Edinburgh College

AUDIT & RISK ASSURANCE COMMITTEE

AGENDA

A meeting of the Audit & Risk Assurance Committee will be held at 15:00 hours on Wednesday 02 October 2024 via Microsoft Teams.

		Lead Speaker	Paper
1	WELCOME & APOLOGIES	Chair	
2	DECLARATIONS OF INTEREST	Chair	
3	MINUTES OF PREVIOUS MEETING ***for approval***	Chair	A
4	MATTERS ARISING REPORT		
	4.1 Matters Arising Update	Chair	B
	4.2 Business Committees of the Board Update		
	• Planning & Resources Committee	A Williamson	Verbal
	• Learning, Teaching & Student Experience Committee	M Walker	Verbal
	• Corporate Development Committee	M Walker	Verbal
5	INTERNAL AUDIT REPORTS		
	5.1 Internal Audit Follow-up Report	BDO	C
	5.2 Internal Audit Report: Estates Management	BDO	D
	5.3 Internal Audit Report: Learning & Development	BDO	E
	5.4 Internal Audit Annual Report 2023/24	BDO	F
6	RISK ASSURANCE		
	6.1 Three Lines of Defence Annual Review	A Williamson	G
	6.2 Risk Management Report	A Williamson	H
	6.3 Annual Report on Data Breach Incidents and Cyber A ttacks Update	A Williamson	I
7	EXTERNAL AUDIT		
	7.1 Compliance with the Code of Good Governance	M Walker	J
	7.2 Internal Control Assurance Statements	A Cumberford	K
	7.3 Draft (Unaudited) Annual Report and Financial Statements to July 2024	I Deed	L
	7.4 External Auditor Briefing	Mazars	M
8	ANY OTHER COMPETENT BUSINESS		
	8.1 Horizon Scanning Update	Mazars / BDO	Verbal

9 FOR INFORMATION

- 9.1 Audit & Risk Assurance Committee Terms of Reference
- 9.2 Audit & Risk Assurance Committee Business Planner 2024/25

10 FOR CIRCULATION

- 10.1 Audit Scotland: Scotland's Colleges 2024
- 10.2 Internal Audit Annual Audit Plan 2024/25

11 DATE OF NEXT MEETING: 20 November 2024

N.B: The minutes of the Audit & Risk Assurance Committee are reported directly to the Board of Management, with an accompany commentary from the Committee Chair.

AUDIT & RISK ASSURANCE COMMITTEE
02 OCTOBER 2024
PAPER G

Title	**Edinburgh College – 'Three Lines Of Defence' Framework – Annual Review Update 2024**
Appendices	Appendix 1: Edinburgh College Three Lines of Defence Framework
Disclosable under FOISA	Yes ☒ / No ☐
Primary Contact	Ian Deed, Director of Finance and Estate Infrastructure
Date of Production	02.09.24
Action Required	For Approval ☐ / For Discussion ☒ / For Information ☒
Aligned to Strategic Risk	Yes ☐ / No ☒ *(If 'yes' please complete Section 5.3)*

1. RECOMMENDATIONS

The Committee is asked to NOTE and CONSIDER the 2024 annual review of the Edinburgh College 'Three Lines of Defence Framework'.

2. PURPOSE OF REPORT

The Board and Senior Management collectively have responsibility for setting College objectives, defining strategies to achieve them and establishing the necessary governance risk management and control frameworks to manage the associated risks.

This report provides the 2024 annual review update on the overall control, assurance, and risk management arrangements for managing risk and exercising control within the College shown in the Edinburgh College 'Three Lines of Defence' Framework.

3. KEY INSIGHTS

The 'three lines of defence' model is designed to improve an organisation's approach to internal control, assurance and risk management. The model can be summarised as follows:

- **First line of defence** – functions that lead on designing and implementing appropriate mitigating controls rests with operational management who own and manage risks within key business areas.

- **Second line of defence** – risk management and compliance functions that help build and/or to monitor the first line of defence controls across an organisation.

- **Third line of defence** – functions that provide internal and external audit assurance and / or independent assurance of key business areas and risks across an organisation. Internal audit provides assurance on the effectiveness of governance, risk management and internal controls, including the first and second- line controls. External auditors/ regulators play an important role through their considerations of the governance and control structure where this is relevant to financial reporting.

In September 2024 the third annual review took place of arrangements in place across 22 key areas of college business, and associated risks described in the Framework.

Specifically, the College has strengthened first and second line defences in some areas. This includes:

- Curriculum and credit delivery – a recent Education Scotland visit and associated report has identified areas of good practice as well as recommendations for improvement which are being put into place.

- Commercial delivery – Work has been completed by the Commercial Team and Finance Team in clearly identifying income streams across all College areas. This has been shared with the SMT, and regular 'more accurate' quarterly reporting is now being used. As a result, there will be improved internal control and co-ordination of income streams associated with apprenticeships, international, commercial, facilities provision (nursery, accommodation etc) and industry engagement activities. The current phase is matching associated expenditure against these income streams.

- Learning Teaching & Assessment – The LTSE Committee of the Board provides a more focused approach to LTSE matters at a more strategic level but underpinned by robust performance oversight which incorporates key operational matters. The Board are currently reviewing its Committee structure and there is potentially a further Committee change which will cover curriculum planning and student success.

- Financial and other Internal Controls – The approved annual Audit Plan by the Audit & Risk Assurance Committee, and the work undertaken by external auditors during the year has provided a level of assurance that internal controls continue to be robust.

- Fraud and Irregularity – The Counter-Fraud, Bribery and Corruption policy has been reviewed and updated where required.

- Cyber Security & Information Management – An internal audit review identified recommendations to improve cyber resilience, work continues to close these off.

In summary, the internal control arrangements identified in the Framework continue to **operate effectively**. No significant gaps were identified across the 22 key areas of business, and consequently, no further action is proposed.

4. IMPACT AND IMPLICATIONS

Effective operation of the 'three lines of defence' framework improves the College's effectiveness in managing top level risks and operational risks across the College. The framework also enables effective management of key business areas tasked with delivering college's strategic objectives.

5. ALIGNMENT TO STRATEGIC PLAN / KPIs / RISK REGISTER

5.1 Alignment to Edinburgh College Strategic Pillars *[Indicate with an 'X' which Strategic Pillar this paper supports]*:

Curriculum Strategy	☒	Finance Strategy	☒	People Strategy	☒
Commercial Strategy	☒	Digital Strategy	☒	Other	□

5.2 Relevant Key Performance Indictors *[Indicate with an 'X' which performance indicators this paper supports]*:

Student Success	☒	Credit Target	☒	Equality, Diversity & Inclusion	☒
Student Satisfaction	☒	Adjusted Operating Position (AOP)	☒	Staff Costs	☒
Student Retention	☒	Non-SFC Income	☒	Staff Engagement	☒
Student Enrolments	☒	Gross Carbon Footprint	☒	Partner Engagement	☒

5.3 Alignment to the Top-Level Risk Register *[Strategic risk information should be copied directly from the most recent TLRR]*:

<table>
<tr><th>Strategic Risk(s)</th><th colspan="3">Risk Score*</th></tr>
<tr><td rowspan="7">Not Applicable.</td><td colspan="3">Inherent (Gross) Risk</td></tr>
<tr><td><i>Probability</i></td><td><i>Impact</i></td><td><i>Score</i></td></tr>
<tr><td>-</td><td>-</td><td>-</td></tr>
<tr><td colspan="3">Residual (Net) Risk</td></tr>
<tr><td><i>Probability</i></td><td><i>Impact</i></td><td><i>Score</i></td></tr>
<tr><td>-</td><td>-</td><td>-</td></tr>
<tr><td colspan="2">Movement (since last review)</td><td>-</td></tr>
</table>

**Risk Score Key: 0-10 Low Risk; 11-15 Moderate Risk; 16-25 High Risk. [Further information on risk scoring can be found in the EC Risk Management Policy & Procedure]*

Appendix 1

Edinburgh College - Three Lines of Defence Framework – Annual Review Update – September/October 2024

Business Area	1st line Defence		2nd line Defence		3rd line Defence		Gaps + Remedial Action
	Key Controls	Sources of Assurance	Internal Compliance and Quality Checks	Sources of Assurance	Internal Audit and other Independent Assurance	Sources of Assurance	
1. Student Recruitment and Retention, Attainment, Achievement and Destination	Weekly AP Meetings Recruitment, Admissions and Induction Group (chaired by Student Experience Manager – Recruitment and Admissions) Focus on recruitment, retention and attainment in Course Team meetings with standard agenda – also Heads of School and Curriculum Team Managers meetings. How Good is our Learning and Teaching – (HGIOLT) structured meetings – 3 per year per school, chaired by AP and supported by critical friend MIS produce live reports pathway for review on applications, offers, registrations and withdrawals Quality Team oversight of academic resulting	Minutes from meetings and progress updates on agreed actions from each meeting Regular MIS and chair of group reporting to VP Education and Skills and VP Innovation, Planning and Performance Quality Team agreed academic results	Regular reporting to Executive Team and Senior Management Team Regular reporting to Policy and Resources Committee Deep Dives led by Audit and Risk Assurance Committee ROA reporting to the Board of Management ROA + curriculum results reportage to Learning, Teaching and Student Experience Committee Student destination survey reports to Learning, Teaching and Student Experience Committee	Agreed minutes and progress with actions of Executive Team and Senior Management Team Agreed Board and committee reports and minutes	ROA reporting to the SFC Internal FES audit and FES return to SFC	SFC agreement of the ROA report Agreed internal audit report and actions Approved FES return by SFC	No gaps identified.

2. ROA and Credit Delivery	Assistant Principal (AP) faculty management team meetings reviewing ROA and credit target delivery. Assistant Principal one to one meetings with Heads of School (HoS), and Curriculum Team Managers (CTMs). Faculty Operational Plans including ROA and credit targets. Fixed agenda item at all Team Meetings	MIS credit checker on staff intranet Reports Pathway. How Good is Our Learning & Teaching meetings (HGIOLT) 3 per academic year. Reviews of Faculty Operational Plans.	MIS quality checks on credit delivery. VP Education and Skills meetings with all APs, Heads of School and Curriculum Team Managers to review ROA + credit delivery. Faculty Operational Plan performance meetings. VP Education and Skills reports to Policy and Resources Committee on credit delivery.	Annual plan performance measures MIS reports on credit delivery to VP Education and Skills. Agreed Team Meeting & HGIOLT minutes and progress against actions. Reports to Policy and Resources Committee.	Annual internal FES audit (also reported to Audit and Risk Assurance Committee) and FES submission to SFC.	Year-end internal audit report and FES report sign-off by the SFC.	No gaps identified.
3. Curriculum Relevance and Coherence (including industry and employer engagement)	New courses submitted through Course Manager overseen and approved by HoS, and CTMs. Existing course delivery quality and efficiency checked by HoS, CTMs and Quality Team at HGIOLT meetings Aps weekly meetings with HoS to oversee curriculum design and delivery. Operational Plans indicate new course proposals. ROA annual - curriculum target setting process. External Engagement Group meetings.	Course Manager information signed off by Quality Team Manager and AP / HoS / CTMs. Quality and efficiency reporting from HoS and CTMs to APs. Agreed AP / HoS and CTMs meeting notes. Agreed annual Operational Plans. Agreed ROA – annual. Agreed reports and minutes from the External Engagement Group.	Internal and external verification of courses in line with SQA and other awarding body guidelines. HoS regular discussions with CTMs and agreed actions. CTMs regular discussions and agreed actions with lecturing staff on curriculum delivery. Executive Team Performance Review process looking at ROA target delivery. Curriculum Strategy reviewed by Learning, Teaching and Student Experience Committee, P&R Committee, & Board.	Internal Verification and External Verification processes signed off by Assistant Principal Curriculum Performance and Planning. ROA signed off by the Board. External Engagement Committee meetings agreed reports and minutes. SMT agreed reports and minutes. SCP Strategic Board agreed minutes and actions.	Education Scotland Inspection visits. Evaluative Report and Enhancement Plan submission to Education Scotland. SFC ROA review process - annual. Internal audit of partnership working including industry and employer engagement.	Agreed Education Scotland Inspection Reports. Agreed EREP and actions by Education Scotland. SFC approved ROA – annual report. Agreed internal audit reports and actions.	No gaps identified.

	Commercial Team meetings designing and approving the commercial curriculum offer. Schools College Partnership meetings.	Commercial Team meeting agreed minutes and actions. SCP meeting minutes and agreed actions.	Learning, Teaching and Student Experience Committee monitoring of performance against ROA targets Learning, Teaching and Student Experience Committee review of SDS Regional Skills Assessment. Corporate Development Committee meetings covering industry engagement. SMT discussion on industry and employer engagement. SCP Strategic Board ran by the College.				
4. Learning Teaching and Assessment	How Good is our Learning and Teaching – (HGIOLT) structured meetings – 3 per year per school, chaired by AP and supported by critical friend Course Team meetings with standard agenda Heads of School and Curriculum Team Managers meetings. Engagement with student voice including promotion and delivery of 2 college-wide satisfaction surveys annually Edinburgh College delivery of PDA Teaching Practice in	Completed HGIOLT evaluation and action template Team meeting agreed minutes and actions. Agreed minutes and actions Survey feedback dashboard and records, collated feedback report and student feedback tracker Staff achievement of formal qualifications – learning, teaching, assessment and verification.	Learning, Teaching and Student Experience Committee discussions and papers on learning, teaching and assessment. ECSA surveys, covering issues of the quality of learning, teaching and assessment. SMT and Executive discussion and actions on learning, teaching and assessment.	Learning, Teaching and Student Experience Committee agreed reports and minutes. ECSA published survey results. Student feedback tracker SMT and Executive agreed minutes and actions.	Production and submission of Self Evaluation and Action Plan - SEAP (from November 2024) to SFC. Engagement in Tertiary Quality Enhancement Review (TQER) – 6 yearly cycle from 2024/25 – supported by annual engagement with Quality Agency (QAAS) SQA and other awarding body	Agreed SEAP Successful outcome of TQER Agreed SQA	No gaps identified.

	Scotland’s Colleges, Assessor Verifier awards, Teaching Creative and Critical Thinking. Professional Standards and TFQE programme. Planning and implementation of risk-based internal verification, and engagement with external verification (awarding bodies). Connect Groups related to learning, teaching and assessment. Edinburgh College I V and E V processes.	Agreed college IV and EV findings and remedial actions.			external verification processes.	and other awarding body external verifications.	

