions. • Review of impact of any changes in structure or duties • Whistleblowing arrangements	3	2	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	3	2	6	• Multi-year estates strategy and capital planning • Lobbying of SFC on capital and backlog maintenance funding • Planning for D&A Foundation bids	2	2	4 ↔	• Monitoring of capital plans and expenditures • Regular review of capital plans/timescales relative to funds	VPSO

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

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS: Risks	Impact	Likelihood	Score	TREATMENT: Mitigation Actions	POST MITIGATION EVALUATION: Impact	Likelihood	Score	Monitoring	Lead Responsibility
3 People and Performance										
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	3	2	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	5	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: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

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

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Lead Responsibility
3 People and Performance (cont.)										
3.4 HR&D	Failure to meet the aspirational standards in respect of the health, safety, wellbeing and development of staff and students	3	4	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	3	12	• Marketing strategy • Reputation plan • Positive marketing approaches	4	3	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: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

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

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS: Risks	Impact	Likelihood	Score	TREATMENT: Mitigation Actions	POST MITIGATION EVALUATION: Impact	Likelihood	Score	Monitoring	Lead Responsibility
3 People and Performance (cont.)										
3.7 **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**	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

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

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS: Risks	Impact	Likelihood	Score	TREATMENT: Mitigation Actions	POST MITIGATION EVALUATION: Impact	Likelihood	Score	Monitoring	Lead Responsibility
3 People and Performance (cont.)										
3.10 **HR&D**	College arrangements do not minimise risk associated with Modern Slavery	4	3	12	• Clear and compliant procurement arrangements and procedures • Staff identity checking arrangements and use of PVG.	4	1	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	4	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
3.12	Failure to attract, engage, retain or develop appropriately qualified staff. **New Additional Risk**	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: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

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

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility
4 Infrastructure										
4.1 A&R	Major Disasters – eg Fire, MIS Failure, Failure of Emergency Procedures, RAAC or similar infrastructure failure	5	4	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	4	2	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: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

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

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS: Risks	Impact	Likelihood	Score	TREATMENT: Mitigation Actions	POST MITIGATION EVALUATION: Impact	Likelihood	Score	Monitoring	Responsibility
4 Infrastructure										
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 **New Additional Risk**	4	4	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	3	4	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: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

Agenda Item 10.0

BOARD OF MANAGEMENT

Audit & Risk Committee

Tuesday 5 March 2024

DATE OF NEXT MEETING

Tuesday 4 June 2024 at 5.00pm in Room A625, Kingsway Campus