5. Student Safeguarding	Top desk safeguarding reports from staff monitored and reviewed and actioned by Safeguarding Lead. Safeguarding mandatory training module. Student Experience Team management meetings.	Weekly reporting from Safeguarding Lead to Student Experience Manager – Learning Development and Wellbeing. Compliance data on mandatory training modules. Agreed Student Experience Team reports and minutes on Safeguarding.	Safeguarding update to Assistant Principal Student Experience every six weeks. Quarterly College Safeguarding Forum meeting. SMT discussions and reports on safeguarding. Committee 'deep dives' into safeguarding issue.	Agreed actions from Safeguarding updates (as required). Agreed minute of the Safeguarding Forum. Agreed SMT and committee reports and minutes.	Quality Agency reviews of safeguarding arrangements.	Positive Review Reports.	No gaps identified.
6. Student Experience	ECSA annual plan which shows the priority student initiatives to improve the student experience – annual. Student surveys and polls undertaken. Student Experience Management Team meetings. ECSA liaison meetings with VPs and other SMT members.	ECSA feedback and input at key college management meetings. Agreed student survey findings Agreed management team meeting minutes and actions. Agreed actions from ECSA liaison meetings.	ECSA President provides reports to Learning, Teaching and Student Experience Committee and the Board. ECSA and College student survey findings reported to Learning, Teaching and Student Experience Committee. Regular report to Learning, Teaching and Student Experience Committee from the AP Student Experience about SE matters.	ECSA reports reviewed by Learning, Teaching and Student Experience Committee and Board. Agreed Learning, Teaching and Student Experience Committee minutes and papers. Annual self-evaluation and action plan (SEAP).	Tertiary Quality Enhancement Review. Internal audit on student participation. SFC and QAA feedback on SEAP.	Agreed actions (SEAP) and TQER. Agreed internal audit report and actions.	No gaps identified.
7. Commercial Income and International	Commercial and Employer Working Group. International Working Group.	Working Group agreed actions.	Quarterly reporting of commercial income and forecast figures to Senior Management Team, Executive	Agreed commercial income report to committee and agreed committee minute.	Internal audit report on commercial activity.	Agreed internal audit report and actions.	No gaps identified.

Contract Management	Apprenticeships Working Group. Alternative Income and Innovation Working Group. Commercial income targets set annually as part of budget setting process. Commercial income targets monitored and reported monthly by Director of Commercial and VP Corporate Development. Finance check monthly reports. College finance and procurement policies and procedures for contracting International suppliers. Contracts with direct agents who represent the College and international group contracts include a bribery and corruption clause. Procurement Team oversee compliance with policies and procedures. Due diligence research regarding new college partners can be requested from Corporate Development.	Agreed commercial income figures by finance, VP Corporate Development and Director of Innovation & Knowledge Exchange. Contracts and Financial position monitored through the year. Signed documents and approval processes for international contracts. Completed due diligence reports. APUC policies and procedures.	Team and External Engagement Committee. External Engagement Committee oversight of international contracts.	Agreed External Engagement Committee reports and minutes.	Scottish Government Procurement Capability Assessment self-evaluation process. Internal audit on commercial activity and procurement / contract management.	Agreed Scottish Government PCA score and report. Agreed internal audit reports and actions.	

	APUC policies and guidance on awarding commercial contracts.						
8. Financial Controls (including income and asset recognition + expense and liability recording)	Annual budget setting with each AP and Director included in operational plans. Monthly management account meetings with each AP and Director. Monthly meetings between COO and Director of Finance. Annual SMT assurance statements including financial control, references. Maintaining up to date financial regulations as well as policies and procedures.	Agreed and signed annual budget, and agreed operational plans signed by Executive Team lead. Any actions taken as a result monthly meeting. Agreed email actions between COO and Director of Finance. COO agreed assurance statements. Agreed financial policies and procedures.	Senior Management and Executive Team review of financial controls, management accounts and performance. Quarterly reports to Planning and Resources Committee and the Board. Budget and SFC FFR process and papers to committees and Board. Statement of Internal Control (SIC) process. Budget and SFC FFR considered by P&R Committee and Board. Finance Report (including management accounts) reviewed by P&R Committee and Board. Regional Procurement Strategy approved by P&R Committee. Board Scheme of Delegation. SMT and Finance delegation of authority agreement process. Capital investment control guidelines.	Committee, Board, SMT and Executive Team agreed minutes + actions taken as a result. Agreed minutes + actions. Approved budget and SFC FFR return minute by P&R Committee & Board Statement of Internal Control (SIC) process - signed off by Principal / Chief Executive (annual). SMT delegation of authority statements.	Internal Audit and External Audit of finance including payroll & expenses + EMA, bursaries and student support funds (annual) + purchasing and creditors + procurement) Scottish Government CPA self-evaluation process.	External auditor signed Annual Accounts. Agreed internal audit reports for external audit assurance, and agreed management actions. Annual Account report for Audit Scotland and for Public Audit & Post Legislative Scrutiny Committee. Agreed Scottish Government CPA score and report.	No gaps identified.

9. Financial Performance & Financial Sustainability - including cash management	Draft Annual Accounts prepared by Director of Finance and checked by the Chief Operating Officer. Annual Accounts scrutinised and challenged by the Executive Team. Regular Cash flow forecast prepared and reviewed by Executive and SMT. SFC Cash flows prepared, reviewed and sent monthly. Financial controls relating to cash. Regular meetings between Finance Department and SMT Directors and Aps.	Draft Annual Account approved by Executive Team. Agreed notes and actions relating to discussions with SFC regards timing of grant income. Agreed actions and notes from Finance meeting with Directors and Aps.	Draft Annual Accounts audited by external auditors. External auditors present to Audit and Risk Assurance Committee. Senior Management and Executive Team reviews of financial performance. Quarterly Cash flow reports to Policy and Resources Committee and the Board. 5-year cash flow forecast process and papers to committees and the Board. Executive Team and SMT discussions on financial performance.	Annual Accounts signed off by Audit and Risk Assurance Committee and Board. Agreed committee and Board reports and minutes on financial and cash matters. Agreed Executive Team and SMT minutes and actions	Annual Accounts signed off by External auditors and laid before the Scottish Parliament. Internal Audit and External Audit of Cash flow and cash management.	Annual Accounts endorsed by the Scottish Parliament. Agreed internal audit reports and actions on finance matters.	No gaps identified.
10. Fraud and Irregularity -Fraud, -Theft, -Bribery, -Corruption.	College's Counter-Fraud, Bribery and Corruption Policy. College systems and procedures, which incorporate internal controls, include separation of duties to ensure that errors, fraud theft, bribery and corruption are prevented. Edinburgh College participates in the National Fraud Initiative (NFI). Whistleblowing policy and procedures.	Edinburgh College adherence to the Scottish Public Finance Manual regards fraud. Standards Officer monitors and responds to whistleblowing reports.	Committee, Board, SMT and Executive Team review of Fraud Bribery and corruption policies. The Code of Conduct for Board Members outlines their duty of honesty and the practice relating to declarations of interests.	Agreed Executive Team, SMT and Board reports and minutes regarding fraud. Signed Board member agreements on the code.	Internal and external audits of fraud and irregularity. Annual Assurance statement to the SFC.	Agreed internal and external audit reports and actions. Oversight of assurance statement by SFC.	No gaps identified.

	Mandatory module in place as part of general staff training.						

11. Health and Safety	SHE System used to control risk assessments, collate accident reports, and store policy and procedures. Monthly health and safety incident reports to SMT members.	Health and Safety Manager daily reviews of SHE reports. Agreed SMT actions to address issues arising from monthly reports.	Health and Safety Committee Meeting with Management and Trade Unions. Annual Health and Safety Report to the Board.	Agreed minutes of the meeting. Annual Health and Safety Report agreed by the Board.	Annual audit process for 18001.	Agreed 18001 audit report and agreed actions.	No gaps identified.
12. Estates Management and Compliance and Alignment to College Needs	Estates managers meetings with COO and other SMT members. Estates strategy and capital funding allocation prioritised and agreed by the Executive and SMT. Estates condition reviewed six monthly + monthly review of estates critical works register. Sustainability + Nursery + Facilities + Security + Porterage + Print Services + Vehicles + TFM + Halls Catering Contract + Regular management meetings. ISS contract management meetings weekly. Catering provider monthly contract meetings to review contract.	Agreed actions from estates Managers meetings. Oversight of performance, and statutory reports. Estates strategy signed off by the Executive Team. Estates expenditure included in monthly management accounts. Updated and agreed critical works register + condition survey. Agreed email actions from COO to Director of Finance and Estates Infrastructure. Agreed actions from the ISS contract meetings. Agreed actions from catering contract meetings.	SMT + Executive Team discussions on estates. Policy and Resources Committee papers and discussions on estates matters. Estates management matters are also included also in the Health and Safety Report to Health and Safety Committee.	SMT + Executive agreed reports and minutes on estates matters. Policy and Resources Committee agreed reports and minutes. Agreed Health and Safety Committee reports and minutes.	NQA Auditor process. Internal audit on estates management. Statement on estates management in the annual report. Care Inspectorate inspections of the nursery. HMO licence inspections of the Halls of Residence.	NQA agreed audit report and actions. Agreed internal audit report. Agreed annual report and accounts estates section. Agreed Care Inspectorate inspection reports and college actions relating to the nursery. HMO licensing report on Halls.	No gaps identified.

	Monthly utility monitoring.	Utility monitoring reports to estates management Team.					
13. **Digital / IT Capability and Alignment to College Needs**	IT Management Team meetings which cover cyber security. Estates and IT Management Team meetings. Digital Connect Group meetings. Learning, Technology and Teaching Connect Group meetings. Cyber security meetings and matters included at the Information Governance Group meetings.	Agreed IT meeting minutes and actions. Agreed Estates and IT Team meeting minutes and actions. Agreed Digital Connect Group and LTT Connect Group reports and minutes. IGG action plan and updates.	Audit and Risk Assurance Committee meetings + 'deep dives' to discuss digital + IT capability. SMT and Executive Team discussions on digital and IT capability. New Digital Strategy Board meetings.	Agreed reports and minutes of Audit and Risk Assurance Committee. Agreed SMT and Executive reports and minutes. Agreed Digital Strategy and Board minutes. A+RA Committee 'deep dives' into cyber security. Policy and Resources Committee scrutiny of digital strategy delivery.	Internal audits of IT related matters. External thematic audits by Audit Scotland.	Agreed internal and external audit reports and management actions.	No gaps identified.
14. **Organisation Development and Staff Wellbeing**	Monthly HR business partner meetings with all SMT members when staff wellbeing + OD is discussed. Team management and one to one meetings covering wellbeing and OD. Annual 'enhance' meeting assessing personal development.	Agreed actions from monthly HR meetings on wellbeing + OD. Agreed team meeting and one to one notes and actions on wellbeing + OD. Agreed 'enhance' records between managers and line reports.	HR reports to Policy and resources Committee. SMT reports on HR / OD matters, including HR / OD policy approval from Policy Committee. Director of HR & OD regular meetings with Executive Team members + Executive Team meeting reports on HR.	Policy and Resources Committee agreed minutes and reports on HR / OD. Agreed Executive Team minutes and actions relating to HR. Agreed HR / OD policies published on intranet.	Internal audits on HR and Od matters. External audit on HR matters as part of the annual audit report by Audit Scotland. Trade Union meetings.	Agreed internal audit reports and actions. Agreed annual audit report. Trade Union meeting minutes and	No gaps identified.

						agreed actions.	
15. Workforce Planning	Regular reviews of progress against operational plan objectives for OD team with Director of HR&OD. OD / HR Team meetings. Monthly HR business partner meetings with all SMT members – including establishment and vacancy lists and workforce planning. LJNC meetings and TU and Management Policy Committee meetings to develop and agree HR policies and discuss workforce planning. Succession planning included in SMT operational plans. Edinburgh College Workforce Plan developed by Director of HR and OD.	Agreed notes and actions arising from reviews. Agreed OD / HR team meeting minutes and actions. Agreed actions notes from SMT meetings with HR Business Partners. Agreed actions and minutes of LJNC and Policy Committee meetings. Agreed succession planning content in SMT operational plans. Agreed actions emanating from the workforce plan.	Regular reviews with progress and issues in HR & OD between COO and Director of HR & OD. SMT and Executive Team discussions and reports on workforce planning. HR reports to Policy and Resources Committee on workforce planning.	Agreed notes and actions from COO reviews with Director of HR & OD. Agreed Executive Team and SMT minutes and reports on workforce planning. Agreed Policy and Resources Committee reports and minutes on HR / OD and workforce planning.	Internal audit covering workforce planning. Audit Scotland Annual Report covers workforce planning matters.	Agreed internal audit report and actions.	No gaps identified.
16. College Industrial and Employee Relations	Edinburgh College RPA development process – including agreed remission time for TU officials. LJNC meetings with Executive management and the Director of HR & OD.	Agreed RPA by the Local Joint Negotiating Committee (LJNC). Agreed LJNC reports and minutes. Agreed Health and Safety Committee meetings reports and minutes.	Strategic Partnership meeting between Principal / Chief Executive and TU officials. Policy and Resources Committee discussions and reports. Audit and Risk Assurance Committee review of top-level	Agreed reports and minutes from Strategic Partnership meeting. Agreed Policy and resources Committee reports and minutes.	National bargaining arrangements / the Employers Association now cover many aspects of industrial and employee relations.	Agreed minutes and circulars from national bargaining / Employers Association.	No gaps identified.

	H+S Committee meetings including TU officials. Monthly meetings between COO and Director of OD / HR.	Agreed email actions between COO and Director of HR / OD.	risk register – which includes industrial relations risk. Executive Team and SMT meetings + reports – industrial and employee relations matters. Staff representation and TU observers at the Board.	Agreed SMT and Executive Team reports and minutes. Agreed minutes from the Board covering staff and TU matters.			
17. Strategic Direction	Executive and Senior management Team engaged in national policy and strategy development. Strategy, Plan and Policy Register reviewed regularly by Information Manager and of CGR+P (register contains all college strategies, plans and policies organised into 3 tiers). Regular review of key college strategies and plans. Annual operational planning process, linked to key college strategies and plans, and PESTLE analysis. Horizon scanning information included in the Principal's report to the Board. Strategy delivery monitored annually and included in the College Annual Report.	Executive and SMT agreed discussions and reports on national policy and strategy developments. Register updated quarterly by Information Governance Manager. Agreed quarterly Horizon Scanning Report. Agreed and published college strategies and plans, published on intranet and website. All operational plans approved by Executive Team.	Approval sought from Policy and Resources Committee for all key strategies and plans. All Committees and Board of Management consider Horizon Scanning report every cycle. Information Governance Group reviews the register quarterly, with a focus on strategy and plan development. Approval sought from SMT and Executive Team on new or revised strategies and plans. Board considers Annual Review Report. Executive Team performance reviews of Operational Plans.	Agreed reports and minutes, strategies and plans from Policy and Resources Committee. Agreed quarterly Horizon Scanning Report and committee and Board minutes. Agreed annual review report. Agreed reports and minutes from SMT on strategy and policy development. Agreed minutes and actions of performance review meetings.	Internal audit of strategic planning and performance. External audit of key college strategies and plans. SFC scrutiny of the College ROA and related strategies.	Agreed internal audit report and management actions. Agreed external audit reports and management actions. Agreed SFC ROA annual report.	No gaps identified.

18. Risk Management	Operational risk register review process – quarterly by Risk Management + Assurance Group (RMAG) meeting. Operational Plan review – top 3 operational risks - annual review process led by SMT and Executive.	Updated and agreed operational risk registers. Updated and agreed Operational Plans (top 3 risks for operational risk registers). Operational Plan sign off from Executive team lead members.	Top Level Risk Registers reviewed quarterly by the RMAG. A+RAA Non-Executive member always present at RMAG. SMT and Executive team discussions and reports on risk management + approval of top-level risk register to the Board.	Agreed Audit and Risk Assurance Committee reports and minutes on the top-level risk register and key risks from operational risk registers. Agreed Board minutes and top-level risk register + summary report – quarterly.	Internal audit of risk management framework. Audit Scotland external audit Annual Report covers risk management.	Agreed internal audit report and agreed actions. Agreed annual report sections on risk.	No gaps identified.
19. Cyber Security and Information Management	IT Operations and Controls: - Security procedures - Secure device configuration - Intrusion detection and penetration testing - Secure network configuration - Inventory information (assets, devices, software) - Least-privilege access - Vulnerability management - Change control - Cyber-security education and awareness programme IT management team meetings which cover cyber security. Corporate Development Team meetings which cover information management. Information Governance Group (IGG) meeting cover information security matters.	Agreed IT meeting minutes and actions. Agreed CD Team meeting minutes and actions. IGG action plan and agreed minutes and action from the IGG meetings. Risk register updates. Documented policies and procedures. Audit logs. SOC reports. Configuration change records. Vulnerability scanning reports. Reports on completion of mandatory training.	Audit and Risk Assurance Committee meetings + 'deep dives' to discuss cyber security and information management. RMAG meetings which monitor and mitigate risks relating to cyber security and information management. Security policies. Cyber threat intelligence. Business continuity and disaster recovery planning. Third-party supplier and service provider management. HEFESTIS CISO Share.	Agreed report and minutes of Audit and Risk assurance Committee. Risk register updates. Risk mitigation action plans. Threat intelligence reports. BC/DR plans. BC/DR test results. Audit reports on BC/DR compliance. Third-party risk assessments. Third-party audit reports or certificates (e.g. ISO27001, Cyber Essentials)	Internal audit of cyber security. Cyber Essentials Plus assessment process. JISC audit of data protection. Internal audit of data protection. Penetration testing	Agreed internal audit report and actions. Audit evidence. Cyber Essentials Plus assessment reports, remediation plans, and certificates. JISC audit reports. Data Protection Impact Assessments.	No Known gaps identified

20. Business Continuity and Critical Incident Management -non cyber security and information management	BCM Framework developed by Corporate Development. Business Impact Assessments (BIA) process coordinated by Corporate Development. BCM planning process with SMT members based on BIA risk analysis. Development of the Critical Incident Management (CIM) Policy.	Agreed BCM Framework. Agreed BIA templates. Agreed BCM Plans. Critical Incident Management policy. Learning and remedial actions emanating from the testing of the CIM policy and BCM Plans.	Audit and Risk Assurance Committee meetings to discuss BCM Framework, BIAs and BCM Plans. Risk Management Assurance Group (RMAG) meeting have a regular schedule of review of BIAs and BCM Plans.	Agreed BCM Framework, reviewed every three years. Agreed RMAG minutes and actions relating to BCM. Agreed actions and minutes from the RMAG.	Internal audit reports relating to business continuity and major incident management.	Agreed internal audit report and actions. Facilitated BCM desk top exercises	No gaps identified.

	Testing of CIM Policy and BCM Plans.						
21. Compliance with codes of good practice (governance)	Regular Board governance meetings between Board Secretary and COO. COO oversight of good governance. Monthly Director of Finance and Estates Infrastructure meetings with COO. Board Secretary meetings with Colleges Board Secretaries Group.	Agreed email actions and reports emanating from COO, Board Secretary and others meetings	Review of compliance with Colleges Code of Good Governance by A&RA Committee (annual). Review of Compliance with Scottish Government Audit and Assurance Committee handbook by A&RA Committee (2018/19). Nominations Committee – board recruitment and committee membership Induction including CDN training. Annual self-evaluation of Board and Committees, and Board Development plan	Agreed reports and minutes from committees and Board. Agreed governance report to the Board. Executive Team agreed minutes on governance matters.	Regular Internal Audits. External audit – Audit Scotland annual report. External Independent Effectiveness Review – required by SFC	External Auditor's Report in the Annual Accounts. External Review of the Board. Agreed internal audit report and actions. Agreed Board review report submitted to the SFC.	No gaps identified.
22. Partnership Working and Engagement with key Stakeholders (including Community Planning Partnership work).	Monthly cross college External Engagement Group meetings. Weekly meetings of communications, marketing and engagement managers to coordinate activity. Weekly cross college events coordination meeting.	Agreed action note from the External Engagement Group. Updated list of events at the college from the weekly events coordination group Agreed SMT reports and minutes on CPP and other partnership activity.	Corporate Development Committee meetings (quarterly) where CPP activity is discussed. Corporate Development Committee meetings (quarterly) where communications, marketing and engagement activity is assessed.	Agreed Corporate Development Committee reports and minutes.	Internal audit report on partnership activity. Audit Scotland best value reviews of CPP arrangements by CPP area.	Agreed internal audit report and actions. Published Audit Scotland best value audit reports on CPPs.	No gaps identified.

	Quarterly meetings of each CPP Team to review CPP activity and actions. Reporting to SMT on CPP and other partnership and engagement activity. Industry and Business Engagement working group meetings.	Agreed actions from the Industry and Business Engagement Working Group.					

AUDIT & RISK ASSURANCE COMMITTEE
2 OCTOBER 2024
PAPER H

Title	**Risk Management Update**
Appendices	Appendix 1: Top level Risk Register Infographic August 2024 Appendix 2: Top Level Risk Register August 2024 Appendix 3: Risk Management Policy and Procedure
Disclosable under FOISA	Yes ☒ / No ☐
Primary Contact	Alan Williamson, Chief Operating Officer
Date of Production	21.08.24
Action Required	For Approval ☒ / For Discussion ☒ / For Information ☒
Aligned to Strategic Risk	Yes ☐ / No ☒ *(If 'yes' please complete Section 5.3)*

1. RECOMMENDATIONS

1.1. For Approval

The Risk Management Policy and Procedure has undergone its annual review which involved key managers and the senior management team to ensure accuracy and relevance. Following this comprehensive assessment, the policy and procedure is now ready for committee approval.

- Appendix 3: Risk Management Policy and Procedure

1.2. For information

The Audit & Risk Assurance Committee is asked to note the changes to the top-level risk register agreed at the recent Risk Management and Assurance Group (RMAG).

- Appendix 1: Top level Risk Register Infographic August 2024.
- Appendix 2: Top Level Risk Register August 2024.

2. PURPOSE OF REPORT

This paper provides an update on matters relating to risk management and business continuity at the College.

3. DETAIL

At its most recent meeting on 20th August, the RMAG discussed the following:

Equality, Diversity, and Inclusion (EDI) Risk Management Considerations

The group discussed the integration of Equality, Diversity, and Inclusion (EDI) legal obligations into Edinburgh College's overall risk management strategy and approach, emphasising the importance of full compliance and proactive risk mitigation.

Following a thorough conversation, it was agreed to embed EDI considerations and associated compliance requirements, within the Risk Management Policy and Procedure. Additionally, this EDI document will be included as a reference resource for all future RMAG meetings and discussion points, with a prompt to be used when considering all college risks.

Top Risk Register
The RMAG agreed that the current top risks for the college are:

- (1) National bargaining impact on college operations
- (33) Financial sustainability (insufficient budget / funding to cover cost of living, job evaluation, employer pension contribution increases)
- (24) Cyber security breaches within the college

The RMAG agreed to increase the residual probability for risk (32) – "Failure to meet SFC funded activity targets and fees (recruitment, credits, SAAS and fee income", elevating the residual risk to Amber due to current uncertainty around enrolment numbers at the beginning of an academic year. The group will undertake a credits' review and forecast when the FT enrolment period closes.

In contrast, the RMAG agreed to reduce the probability score for risk (25) – "Fineable breach of GDPR or PECR" due to the robust internal controls in place and no violations to date since the introduction of GDPR in 2016.

Note: GDPR – General Data Protection Regulations 2016
PECR - Privacy and Electronic Communication Regulations 2003

Similarly, the RMAG agreed to reduce the probability score for risk (15) – "Health & safety non-compliance" due to the absence of any instances of health and safety non-compliance situations or major incident reports.

Operational risk registers
Human Resources and Organisational Development – The Director advised the RMAG that the department's top risks and mitigations include:

Top risk **Relationships with local trade unions breaking down**
Mitigations*:* The College mitigates the risk of union relationship breakdowns through preventative and remedial measures. These include maintaining a strong Relationship and Partnership Agreement (RPA), incorporating Avoidance of Dispute procedures, and holding regular meetings with trade unions.

HR also conducts case management meetings to ensure consistent risk management and fosters partnership working with unions. A solution-focused and collaborative approach are embedded in employee relations and Local Negotiating Committee (LNC) meetings to address any challenges and to maintain positive relationships.

2nd risk **Failure to implement changes in employment and case law**
Mitigations: The HR team regularly attends employment law update sessions, listens to podcasts, and stays informed via legal communication. They also discuss relevant changes in team meetings and update policies and procedures as required.

Remedial support includes ongoing advice from the College's legal advisors. Additionally, the sector's HR Strategic Group network is used as required to ensure compliance, and effective implementation of legal updates.

3rd risk **Failure to provide conduct pre-employment checks for new staff**

Mitigations: The college undertakes pre-employment checks and complies with the Recruitment & Selection Policy, as well as offering manager training, and keeping HR staff informed and updated on legal provisions such as PVG checks. The college also ensures that new staff undergo induction training and uses a recruitment process map, and risk assessments if a PVG is delayed.

HR follows up with managers and staff on any matters arising. Additionally, a checklist is used to ensure all recruitment steps are correctly completed.

Quality and Improvement – The Assistant Principal advised the RMAG that the department's top risks and mitigations include:

Top risk **Overdue resulting of qualification outcomes resulting in risk to student progression (internal and external), potential malpractice and reputational damage**

Mitigations*:* Preventative actions include clear instructions to Curriculum Team Managers (CTMs) and course teams for timely resulting, swift action on missing results, and consultation with unions to mitigate the effects of potential industrial action should this situation arise.

Remedial measures include performance management by Heads of School and actions such as deeming pay where staff fail to complete assessments/resulting due to strike action. Additionally, a collaborative approach among support teams and key staff ensures emergency actions are taken as required.

2nd risk **A high number of student withdrawals resulting in poor KPIs, overpayment of awarding body fees, and reputational damage**

Mitigations: Preventative actions include robust monitoring of attendance registers to identify disengagement early in the process, and using curriculum progress monitoring tools to inform withdrawal policies.

Remedially, improved monitoring across all course levels helps guide interventions to prevent in-year withdrawals. Additionally, the Senior Management Team collaborates to create focused short-term action plans when necessary to address emerging issues.

3rd risk **Failure to deliver digital services for learning and teaching (Moodle)**

Mitigations: Preventative actions include developing in-house expertise within the Learning Technology and Business Solutions Development teams, collaborating with Edinburgh Napier University (the host), documenting work processes, and maintaining a detailed Business Continuity Management (BCM) plan.

Remedially, issues are addressed according to contractual agreements, with IT support available for network-related problems and a well-established communication plan for staff and students. Additionally, departmental monitoring ensures performance issues are identified and resolved proactively.

4. IMPACT AND IMPLICATIONS

The development and management of the College's Risk Management Policy & Procedure and Business Continuity Management Framework improves the College's capacity to:

- Identify, mitigate, and monitor college risks and possible major disruptions.
- Develop business continuity and recovery plans for major disruptions.
- Devise action plans to minimise high level adverse risk situations.
- Identify the colleges risk tolerance and risk appetite for each strategic aim.
- Improve academic and support services to deliver an excellent student experience.
- Address specific financial shortfalls to safeguard future financial sustainability.
- Invest in the workforce through an impactful people strategy.
- Maintain good College governance and oversight.

5. ALIGNMENT TO STRATEGIC PLAN / KPIs / RISK REGISTER

5.1 Alignment to Edinburgh College Strategic Pillars *[Indicate with an 'X' which Strategic Pillar this paper supports]*:

Curriculum Strategy	☒	Finance Strategy	☒	People Strategy	☒
Commercial Strategy	☒	Digital Strategy	☒	Other	☐

5.2 Relevant Key Performance Indictors *[Indicate with an 'X' which performance indicators this paper supports]*:

Student Success	☒	Credit Target	☒	Equality, Diversity & Inclusion	☒
Student Satisfaction	☒	Adjusted Operating Position (AOP)	☒	Staff Costs	☒
Student Retention	☒	Non-SFC Income	☒	Staff Engagement	☒
Student Enrolments	☒	Gross Carbon Footprint	☒	Partner Engagement	☒

5.3 Alignment to the Top-Level Risk Register *[Strategic risk information should be copied directly from the most recent TLRR]*:

Strategic Risk(s)	**Risk Score***		
Not Applicable.	Inherent (Gross) Risk		
	Probability	*Impact*	*Score*
	-	-	-
	Residual (Net) Risk		
	Probability	*Impact*	*Score*
	-	-	-
	Movement (since last review)		-

**Risk Score Key: 0-10 Low Risk; 11-15 Moderate Risk; 16-25 High Risk. [Further information on risk scoring can be found in the EC Risk Management Policy & Procedure]*

APPENDIX 1

Edinburgh College

Top Level Risk Register Aug 2024

Overview - The following have been identified as the top strategic risks of Edinburgh College for the reporting period as of August 2024. The colour status applied to each listed risk is based on the residual (Net) score applied within the top risk register maintained by the College.

RED Score

- ↔ (1) National bargaining impact on college operations
- ↔ (33) Financial Sustainability (Insufficient budget / funding to cover cost of living, job evaluation, employer pension contribution increases)
- ↔ (24) Cyber security breaches within the college

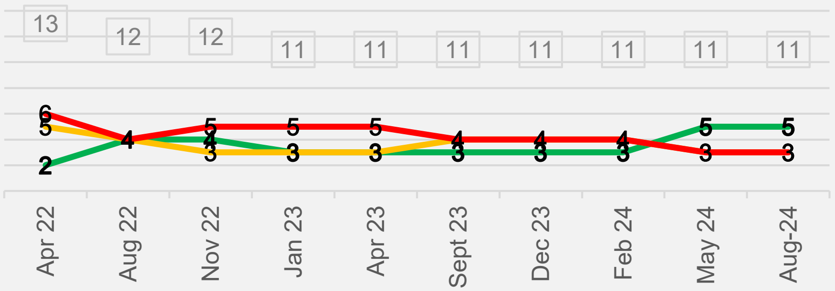
AMBER Score

- ↔ (2) Student retention and attainment
- ↑ (32) Failure to meet SFC funded activity targets and fees (recruitment, credit, SAAS and fee income)
- ↔ (28) College estate infrastructure not aligned to meet business need

GREEN Score

- ↔ (35) Public health risk
- ↔ (3) College does not support or invest in commercial opportunities that contribute to financial sustainability
- ↓ (25) Finable breach of the GDPR or PECR
- ↔ (27) Workforce planning and development
- ↓ (15) Health & safety non-compliance

Risk Movement



RAG Key

- ↔ *No score movement from last reporting period*
- ↑ *Residual (Net) score increase from last reporting period. Colour of arrow denotes the risks previous RAG score*
- ↓ *Residual (Net) score decrease from last reporting period. Colour of arrow denotes the risks previous RAG score*
- ▪ *New Risk*
- ↨ *Combination of previously separate risks within the top risk register*

For the future you want

APPENDIX 2

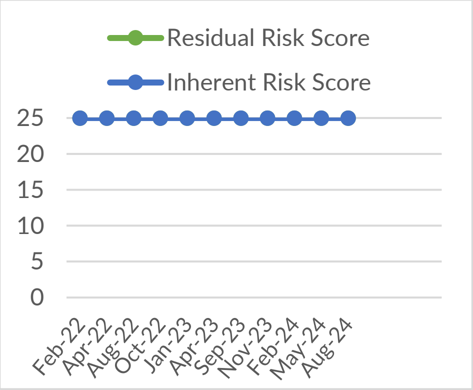
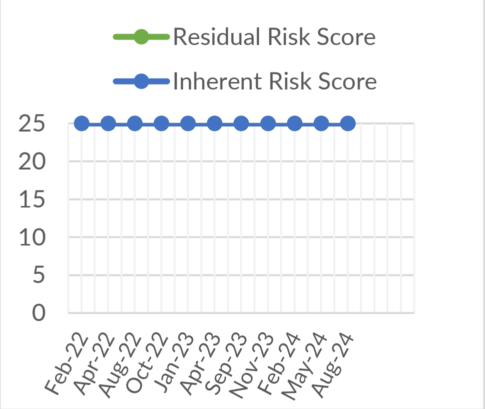
Edinburgh college top level strategic risk register for reporting period up to August 2024

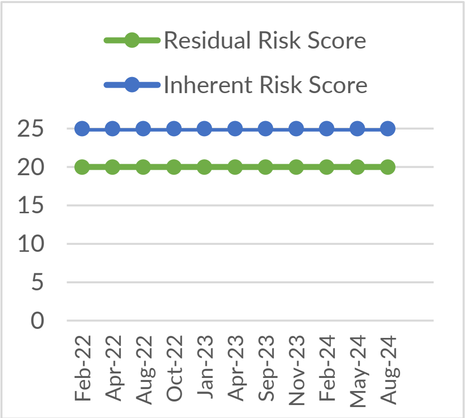
LEAD: Chief Operating Officer

DEPUTY: Vacant

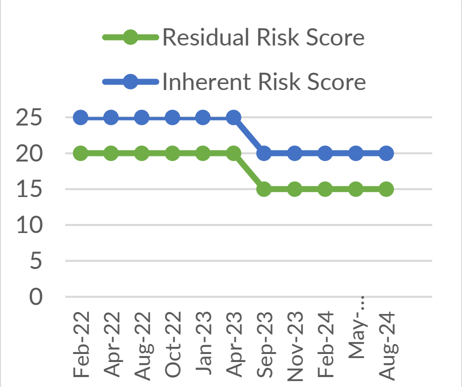
RAG Key	Description
16 – 25 High Risk	**At Risk or Late – Not Under Management Control – Action Required** **When Red**, significant concerns over the adequacy/effectiveness of the controls in place and assurances obtained in proportion to the risks
11 – 15 Moderate Risk	**At Risk or Late – Under Management Control** **When Amber**, some areas of concern over the adequacy/effectiveness of the controls in place and assurances obtained in proportion to the risks
0 – 10 Low Risk	**On Target and Under Management Control** **When Green**, controls and assurances are adequate/effective in proportion to the risks
Blank	Insufficient information at present to judge the adequacy/effectiveness of the controls and assurances

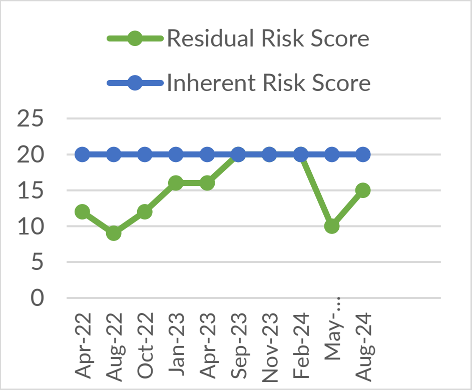
Risk appetite summary	Adverse – Low	Cautious – Medium	Open – Medium-High	Eager – High
Cyber & Information	**Cyber-attack / GDPR** - There are no positive outcomes from a cyber or GDPR event. No deliberate breach of compliance is acceptable.		**IT / Technology** - Innovation and growth necessarily will bring new technological and information risks. We will seek technological advancement to become a high-performing digital organisation.	**IT Technology**
Regulatory & Compliance	**Regulatory breach** - No deliberate significant breach of compliance is acceptable.		**Policy change** - Some risk taking is necessary with the potential for legal or regulatory challenge. We accept the potential for regulatory challenge where we can justify it.	
Finance		**Financial management** - It is necessary to take some considered risk to innovate and tackle the financial challenges ahead.	**Commercial opportunities** - Our financial approach needs to adapt to accommodate different funding models and the need to take new commercial opportunities which may be more within our control and will support our aspirations for innovation and growth.	
Reputation			**Managing consequences** - Limited / controlled publicity cannot be avoided where we want to grow and innovate.	**Taking opportunities** - We will actively promote innovations and be prepared to justify them externally if necessary.
Workforce	**Workforce wellbeing** - We want to avoid any adverse impact on workforce wellbeing.	**Workforce development** - Some risk is acceptable to innovate and develop skills and capacity.		
Quality Service	**Student outcomes** - We do not seek to take risks that could adversely impact student outcomes		**Curriculum** - We acknowledge there may need to be short term impact to achieve longer term rewards, such as curriculum changes.	
Commerciality				**Realising potential** - Investment and innovation are key to growing alternative income streams.

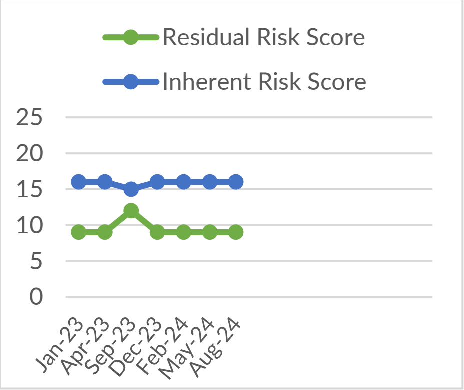
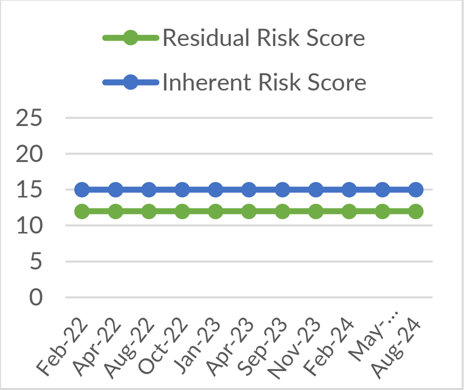
RISK DETAILS	RISK SCORING & TRACKING	RISK MITIGATIONS & CONTROLS	RISK MONITORING & ASSURANCE	CONTINGENCY IF RISK MITIGATIONS & CONTROLS FAIL	CHANGE LOG - FROM PREVIOUS REPORTING PERIOD
(1) National bargaining impact on college operations **Management Lead:** Director of HR&OD **Lead Committee:** Planning and Resources Committee **Strategic Pillar:** People	**Inherent (Gross) Risk** *Probability* 5 / *Impact* 5 / *Score* 25 **Residual (Net) Risk** *Probability* 5 / *Impact* 5 / *Score* 25 **Movement** ⟺ 	**Preventative (Probability):** • Senior staff work (Principal, COO, HRD, VP's) present on national work and bargaining groups to influence future direction • EIS-FELA members advised that taking ASOS is a breach of contract and pay can be deducted **Remedial (Impact):** • HR regularly review national circulars and determines national impact on college **Both:** • Strong partnership working between management and unions	**1st line of defence:** • Senior staff present on national work and bargaining groups to influence future direction • Regular internal HR/Executive discussions to review national initiatives and determine college actions • HR work with managers and SMT leads to discuss impact in their areas • General discussions with Finance regarding financial impacts • Monthly meetings between COO and HRD • Advising EIS-FELA members of the potential impact on them of taking ASOS • Faculties and Quality Dept planning to minimise impact of any ASOS on students **2nd line of defence:** • Policy and Resources Committee discussions and reports • Audit and Risk Assurance Committee review of top-level risk register – which includes industrial relations risk • Executive Team and SMT meetings + reports – industrial relations matters **3rd line of defence:** • Local Negotiation Committees – COO chairs LNC with Unison and Vice Principal with EIS (HRD attends both) - National issues are discussed with a view to determine college actions	• Focused management and oversight of situation by Executive, and senior management teams	Three year pay deal has been tabled but not accepted. Cuts to sector funding put further pressure on the affordability of pay increases
(33) Financial sustainability (insufficient budget / funding to cover cost of living, job evaluation, employer pension contribution increases) **Management Lead:** Director of Finance & Estates Infrastructure Director of HR&OD **Lead Committee:**	**Inherent (Gross) Risk** *Probability* 5 / *Impact* 5 / *Score* 25 **Residual (Net) Risk** *Probability* 5 / *Impact* 5 / *Score* 25 **Movement** ⟺ 	**Preventative (Probability):** • Active engagement at national level via Principal, COO and HRD. • Develop a more unified response with other colleges through HR and Finance networks. • Improved involvement with the NJNC via HRD • Increase volume of lobbying with MSP's to promote needs of college. • Financial Forecasting and sensitivity analysis in place taking account of additional financial requirements and cost savings. • Together with other affected public sector organisations engage with bodies setting SPPA and LPF employer pension rates. • Better workforce planning to ensure that staffing costs are contained, Led by COO and SMT. **Remedial (Impact):** • 6% contribution (Middle Managers 3%) to Job Evaluation awarded from the SFC.	**1st line of defence:** • Ensure EC has the latest information available on future pension rate movements (review all published information). • Annual budget setting with each AP/Director, included in operational plans. • Monthly management accounts meetings with each AP/Director • Monthly meetings between COO and Director of Finance & Estates Infrastructure • Annual assurance statements including financial control, references. • Maintaining up to date financial regulations as well as policies and procedures. • Annual Accounts scrutinised by the Executive Team. • Regular Cash flow forecast prepared and reviewed • SFC Cash flows prepared, reviewed, and sent monthly. • Regular joint reviews by Directors of HR&OD & Finance & Estate Infrastructure of budget aligned to establishment.	• Seek further income from external revenue streams. • Impose a moratorium on expenditure. • Reduction in staff costs through restriction on filling vacancies. • National lobby on ability to create further revenue for the college.	

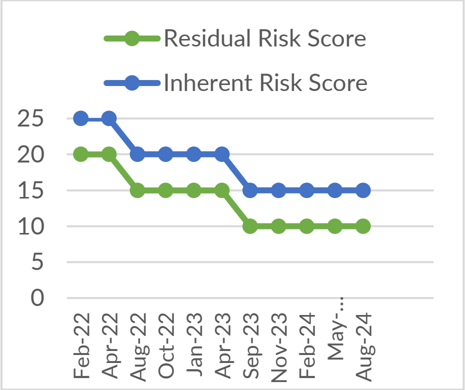
RISK DETAILS	RISK SCORING & TRACKING	RISK MITIGATIONS & CONTROLS	RISK MONITORING & ASSURANCE	CONTINGENCY IF RISK MITIGATIONS & CONTROLS FAIL	CHANGE LOG - FROM PREVIOUS REPORTING PERIOD
Planning and Resources Committee **Strategic Pillar:** Finance		- SFC funding of increases in employer lecturer pension costs. - Planning for a continued lack of SG direct funding for cost-of-living increases. - SFC approved business case to remove up to £7.2m of staffing costs through to 2025/26. Initial VS scheme delivered in June '24 to deliver £1.4m of recurring savings with further schemes planned for 2024/25. Purpose to achieve balanced budget. - Ensure all costs associated with reduced income are removed where possible. - Recruitment freezes remain an option in 2024/25 and beyond. - SMT driving continued efforts to reduce recurring costs (through regular meetings with dept heads to review operational costs) and maximise commercial income. Director of Finance and Estates and Director of Commercial Development established FAIM project (Futureproofing Alternative Income Management) to drive this. **Both:** - Total impact fully disclosed to BoM. - Cost of Living increases at an estimate of Public Sector Pay Policy. No agreement with Lecturer Unions for 2022/23 to 2025/26, negotiation will be ongoing until agreed. - Working with national employer's association to request additional Grant funding.	- SMT meeting regularly. **2nd line of defence:** - Senior Management and Executive Team reviews of financial controls, cash management, management accounts and performance. - Quarterly reports to Planning and Resources Committee and the Board. - Budget and 5-year forecast process and papers to committees and board. - Finance Report (including management accounts) reviewed by P&R Committee & Board. - Regional Procurement Strategy approved by P&R Committee annually. **3rd line of defence:** - Full impact disclosed to BoM. - External Audit of finance including cash flow & management, payroll & expenses, purchasing & creditors and procurement as well as annual internal audit of EMA, bursaries and other student support funds. - Annual Accounts signed off by External auditors and laid before the Scottish Parliament.		
(24) Cyber security breaches within the college **Management Lead:** Chief Operating Officer Digital Infrastructure Service Lead **Lead Committee:** Planning and Resources Committee **Strategic Pillar:** Digital	**Inherent (Gross) Risk** *Probability* 5 · *Impact* 5 · *Score* 25 **Residual (Net) Risk** *Probability* 4 · *Impact* 5 · *Score* 20 **Movement** ⟺ 	**Preventative (Probability)** __Technical__ - Secure configurations of college systems. - Software restrictions on endpoints to limit application usage. - Regular vulnerability management and penetration testing. - Tight control over privileged accounts. - Patch management and strict data access control measures. - Robust boundary intrusion detection defences such as firewalls, network inspection, and event monitoring. - Office 365 Multi-factor Authentication for staff. - Email/phishing defence - SPF, DKIM, DMARC, Barracuda Email Gateway Defence, Impersonation Protection, and Incident Response.	**1st line of defence:** - IT management team - regular meetings focusing on cybersecurity and internal controls, discussing preventative and remedial actions in detail. - Information Governance Group meetings to establish and manage data/information risk. - Policies and procedures – development and regular review of comprehensive policies and procedures to guide staff and manage risks effectively. **2nd line of defence:** - Audit and Risk Assurance Committee meetings - these meetings, including in-depth 'deep dive' sessions, are vital for discussing audit reports and compliance issues related to cyber-security and information management, and audit and compliance reports. - RMAG meetings monitor and mitigate risks relating to cyber security and information management	- Use of overtime budgets for out of hours cover, ensuring continuous efforts in incident management. - Data/information insurance in place to provide financial support to cover the costs associated with data loss and recovery from any incidents. - Escalation to SMT and Executive Team to approve budget for incident containment (e.g., external expertise). - Cyber Security Attack Business Continuity Management plans. - Security Operations Centre assistance. The SOC will play a crucial role in containing and managing an incident, providing	**Mobile Device Management (MDM)** Software used by the IT department to monitor, manage, and secure employee mobile devices is under review for modernisation related to Cyber Essentials Plus requirements. **DLP and Insider Risk Pilot Underway** In tandem with a Microsoft partner and designed to help the college effectively identify, protect, and govern sensitive data that resides on our Microsoft 365 platform.

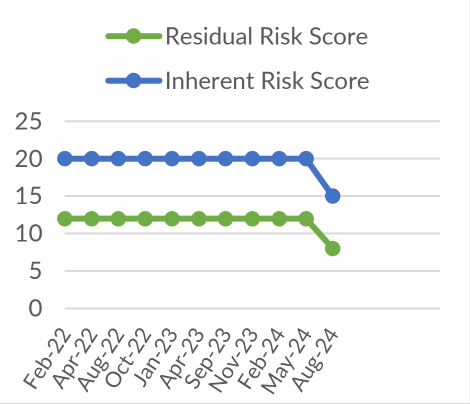
RISK DETAILS	RISK SCORING & TRACKING	RISK MITIGATIONS & CONTROLS	RISK MONITORING & ASSURANCE	CONTINGENCY IF RISK MITIGATIONS & CONTROLS FAIL	CHANGE LOG - FROM PREVIOUS REPORTING PERIOD
		• Secure Remote Access VPN system with endpoint protection and vulnerability management. • Backup solutions on-premises and in Office 365 to secure data from loss. • Wireless security controls including authentication and network segmentation. **Organisational** • Information Governance programme - Information Manager and Data Protection Officer posts, supported by the Information Governance Group. • Engagement with UCSS CISOShare and participation in CiSP/SCiNET. • Development of data breach response testing and business continuity plans. • Relevant policies, procedures and guidance on information security and procurement. **Behavioural** • Staff awareness training and vigilance. • Encouragement for staff to report cybersecurity issues. **Remedial (Impact)** • Incident response planning • Data recovery systems and procedures. **Both** • 24/7 Managed Detection and Response (MDR) service. • Business Continuity Management (BCM) programme with procedures and alternative processes for maintaining critical operations during an incident. • Annual and targeted penetration testing.	through regular meetings and closing-off any actions arising. **3rd line of defence:** • Audit - regular audits conducted by external and internal parties to provide an unbiased assessment of the cybersecurity measures and their effectiveness. • Internal audits on data protection. • Accreditation – alignment with and assessment against known standards such as Cyber Essentials and the CIS Security Controls. • HEFESTIS CISOShare and Data Protection Officer shared services. These services provide expert support and guidance, ensuring continuous improvement and adaptation to evolving cyber threats and data protection regulations.	real-time analysis and rapid response to mitigate the impact.	
(2) Student retention and attainment **Management Lead:** VP Innovation Planning & Performance VP Education & Skills **Lead Committee:** Planning and Resources Committee	**Inherent (Gross) Risk** *Probability* *Impact* *Score* 4 5 20 **Residual (Net) Risk** *Probability* *Impact* *Score* 3 5 15 **Movement** ⟺	**Preventative (Probability):** • Education Scotland annual engagement visit (AEV) in Jan/Feb 2024 provided positive feedback - all actions in plan have been completed, including Thematic focus on services to support learning for retention • Curriculum management structure has 50+ staff in management roles. A greater focus on the quality of learning and teaching (HGIOLT reviews across the year) help lead to improvements in both retention and attainment • MIS email staff proactively around student with cause for attendance concerns (targeting support before course starts) • Tracking and monitoring in place, and working towards a consistent format	**1st line of defence:** • CTM and HOS meetings • Assessment board meetings • LDTs attend course teams meeting • Weekly AP meeting • Education Scotland reports discussed at SMT meetings • AP led HGIOLT reviews between HOS, CTM, CL, (in addition 2 x per year to reviews with HOF and CM) using operational plan targets • Quality team meetings with CM's and CL's • Team meetings focused on self-evaluation using student feedback • Annual ongoing curriculum review	• Education Scotland action plan when required	Risk is closely linked with strike action. Strikes disrupt the academic schedule, leading to missed classes and lost instructional time, negatively impacting student engagement and learning outcomes. Prolonged or frequent strikes create an unstable learning environment, causing disengagement and higher dropout rates. Risk score to be closely monitored in tandem with strike actions within college.

RISK DETAILS	RISK SCORING & TRACKING	RISK MITIGATIONS & CONTROLS	RISK MONITORING & ASSURANCE	CONTINGENCY IF RISK MITIGATIONS & CONTROLS FAIL	CHANGE LOG - FROM PREVIOUS REPORTING PERIOD
Strategic Pillar: Curriculum		• Curriculum planning tool in use (Curriculum review) • Review of curriculum and business planning cycle • Use of business intelligence (SFC/SDS/Marketing data) to plan and track recruitment • Improved course information and pre-course guidance • Continued use of application window Continued training and joint working of curriculum and student support teams • Collegiate student focus / retention friendly timetabling • Ensuring all funding in place before start dates • Positive behaviour and anti-bullying and harassment policy and procedure in place • Counselling and wellbeing support in place (inc free sanitary products across all campuses) • Student communications to inform and build engaged student community • Career Coach in place and upgraded to latest version • Course remediation process in place for courses with low KPIs to ensure course is still relevant to continue • Attendance and retention policy in use • Online withdrawals form replaced old paper-based withdrawals, which allows a more streamlined (monitored) process and more accurate withdrawal data within college • ROA and BOM targets outlined in Operational plans • New automation of pathways for progressing students (don't have to go through application process again) • Close working between CTM's and SRA's (student right course) • Monitoring and tracking shared with Schools for SCP. Internal group supports younger students in partnership with local authority and SDS. • LEAN project completed to further refine application process . Head to Ed review of recruitment ongoing **Remedial (Impact):** NA **Both:** • MIS control processes in place – more stringent control around marking of registers with staff and manager alerts	• Fortnightly Edinburgh College Student Association (ECSA) meeting with Assistance Principal of Quality and Improvement • Use of student satisfaction data **2nd line of defence:** • Regular reporting to Executive Team and Senior Management Team • Reporting regularly on AEV progress to the LTSE committee • Deep Dives led by Audit and Risk Assurance Committee • ROA reporting to the Board of Management • Performance against ROA targets report to LTSE Committee • Student destination survey reports to LTSE Committee • Edinburgh College Student Association reporting of student satisfaction to LTSE Committee and Board of Management **3rd line of defence:** • Annual framework audit • ROA reporting to the SFC • Annual internal Further Education Statistics audit (also reported to Audit and Risk Assurance Committee) and Further Education Statistics submission to Scottish Funding Council • Close partnership with external partners and industry		

RISK DETAILS	RISK SCORING & TRACKING	RISK MITIGATIONS & CONTROLS	RISK MONITORING & ASSURANCE	CONTINGENCY IF RISK MITIGATIONS & CONTROLS FAIL	CHANGE LOG - FROM PREVIOUS REPORTING PERIOD
		• Retention working group established and focused on specific areas e.g., full time FE containing national recognised qualifications			
(32) Failure to meet SFC funded activity targets and fees **(Recruitment, credits, Student Award Agency Scotland (SAAS) and fee income)** **Management Lead:** VP Education & Skills VP Innovation Planning & Performance **Lead Committee:** Planning and Resources Committee **Strategic Pillar:** Curriculum	**Inherent (Gross) Risk** *Probability* | *Impact* | *Score* 4 | 5 | 20 **Residual (Net) Risk** *Probability* | *Impact* | *Score* 3 | 5 | 15 **Movement** ⇧ 	**Preventative (Probability):** • Performance Monitoring cycle – encapsulating ROA targets • Active engagement at national level via Principal and Chair • Develop a more unified response with other colleges using College Scotland • Increase volume of lobbying with MSPs to promote needs of college. • Maintaining up to date financial regulations as well as policies and procedures. • Ongoing monitoring of application system • Full college recruitment and enrolment consultation complete and summary to be provided for final recommendations – Sept 2023 **Remedial (Impact):** • More detailed budgeting and reporting now in place to align staff and overhead budgets to prioritised services • Monthly focus on cost control with regular, clear communications with all staff on financial position seeking support in reconciling adverse position • Financial systems, processes and procedures updated in areas where SFC guidance has had an effect, eg, budgeting and forecasting • Reconciliation of SFC guidance changes and allocation letters with monthly SFC Returns and Cash Flow Forecasts • Wider acceptance of financial targets across the SMT, to ensure focus remains on achieving financial targets including alternative income streams if targets not forecast to be achieved • Further guidance from SFC has provided more flexibility around the allocation of credits **Both:** • Analysis of PT courses that lead to break-even/negative funding for the college • Closer working between Finance/HR /Procurement and Department Heads including training sessions and regular meetings • New self-evaluation procedures launched in 2023, performance against attainment data as key ROA measure and supports staff to	**1st line of defence:** • AP, VP, CTM and HOS (invited) conduct regular reviews to monitor targets • Faculty Operational Plans include ROA and credit targets. • Monthly meetings between COO and Director of Finance. • Annual assurance statements including financial control, references. • Regular meetings with regional outcome agreement manager • Regular meetings with Education Scotland **2nd line of defence:** • MIS quality checks on credit delivery. • VP Education and Skills meetings with all Heads of Faculty to review ROA + credit delivery. • Faculty Operational Plan performance meetings. • VP Education and Skills reports to Planning and Resources Committee on credit delivery • ROA and SFC target reporting presented to SMT and LTSE Committee • Tri-partite engagement with SFC/Education Scotland • Monitoring by Education Scotland of progress against actions agreed **3rd line of defence:** • Annual internal Further Education Statistics (FES) audit (also reported to Audit and Risk Assurance Committee) and FES submission to SFC. • Scottish Government CPA self-evaluation process.	• Monitor effect of activity on funding and assess exposure • Action planning and remedial quality assurance and enhancement to include Review of all MIS data and credit activity	Have not recruited enough full-time students and semester 2 applications are lower than hope for SFC removing flexibility for COVID recovery and the number of credits that can be claimed (reduced target by 10%, however likely to not reach number of students in new year required to meet this)

RISK DETAILS	RISK SCORING & TRACKING	RISK MITIGATIONS & CONTROLS	RISK MONITORING & ASSURANCE	CONTINGENCY IF RISK MITIGATIONS & CONTROLS FAIL	CHANGE LOG - FROM PREVIOUS REPORTING PERIOD
		consider planning at operational level to improve this Marketing targeted to demographics highlighted in ROA			
(35) Public health risks **Management Lead:** H&S Manager **Lead Committee:** Corporate Development Committee / Planning & Resources Committee **Strategic Pillar:** People	**Inherent (Gross) Risk** *Probability* | *Impact* | *Score* 4 | 4 | 16 **Residual (Net) Risk** *Probability* | *Impact* | *Score* 3 | 3 | 9 **Movement** ⟺  	**Preventative (Probability):** • Health and safety along with public health colleagues will continue to monitor risk: meningitis, COVID-19, flu, Noro virus, etc • Occupational health nurse working closely with Edinburgh College Student Association (ECSA) and HR on public health campaigns • Hand hygiene, CO^2 monitoring and ventilation procedures in place **Remedial (Impact):** • Alternative working arrangements in place for staff when required • Blended learning default position for classes when required • College and Edinburgh College Student Association (ECSA) maintain engagement with students via various digital and social media platforms and to provide information about keeping well and safe. **Both:** Staff communications to provide updates on situation and risk levels – Staff update email, intranet, website, etc	**1st line of defence:** • Risk Management and Assurance Group monitor risk and overall college response actions • Critical Incident Team to manage major events **2nd line of defence:** • Health and Safety committee • Regular Public health team briefs • SMT fortnightly meetings **3rd line of defence:** • Scottish Government • Health Protection Scotland • Internal and external audits • Trade union feedback	• Business Continuity Management plans and procedures/guidance for communicable diseases • Full campus closure – all activity on-line • College has regular contact with public health to manage any potential outbreak in student population	
(28) College estate infrastructure not aligned to meet business need **Management Lead:** Estates Managers **Lead Committee:** Planning and Resources Committee **Strategic Pillar:** Curriculum People	**Inherent (Gross) Risk** *Probability* | *Impact* | *Score* 3 | 5 | 15 **Residual (Net) Risk** *Probability* | *Impact* | *Score* 3 | 4 | 12 **Movement** ⟺  	**Preventative (Probability):** • Planned maintenance programme in place for statutory compliance • Curriculum review to take account of Estates requirements and lack of funding to make significant changes • Future planning for Motor Vehicle facilities at Sighthill/Midlothian; and Construction facilities to replace Forthside • Major project underway for relocations of all Forthside facilities to college campuses. **Remedial (Impact):** • In-house maintenance team carry out reactive maintenance where possible. Register in place to monitor works and log what works are not completed and prioritised • Loss of catering provision to staff and students with long lead time if retender required **Both:**	**1st line of defence:** • Critical works register in place to monitor outstanding works and monthly maintenance register to monitor works progress against budget availability • KPI's in operational plans for Estates • Staff roles designed to manage Estate's compliance • Estate's strategy and capital funding allocation prioritised and agreed by the SMT • Estate's condition reviewed six monthly + monthly review of estates critical works register • Estates Services Manager's and H&S Manager meet weekly with Dir. of Finance and Estates Infrastructure, H&S + Sustainability + Facilities + Security + Porterage + Print Services + Vehicles + IFM + Catering Contract + Budget issues discussed ISS contract management meetings • Gather & Gather monthly contract meetings for catering contract with Finance and Procurement • Monthly utility monitoring **2nd line of defence:**	• Align decisions on future curriculum to enable estates to review requirements and plan for necessary changes as part of the connect groups • Estate's incident management process and business continuity plans • G&G contract now reduced to minimal service •	

RISK DETAILS	RISK SCORING & TRACKING	RISK MITIGATIONS & CONTROLS	RISK MONITORING & ASSURANCE	CONTINGENCY IF RISK MITIGATIONS & CONTROLS FAIL	CHANGE LOG - FROM PREVIOUS REPORTING PERIOD
		Business Transformation Plan Estates Review completed – focus on Forthside construction and Sighthill Automotive. Flexible approach being taken to reconfiguring classrooms where budget permits	• SMT + Executive Team discussions on estates. • Planning and Resources Committee papers and discussions on estates matters. • Estates management matters are also included also in the Health and Safety Report to Health and Safety Committee. **3rd line of defence:** • NQA Auditor process. • Internal audit on estates management. Care Inspectorate inspections of the nursery.		
(3) College does not support or invest in commercial opportunities that contribute to financial sustainability **Management Lead:** VP Corporate Development Director of Enterprise and Knowledge Exchange **Lead Committee:** Corporate Development Committee / Planning & Resources Committee **Strategic Pillar:** Commercial	**Inherent (Gross) Risk** *Probability* | *Impact* | *Score* 3 | 5 | 15 **Residual (Net) Risk** *Probability* | *Impact* | *Score* 2 | 5 | 10 **Movement** | ⟺  	**Preventative (Probability):** • Robust costing tools, operational plan and strategy in place to achieve income targets • Robust programme monitoring and management systems in place • New programmes in development/research phase to anticipate and meet market demand and generate income • Enhanced utilisation of business intelligence and sector networks to identify new opportunities • Communication and Marketing teams provide support to commercial team to promote services and partnerships for further income generation • Joint ownership of target setting with Commercial Development, Finance and APs Curriculum in regular dialogue • Better monthly forecast procedures incorporated which allow for higher degree of proactiveness **Remedial (Impact):** • FWDF – The College's ability to plan financially is not helped by the lack of information on funding and in-year allocation. The Flexible Workforce Development Fund (FWDF) Year 7 allocation has yet to be announced. The later the announcement, the greater the likelihood of negative impact in terms of workload and pressure on the team. **Both:** • Partnerships with business, colleges and universities strengthened to build sustainable income platforms • Diversified income streams to minimise reliance on any single source • Flexible delivery model to ensure capacity (use of both in-house and external training associates)	**1st line of defence:** • Commercial income targets set annually as part of budget setting process • Enhanced financial reporting to provide clarity and support planning • Monthly reporting to Exec and SMT • 6 weekly monitoring process to be put in place in line with updated reporting structure • Quarterly reporting to Corporate Development Committee and BoM. **2nd line of defence:** • Monthly updates to Executive Team on live programmes and activities under development • Corporate Development Committee oversight of international contracts **3rd line of defence:** • Internal audit report on commercial activity. • Scottish Government Procurement Capability Assessment self-evaluation process.	• Longer term forecast and targeted approach to setting commercial focus • External training associate's costs used to partly service commercial activities • Actions to reduce costs associated with any reductions in Commercial Income • Alternative funding streams being pursued • Scottish Funding Council review will impact on planning and budgeting for alternative funding activities.	• Programme for Scottish Government funding has come in form of credits not revenue therefore will not assist with commercial income • There seems to be some doubt cast on the guarantee of continued Flexible Workforce Development Fund (FWDF) funding, this will become clearer as budget confirmed. • Updated reporting structures in progress to capture all income for transparent monitoring. Risk name updated from "Shortfall in commercial income"

RISK DETAILS	RISK SCORING & TRACKING	RISK MITIGATIONS & CONTROLS	RISK MONITORING & ASSURANCE	CONTINGENCY IF RISK MITIGATIONS & CONTROLS FAIL	CHANGE LOG - FROM PREVIOUS REPORTING PERIOD
		- Costing review project, with scheduled and bespoke programmes to be reviewed in semester 1 23/24 - 23-26 Commercial Strategy now signed off. - College Engagement Plan in place, including employer engagement			
(25) Fineable breach of the General Data Protection Regulation (GDPR) or Privacy and Electronic Communications Regulations (PECR) **Management Lead:** VP of Corporate Development Information Manager **Lead Committee:** Planning and Resources Committee **Strategic Pillar:** People	**Inherent (Gross) Risk** *Probability* | *Impact* | *Score* 3 | 5 | 15 **Residual (Net) Risk** *Probability* | *Impact* | *Score* 2 | 4 | 8 **Movement** ⇩  	**Preventative (Probability):** - Data Protection Handbook published college-wide February 2021 containing guidance on data sharing, verifying ID, secure send via email, & referral of legal data protection requests to DP Team. - EC laptop encryption complete on all known devices. - Data Protection Policy co-designed with DPO; published on internet, intranet and embedded in mandatory staff data protection training. - Mandatory staff GDPR training on Moodle Staff zone - 'Tech Tuesdays' Cyber Security training now in place (training provided by Barracuda). - Full information asset audit completed January 2020 – SMT assigned ownership of EC Info Assets & providing security classifications Nov 2020 onwards. - DPO delivered data protection impact assessment training to middle managers (via OD) three times – now a mandatory training session. - Dedicated data protection inbox created for staff - single point of reporting/email address for data protection issues. - All BDO GDPR audit actions closed October 2021. - College has embedded GDPR-standard student privacy notices; and PECR-standard direct marketing consents, within application & enrolment process. - College has deployed employee, and job applicant, privacy notices on college website privacy page. - Data capture on website is compliant - Participation within FE GDPR collaborative group Scottish Colleges' Information Governance Group (SCIGG) to share college sector approaches to GDPR compliance - College website cookie permissions updated to GDPR and E-Privacy Regulation compliant standard	**1st line of defence:** - Dedicated Information Management manager in post to monitor compliance - Information Governance Group established: DPO and Chief Information Security Officer (CISO) are members. - OD monthly reports to managers on GDPR training uptake - Co-Sharing of common documentation by Scottish College through the Scottish Colleges' Information Governance Group (SCIGG) **2nd line of defence:** - Data Protection Officer in post via HE/FE Shared Technology & Information Services (HEFESTIS) Shared Service: reviewing and actively contributing to college GDPR work and provides independent internal audit and advisory role - GDPR update to SMT on by-request basis **3rd line of defence:** - Internal audit on GDPR compliance (BDO)	- Breach escalation to Director of Communication Policy and Research for assessment and determination of further escalation to Executive team for strategic level oversight	RMAG agreed that as no occurrence of GDPR violation the probability score can be reduced. Mandatory staff GDPR training on Moodle Staff zone (86% as of 30 April 2024).

<table>
<tr><th>RISK DETAILS</th><th>RISK SCORING & TRACKING</th><th>RISK MITIGATIONS
& CONTROLS</th><th>RISK MONITORING
& ASSURANCE</th><th>CONTINGENCY IF
RISK MITIGATIONS &
CONTROLS FAIL</th><th>CHANGE LOG - FROM PREVIOUS
REPORTING PERIOD</th></tr>
<tr><td></td><td></td><td>• Updated staff contracts issued August 2018 containing DPO-approved GDPR/data protection clauses.
• Contracted/part-time workers provided statutory compliance information booklet, which includes key data protection instructions/guidance

<b>Remedial (Impact):</b>
• Single point of reporting/email address for data protection and data breach issues: weekend out-of-hours breach reporting cover provided by security operations centre.
• Data Protection Officer support available out of hours via HE/FE Shared Technology & Information Services (HEFESTIS) shared Data Protection Officer (DPO) service

<b>Both:</b>
• Integrated Action Plan encompassing outstanding data protection, information security and records management compliance requirements developed and being monitored by EC Information Governance Group (IGG).
• Data Sharing Agreements being developed with key external partners to reduce likelihood of breach and to reduce fines in event of breach involving 3rd parties
• Formal Data Breach Reporting Procedure approved by SMT and issued to staff via College Update/available on college website privacy page.</td><td></td><td></td><td></td></tr>
<tr><td><b>(27) Workforce planning and development</b>

<b>Management Lead:</b>
Director of HR&OD

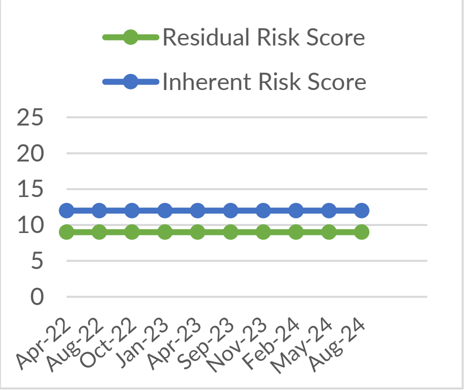
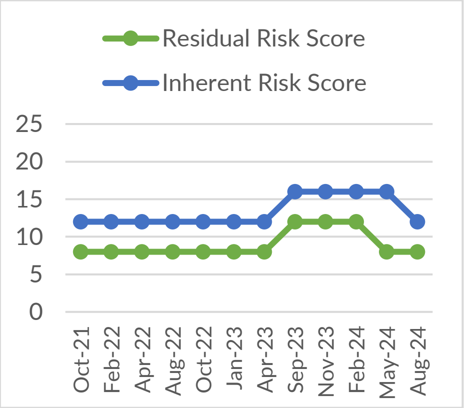
<b>Lead Committee:</b>
Planning and Resources Committee

<b>Strategic Pillar:</b>
People</td><td><table>
<tr><th colspan="3">Inherent (Gross) Risk</th></tr>
<tr><td><i>Probability</i></td><td><i>Impact</i></td><td><i>Score</i></td></tr>
<tr><td>3</td><td>4</td><td>12</td></tr>
<tr><th colspan="3">Residual (Net) Risk</th></tr>
<tr><td><i>Probability</i></td><td><i>Impact</i></td><td><i>Score</i></td></tr>
<tr><td>3</td><td>3</td><td>9</td></tr>
<tr><td colspan="2"><b>Movement</b></td><td>⟺</td></tr>
</table></td><td><b>Preventative (Probability):</b>
• Revised workforce plan for 2025-2028 being developed
• Monthly meetings with managers by HR Partners to review key employee management information including retirements, vacancies, turnover, absence (16)
• Monthly meeting between HR Manager Partnering and AP's/Directors to review staffing issues and needs

<b>Remedial (Impact):</b>

<b>Both:</b>
• Greater scrutiny of vacancy control and staff deployment has been implemented
• Robust process and procedures in place to track vacancies against budget</td><td><b>1st line of defence:</b>
• Staff analytics monthly reports to CTM's and Support Managers
• Management of establishment against budget
• Regular reviews of progress against operational plan objectives for OD team with Director of HR&OD.
• Monthly meeting between HR Partners and managers (curriculum and support staff) to review establishment vacancy, workforce planning, staff wellbeing and OD
• Joint LNC meetings to develop employment policies

<b>2nd line of defence:</b>
• Regular reviews with progress and issues in HR & OD between COO and Directory of HR&OD.
• SMT and Executive Team discussions and reports on workforce planning, OD, and staff wellbeing.</td><td>• Consider development of policy on retraining displaced staff rather than recruiting new staff
• Consider alternative employment models where feasible – ongoing</td><td>WF Plan updated to take account of £3.6m-£5.7m savings to be made currently under review by COO and Exec as part of EC People launch.
Draft people strategy launched in line with new College Strategic Aims and launch of EC People campaign
Further review of costs and vacancy reduction underway
Longer term workforce planning starting in key support areas</td></tr>
</table>

RISK DETAILS	RISK SCORING & TRACKING	RISK MITIGATIONS & CONTROLS	RISK MONITORING & ASSURANCE	CONTINGENCY IF RISK MITIGATIONS & CONTROLS FAIL	CHANGE LOG - FROM PREVIOUS REPORTING PERIOD
			- HR reports to Planning and Resources Committee and SMT on workforce planning. **3rd line of defence:** Internal audit: Workforce & Establishment Management was carried out in 2022 and some actions for improvement were noted.		
(15) Health & safety non-compliance **Management Lead:** Chief Operating Officer H&S Manager **Lead Committee:** Planning and Resources Committee **Strategic Pillar:** People	**Inherent (Gross) Risk** *Probability* *Impact* *Score* 3 4 12 **Residual (Net) Risk** *Probability* *Impact* *Score* 2 4 8 **Movement** ⇩ 	**Preventative (Probability):** - Corporate policies and procedures in place. - Document control tracker maintained - Mandatory training requirements in place for all staff - Communications support to ensure staff understand compliance responsibilities - H&S documentation to be implemented and maintained by Faculty/Function heads or nominated managers **Remedial (Impact):** - Early detection of risk/s and resolve quickly and efficiently. **Both:**	**1st line of defence:** - Reactive date (e.g., accident/incident reports) monitored to identify and correct procedural deficiencies - Operational planning - Annual review of H&S policy; maximum review timeframe for procedures is 3 years - All new or significantly altered policies and procedures sent for consultation (H&S Committee, management, relevant staff) and all feedback recorded - H&S Committee in place with engagement of staff and unions **2nd line of defence:** - Ongoing monitoring of budget availability to carry out reactive work with H&S implications and reporting to SMT/Executive **3rd line of defence:** Programme of internal and external audits in place	- Enforcement of H&S management systems and procedures for area/department. - Immediate implementation of any required local or organisation-wide deviation from procedure as short-term control - Formal review and consultation on need for procedural change/update. - Dependent on outcome, implement corrective actions	RMAG agreed that as no occurrence of non-compliance the risk probability score can be reduced.

APPENDIX 3

Edinburgh College

Corporate Ref.	CD 011
Level	Three
Senior Responsible Officer	Director of Communications, Policy & Research
Version	4
EIA	
Approved by	
Approved date	
Superseded version	3
Review date	

Risk Management

Policy & Procedure

Version Control

Version	Author	Date	Changes
4	COO	05/09/2024	Changed to new formatting and narrative updated.

1. INTRODUCTION

This policy and procedure outline Edinburgh College's approach to risk management, including the evaluation of internal controls and corporate governance arrangements. The College recognises that effective risk identification and management are essential for protecting our people (staff, students, and visitors), safeguarding our resources, and preserving our reputation. By understanding and mitigating risks, the College is better equipped to make informed decisions, respond swiftly and effectively to challenges, and capitalise on emerging opportunities.

2. PURPOSE

The purpose of this policy is to articulate Edinburgh College's objectives and strategy for risk management and to describe the specific arrangements in place to manage risks effectively. Rather than aiming to eliminate risk entirely, this Policy and Procedure seek to ensure that risks are managed in alignment with the College's risk appetite. It also clarifies roles and responsibilities related to risk management and establishes the processes for reporting and monitoring risk within the College.

3. RISK MANAGEMENT STATEMENT

The Edinburgh College Risk Management Policy and Procedure applies to all College business activities, at all levels within the organisation.

What is Risk and Risk Management?

Edinburgh College defines risk as an event or cause, that has the potential to result in an uncertain positive or negative outcome. Risk is further defined as the combination of the 'probability' of an event occurring and the 'consequences' of that event.

Risk management identifies and manages the risks that threaten the ability of the College to meet its objectives. Risk management identifies, monitors and aims to eliminate the range of threats to College operations and activities, understand where the College has vulnerabilities, and develop cost effective counter measures. Through risk management the College will minimise exposure to harmful risk whilst taking advantage of risk opportunities, particularly in relation to ethical, social, reputational, compliance, and financial risks.

Approach to Risk

The College maintains two lines of risk management: Strategic and Operational. Edinburgh College’s approach is to appraise and manage risks and opportunities in a systematic, structured, timely manner, and in accordance with the College's Risk Appetite Statement, to ensure that there is clear accountability and responsibility for risk within the College and that risks are managed at the most appropriate level. The College understands that risk is inherent and that encouraging an increased degree of risk taking, (agreeing the level of risk appetite and risk tolerance) in pursuit of its strategic objectives is welcome and necessary.

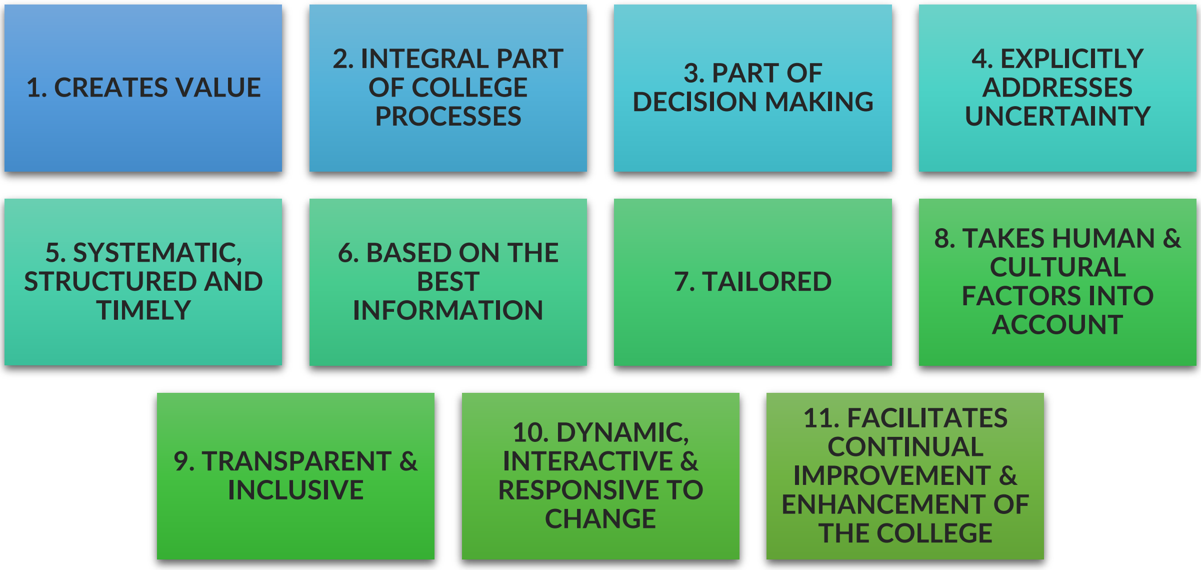
It is also understood that in some cases there is no clear strategic benefit from accepting some risks, e.g. risks associated with illegal, unethical or inappropriate, or dangerous activity. The College therefore recognises that its appetite and tolerance for risk will always vary according to the activity undertaken.

4. RISK MANAGEMENT PRINCIPLES AND CULTURE

Edinburgh College follows ISO 31000 principles of risk management (as shown in Figure 1), which fosters a shared understanding of risks, their nature, and ways to manage them across an organisation; help embed risk management into an organisation’s governance, strategy, planning, reporting processes, policies, values, and culture; lead to efficiency gains, as it helps organisations recognise potential threats and opportunities in time, allocate resources wisely, and enhance stakeholder confidence; equips organizations to anticipate and address risks head-on, turning potential challenges into strategic advantages; and signals to stakeholders that the organization is robustly prepared to navigate uncertainties, reinforcing trust and credibility.

Using these principles Edinburgh College seeks to develop and maintain a strong effect on compliance, organisational performance, and effective risk management.

Figure 1 - Risk Management Principles



1. CREATES VALUE

2. INTEGRAL PART OF COLLEGE PROCESSES

3. PART OF DECISION MAKING

4. EXPLICITLY ADDRESSES UNCERTAINTY

5. SYSTEMATIC, STRUCTURED AND TIMELY

6. BASED ON THE BEST INFORMATION

7. TAILORED

8. TAKES HUMAN & CULTURAL FACTORS INTO ACCOUNT

9. TRANSPARENT & INCLUSIVE

10. DYNAMIC, INTERACTIVE & RESPONSIVE TO CHANGE

11. FACILITATES CONTINUAL IMPROVEMENT & ENHANCEMENT OF THE COLLEGE

5. RISK APPETITE

The College's statement of risk appetite guides the College's approach to the acceptance of risk. The College's current Risk Appetite Statement is included at Appendix 1.

The Risk Appetite Statement has been agreed by Board and gives a guide to staff on the parameters in which the College expects to operate. Committees, decision makers, and risk owners across the College should therefore use the statement as a guide to where they have more freedom to be innovative and where there is an expectation of greater caution.

6. RISK REGISTERS

Risk registers are essential tools for identifying, classifying, and managing risks consistently across the College. They serve to assign ownership for each risk, document existing controls, track the current status of risks, and outline actions being taken to mitigate them.

Risk registers are maintained at both the strategic and operational levels within Edinburgh College:

- **Strategic Risk Register**: This top-level register, known as the College Top Level Risk Register (TLRR), summarises the key risks that impact the institution as a whole. It is the primary document used by the Board and the Audit & Risk Assurance Committee to monitor and manage these overarching risks. The TLRR is reviewed and updated quarterly by the Risk Management and Assurance Group (RMAG) and the Senior Management Team (SMT). It also informs the Risk Management Statement in the College's Financial Statements.
- **Operational Risk Registers:** These registers focus on risks specific to individual departments or faculties within the College. Each operational risk register records detailed information on identified risks, their analysis, and the corresponding risk treatment plans.

Both the strategic and operational risk registers are regularly updated and reviewed by the RMAG, the Audit & Risk Assurance Committee, and the Board to ensure effective oversight and management of risks at all levels of the College.

7. THREE LINES OF DEFENCE (ASSURANCE) FRAMEWORK

Edinburgh College adheres to the 'Three lines of defence' model (https://www.iia.org.uk/policy-and-research/position-papers/the-three-lines-of-defence/) to improve the College's approach to internal control, risk assurance and risk management.

The model aims to provide a comprehensive framework that enables the Governing body to have oversight of the appropriateness of structures and processes, to ensure that they are in place for effective governance. The Governing body is accountable to stakeholders for oversight.

The model framework is shown below:

First Line	Second Line	Third Line
Risk Ownership	Risk Oversight	Risk Assurance
Operational management	**Work closely with first line**	**Independent assurance function**
• Operational management control of organisational risks. • Leads and directs actions (including managing risk) and application of resources to achieve the objectives of the organisation. • Establishes and maintains appropriate structures and processes for the management of operations and risk (including internal control). • Ensures compliance with legal, regulatory, and ethical expectations.	• Risk management and compliance functions, reporting to senior management. • Provides complementary expertise, support, monitoring, and challenge related to the management of risk. • Provides analysis and reports on the adequacy and effectiveness of risk management (including internal control).	• Internal audit to provide risk assurance. • Maintains primary accountability to the governing body and independence from the responsibilities of management. • Communicates independent and objective assurance and advice to management and the governing body on the adequacy and effectiveness of governance and risk management. • Reports impairments to independence and objectivity to the governing body.

8. EDI RISK MANAGEMENT CONSIDERATIONS

The following outlines the key legal risks related to Equality, Diversity, and Inclusion (EDI) within Edinburgh College. It highlights the importance of adhering to relevant legislation to mitigate potential risks and ensure compliance.

PDF

EDI Risk
Management Consi

9. ROLES AND RESPONSIBILITIES

Role of Board of Management

- Provide oversight to ensure that risk is being managed effectively and solutions to risk mitigations are implemented to reduce the impact of significant risks facing the college.
- Ensure that the College's risk management framework, policies, and procedures are robust, effectively implemented, and complied with.
- Define and set the overall College risk appetite, ensuring it aligns with the College's strategic aims, and values. See Risk Appetite Statement.
- Stay informed about the most significant risks facing the College, including emerging risks and their potential impact.
- Monitor and ensure that risks are being managed effectively across the College and within the Board.
- Promote a culture of continuous improvement in risk management practices, encouraging compliance, feedback, and regular updates on risk management.
- Ensure ongoing training and development for staff and Board members on risk management principles and practices.

Role of Executive Team

- The Principal and the Executive Team are responsible for overseeing, implementing, and maintaining the risk management policy approved by the Board of Management, thereby enhancing risk management practices across the College.
- Ensure the effective implementation of the College's Risk Management Policy and Procedure, embedding both into strategic plans and daily operations.
- Translate the Board's defined risk appetite into actionable strategies and decision-making, ensuring alignment with the College's operational objectives.
- Foster and promote a holistic approach to risk management, integrating it into the College's culture and all levels of decision-making.
- Report new significant risks or emerging risks that arise within functional areas of responsibility to the Risk Management and Assurance Group and Board.
- Communicate the cessation of any risks that no longer exist to the Risk Management and Assurance Group and Board.
- Escalate any risks that cannot be managed at the local level to the Risk Management and Assurance Group for further action and support.
- Ensure that there are appropriate levels of risk oversight and awareness throughout the organisation, promoting risk-conscious behaviour among staff and stakeholders.
- Maintain functional control of major risks faced by the college ensuring that risk mitigation measures are effectively implemented and monitored.

- Encourage continuous improvement in risk management practices by supporting ongoing training and development for staff, thus ensuring they are equipped to manage and mitigate risks effectively.

Role of Internal Audit

- Ensuring the effectiveness of organisational and financial control systems, including monitoring performance against quality assurance standards

Role of Audit and Risk Assurance Committee

- Conduct thorough reviews of new major risks and assess the potential for any failures in existing control measures, ensuring prompt identification and appropriate responses to emerging threats.
- Regularly evaluate the ‘probability’ and ‘impact’ scoring of strategic-level risks, ensuring accurate and current assessments that reflect the evolving risk landscape of the College.
- Review the adequacy and effectiveness of internal control systems designed to mitigate risks, ensuring that these systems are robust and aligned with best practices in risk management and assurance.
- Receive reports from the Risk Management and Assurance Group, consider findings, and make informed recommendations to enhance and improve the College's systems of control.
- Provide strategic guidance and advice to the Risk Management and Assurance Group on risk-related matters, helping to shape the College’s overall risk management strategy and policies.
- Ensure that the Board of Management has confidence that risks are being managed effectively within the organisation, and that appropriate solutions to identified risks are in place and functioning as intended.

Role of Risk Management and Assurance Group

- The Risk Management and Assurance Group (RMAG), a sub-committee of the Audit and Risk Assurance Committee, is responsible for assessing the top risks facing the College and developing strategies to manage and mitigate that risk and reporting progress to the Audit and Risk Assurance Committee. The membership of the Group includes:
    - Chief Operating Officer (Chair)
    - Member of the Board of Management
    - Senior Management Team members
    - Portfolio Manager
- Foster a collaborative environment among members to ensure a holistic approach to risk management across the College.
- Review the Top Risks: Conduct comprehensive assessments of the top risks facing the College and develop robust strategies to manage and mitigate these risks, ensuring alignment with the College’s strategic objectives.

- Reporting and Progress Tracking: Report progress on risk management initiatives to the Audit and Risk Assurance Committee, providing regular updates and insights on risk status and mitigation approaches.
- Regularly review and update the Strategic Risk Register, known as the Top-Level Risk Register, and agree the ‘probability’ and ‘impact’ of the top College risks.
- Annually review operational risk registers for all College departments/faculties and teams, ensuring comprehensive risk management practices are in place across the College.
- Oversee the overall coordination of risk management activities within the College, ensuring that risk management training and practices are consistent and effective across all departments.

Role of Senior Management Team

- The Senior Management Team (SMT) has the functional responsibility to manage and mitigate risks within their respective areas, both individually and collectively.

  This includes the development, implementation, and regular review of operational risk registers that detail the top risks in their functional areas.

  Maintain awareness of risks within their areas of responsibility, understand the potential impacts, and actively manage and mitigate these risks. This includes monitoring outcomes against identified risks and ensuring that corrective actions are documented and implemented to minimise future risks.
- Report systematically and promptly to the Executive Team and the Risk Management and Assurance Group (RMAG) any new perceived/emerging risks or failures of existing control measures.
- Provide regular updates to the RMAG on current ‘active’ risks, highlighting the effectiveness of mitigating actions and their impact on risk reduction through relevant operational risk registers.
- Ensure that operational risk registers are kept up to date, accurately reflecting the current risk landscape and mitigation efforts within their areas of responsibility.
- Foster a collaborative approach to risk management, encouraging cross-departmental communication and co-ordination to address and mitigate risks effectively.
- Actively seek opportunities for continuous improvement in risk management practices, incorporating feedback and best practice to enhance the College’s overall risk resilience.

Role of Portfolio Manager

- Ensure that reviews of the risk register(s) are carried out on a regular basis and that the strength of all controls are properly understood and recorded.

- Ensure that the information on the risk register is complete and up to date and that risks are regularly reviewed.
- Ensure all risks have an owner and that the owner clearly understands the risk and how the risk is managed.
- Ensure that the assessment of the inherent/residual risk score is appropriate.
- Complete spot-checks of the risk register to ensure owners fully understand their role/responsibility in managing the risk.
- Continuously seek feedback on best practice and adapt risk management strategies to address emerging risks and changing conditions within the College environment.

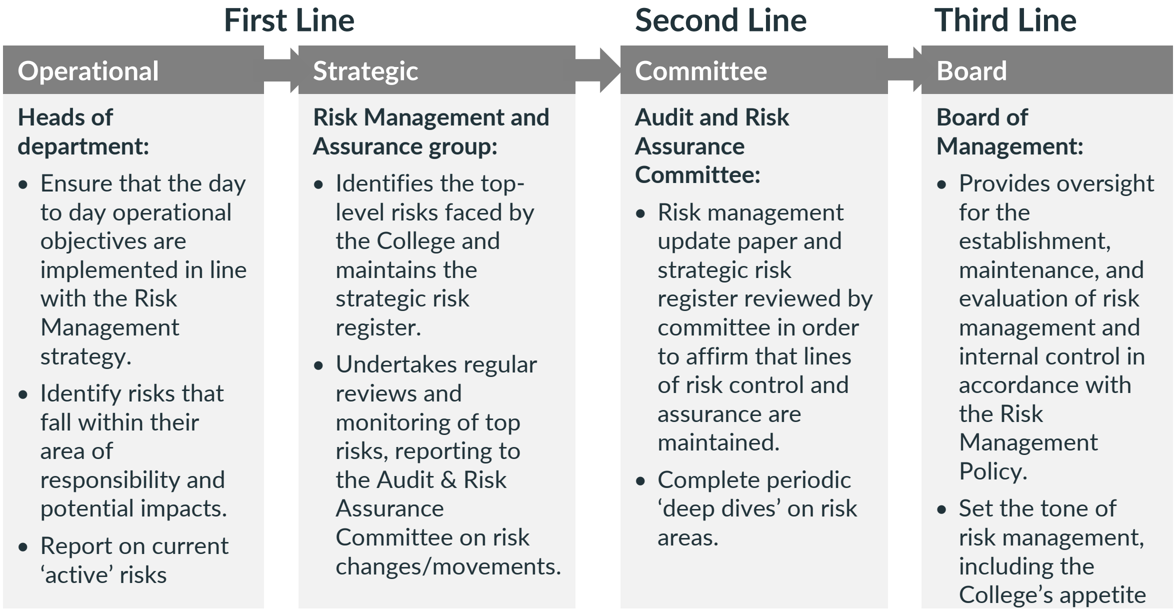
Role of College Staff

- Acknowledge and understand their responsibility for individual risks.
- Understand how they can enable continuous improvement of risk management and risk awareness.
- Report systematically and promptly to a member of the Executive Team or Senior Management Team on any perceived new risks or failures of existing risk control measures

10. RISK REPORTING

Edinburgh College maintains risk registers at strategic and operational levels. These registers record details of the key identified risks plus a risk analysis and associated mitigation plans.

The diagram below shows the risk management reporting route for the 'three lines of defence' model:



First Line

Operational

Heads of department:

- Ensure that the day to day operational objectives are implemented in line with the Risk Management strategy.
- Identify risks that fall within their area of responsibility and potential impacts.
- Report on current 'active' risks

Strategic

Risk Management and Assurance group:

- Identifies the top-level risks faced by the College and maintains the strategic risk register.
- Undertakes regular reviews and monitoring of top risks, reporting to the Audit & Risk Assurance Committee on risk changes/movements.

Second Line

Committee

Audit and Risk Assurance Committee:

- Risk management update paper and strategic risk register reviewed by committee in order to affirm that lines of risk control and assurance are maintained.
- Complete periodic 'deep dives' on risk areas.

Third Line

Board

Board of Management:

- Provides oversight for the establishment, maintenance, and evaluation of risk management and internal control in accordance with the Risk Management Policy.
- Set the tone of risk management, including the College's appetite

highlighting mitigating actions to reduce risk effect. - Maintain operational risk register, and reports to RMAG.	- Conducts regular review of all operational risk registers, providing recommendations accordingly.	- Review adequacy of internal control systems designed to minimise risk. - Provide recommendations which will effectively improve systems of control.	and tolerance for risk. - Understand the most significant risks facing the organisation. - Ensure that risk is being managed effectively and mitigations to risk are in place.
Review frequency: Operational register reviewed once per year and presented to RMAG.	**Review frequency:** Meets 4 times per calendar year.	**Review frequency**: Approximately 4 times per calendar year in line with Board of Management calendar.	**Review frequency**: Meets 4 times per calendar year in line with Board calendar.
Reporting path: To the Risk Management and Assurance Group.	**Reporting path**: To the Audit and Risk Assurance Committee.	**Reporting path**: To the Board of management.	**Reporting path**: To external governing bodies and stakeholders.

11. RISK MANAGEMENT PROCEDURE

The purpose of this document is to ensure that Edinburgh College makes effective use of its risk management procedures to inform decision making across the organisation whilst meeting its statutory duties.

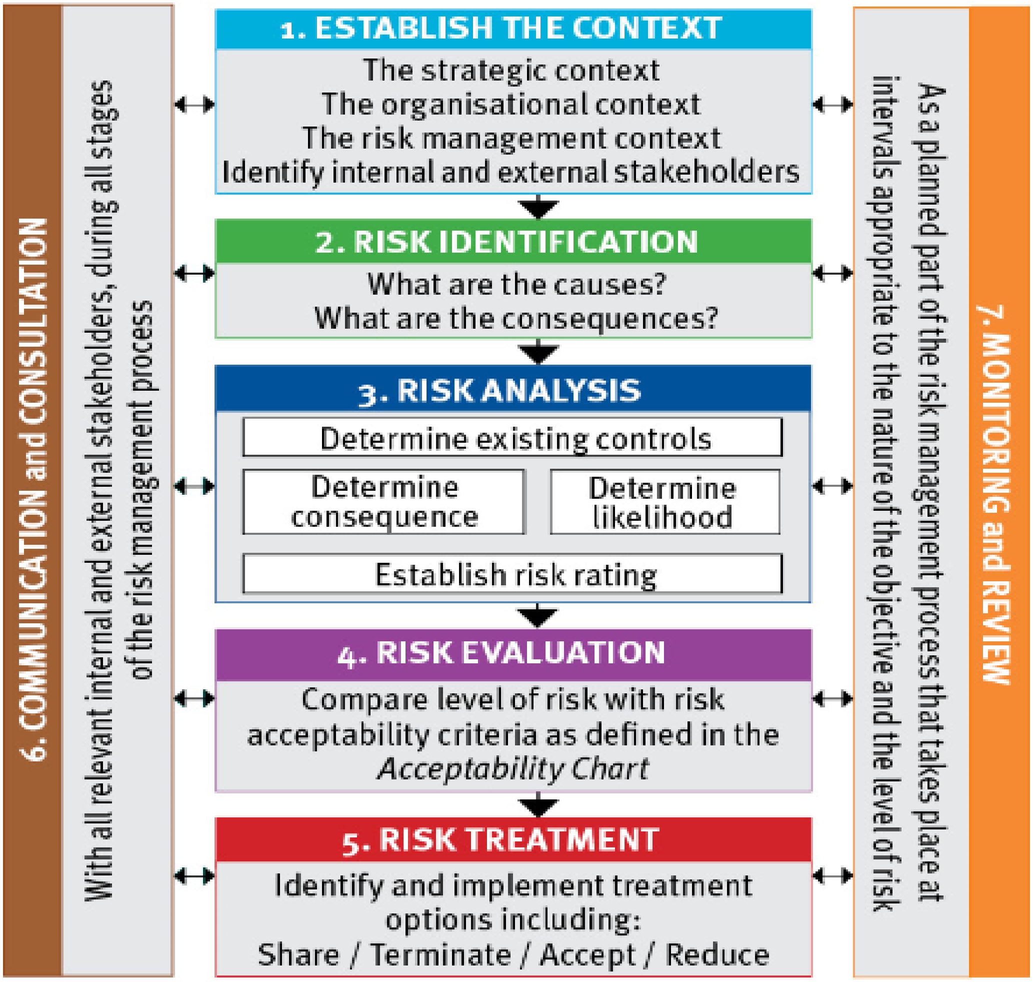
This procedure is to ensure that all staff have a clear understanding of how risk management is applied within the College and that the process of risk management is consistent, appropriate and embedded within the organisation's activities.

Risk Management improves internal control and supports better decision making through a good understanding of individual risks and the overall risk exposure to the service at any given time.

Actively managing risk is important to the continuous development of the organisation, and effective risk management will improve performance against the organisation's strategic objectives.

The steps outlined in this section (refer figure 2) should be followed when updating/developing the relevant Risk Register template document.

Figure 2 - ISO31000: Risk Management Procedure


1. ESTABLISH THE CONTEXT
The strategic context
The organisational context
The risk management context
Identify internal and external stakeholders
2. RISK IDENTIFICATION
What are the causes?
What are the consequences?
3. RISK ANALYSIS
Determine existing controls
Determine consequence
Determine likelihood
Establish risk rating
4. RISK EVALUATION
Compare level of risk with risk acceptability criteria as defined in the *Acceptability Chart*
5. RISK TREATMENT
Identify and implement treatment options including:
Share / Terminate / Accept / Reduce
6. COMMUNICATION and CONSULTATION
With all relevant internal and external stakeholders, during all stages of the risk management process
7. MONITORING and REVIEW
As a planned part of the risk management process that takes place at intervals appropriate to the nature of the objective and the level of risk

- Process based on ISO 31000: 2009
- Risk can be described as anything; event, practice, process, activity, etc. that could hinder or help achievement of stated goals or objectives

STEP 1 – ESTABLISH CONTEXT

Consideration should be given to the environment and activity in which a risk is being assessed, for example, College strategy, departmental objectives and priorities, scope of activity.

If considering organisational or operational risks, consideration should be given to what could adversely impact the day-to-day processes, people or systems currently in place.

If considering project or programme risks, consideration should be given to the potential impact on completing the project/programme to the predefined success criteria (time, cost, and quality).

STEP 2 - RISK IDENTIFICATION

Consider what possible risks there are or could be, including what, when and how something could happen that represents a source of potential risk to the College.
It is important to ensure that any risk assessment is considered objectively and balanced. Making use of existing information that has already being collated, discussing with colleagues, and aligned to any similar risks already being considered.
Below is a list of useful questions to apply when considering risk identification:

- Is there any risk to compliance, statutory, regulatory, policy and/or contractual requirements?
- Is there any risk of potential litigation against the College, its staff, students or stakeholders?
- Is there any risk or danger to staff or students?
- Is loss of service or closure of campus a possibility? Does this require a Business Continuity plan?
- Is there any risk to the reputation of the College?
- Is there a perceived lack of internal control or management oversight of any identified issue that can be improved?
- Are there any objectives that are not being met or won't be met?
- Does the risk pose a financial challenge or risk to the College?

STEP 3 - ANALYSE THE RISK

Existing controls

It is important to consider and document the controls that are currently in place which prevent risks from occurring, or help mitigate (limit) the damage that could occur. There are three types of controls to consider:

- **Physical Controls** – such as equipment (including protective), lifting and handling, visual warning signs and task design reviews.
- **Procedural Controls** – such as policies, procedures, work protocols.
- **Professional Controls** – such as compliance with external regulatory standards, national and local guidelines, quality standards, risk assessments.

Controls are ineffective without the necessary information, instruction, guidance, and training. Therefore, consider the adequacy of any training, equipment, staffing or resources on a regular basis and correct as necessary.
It is also essential to think about any gaps in control – e.g. out of date policies, ineffective policies or absence of procedural documents. The gaps in control should be considered and addressed in the risk register.

Scoring

All identified risks are scored by applying RAG classifications consisting of – high risk (Red), moderate risk (Amber) and low risk (Green).
Risk scoring is documented within each register and is reviewed by the register owner, prior to presentation to the RMG, Audit & Risk Assurance committee, and Board.

The RAG classifications are applied to each risk based on the following:

1. The **PROBABILITY (likelihood)** of the specific risk occurring. If existing control fails, or if planned effective safeguards cannot be applied.
    - [Refer Appendix 2 – Probability Factor Scoring, for further details on how to score risk probability].
2. The **IMPACT (consequence)** if the risk occurs. This is measured in terms of the actual or potential impact, including financial, reputational, health & safety, stakeholder, and/or schedule.
    - [Refer Appendix 3 – Impact Factor Scoring for further details on how to score risk impact].

Probability and Impact are each scored from **1 to 5** and are then multiplied to produce an overall risk score. **Probability x Impact = Risk Score**
Probability and Impact should be regularly monitored and updated to give an accurate appraisal of the risk. The risk matrix below shows the 'RAG' classifications applied based on the risk score:

RAG SCORE KEY	LEVEL OF RESPONSIBILITY
0 – 10 LOW RISK	**On Target and Under Management Control** **When Green**, controls and assurances are adequate/effective in proportion to the risks
11 – 15 MODERATE RISK	**At moderate risk – Under Management Control** **When Amber**, some areas of concern over the adequacy/effectiveness of the controls in place and assurances obtained in proportion to the risks
16 – 25 HIGH RISK	**At high risk– Not Under Management Control – Action Required** **When Red**, significant concerns over the adequacy/effectiveness of the controls in place and assurances obtained in proportion to the risks

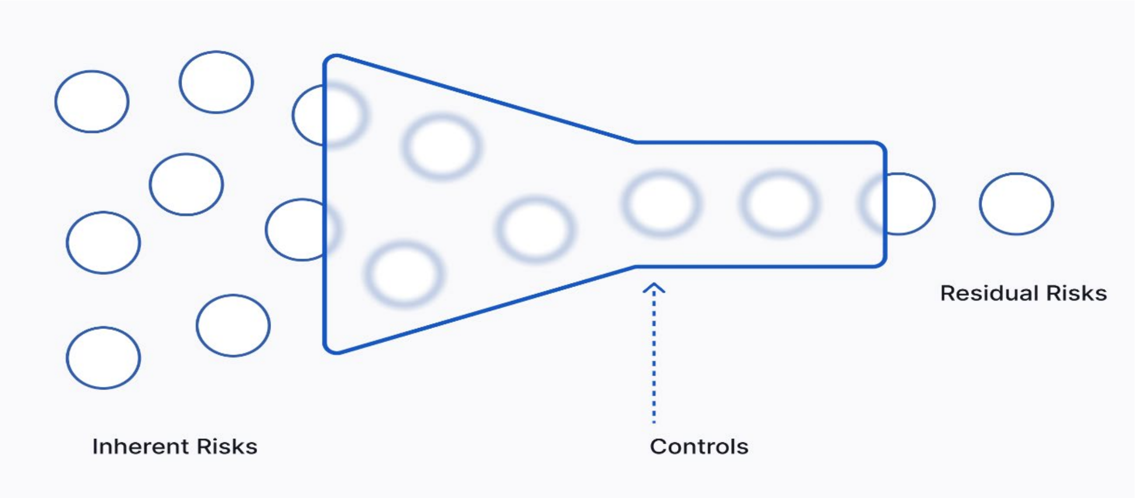
When it comes to risk analysis, there are two types of score assessments for each identified risk.
Inherent risk and residual risk (Refer Figure 3):

1. **Inherent risk** represents the amount of risk that exists in the absence of controls.

2. **Residual risk** is the risk that remains after controls have been accounted for, and are in place.

An overall RAG classification (as shown below) is applied to both inherent and residual risk.

Figure 3 - Inherent risk vs. Residual Risk



STEP 4 - EVALUATION

Risk evaluation attempts to define what the estimated risk actually means to people concerned with or affected by the risk. A large part of this evaluation will be the consideration of how people perceive risks, and the level of oversight that should be applied.

Significance

Risk significance is applied by considering the level of acceptability of the risk:

1. **Acceptable** - The risk does not necessarily require further action or mitigation, as controls in place are sufficient to adequately manage the risk.
2. **Unacceptable** – The risk will require further action to reduce its severity / probability of occurrence to a more acceptable level.

Oversight

The following are the levels of risk oversight required within the College:

1. **Strategic** risks at this level tend to be overarching and will significantly affect most, if not all, of the College and therefore require oversight and continued monitoring by top management levels via the Strategic risk register.

2. **Operational** risks at this level are specific to particular business areas within the College and thus require departmental oversight through an Operational Risk Register. These risks should directly correspond to the department's operational plans, addressing the question: What risks does the College face in achieving the objectives outlined in the operational plan?

When risks are identified and recorded, it is expected that decisions are made by management to determine whether the risk is recorded on the faculty or department operational risk register, or whether the risk affects the whole College and should be escalated to the strategic top-level risk register.

STEP 5 – RISK TREATMENT

Based on the outcome of the risk evaluation (Step 4) the following options should be considered:

- **Share:** if practical, share some of the risk with other teams, partnerships, suppliers or insurers.
- **Terminate:** cease or take steps to cease the activity causing the risk altogether. Proper operational approvals should be obtained via RMAG.
- **Reduce:** the most common treatment, reduce the risk exposure until the risk becomes acceptable, or redundant.
- **Accept:** some risks may be unavoidable in which case future actions should minimise the impact to the College if the risk becomes 'live'.

Each risk must be allocated a risk owner who will be responsible for taking appropriate action to minimise its impact on the College or faculty/department.

STEP 6 – COMMUNICATION AND CONSULTATION

Communication of risk management activities and outcomes across the College is necessary to provide information for decision-making; improving risk management approaches, and identifying emerging threats.

STEP 7 – MONITORING AND REVIEW

Monitoring and review periods should be incorporated in the risk management process, and should take place at intervals appropriate to the objective and level of risk.

Risk deep dive reviews

The Audit and Risk Assurance Committee and Board of Management will systematically conduct deep dive reviews into risk areas they deem appropriate during the year.

Strategic Level Reporting

The top-level risk register is monitored by the RMAG four times per calendar year. A risk management update including the top-level risk register is submitted to the Audit and Risk Assurance Committee and Board for review and comment.

Note: The college also references the Counter Fraud Maturity Model (https://www.gov.scot/publications/counter-fraud-maturity-model/) when incorporating counter fraud controls into strategic level risk monitoring.

Operational level Reporting

Each department Assistant Principal/Director is responsible for reviewing and presenting their operational risk register to the RMAG once per calendar year.

12. APPENDIX 1 – Risk Appetite Statements

Updated June 2024

Risk Approach.

Appetite	Averse – Low	Cautious – Medium	Open – Medium- High	Eager – High
Approach	Actively avoid or minimise risk.	Acceptance of a low element of risk with a limited reward potential.	Willing to take moderate levels of risk.	Willing and able to take higher risks with higher rewards in pursuit of objectives despite greater inherent risk.

Risk Appetite Summary.

	Averse – Low	Cautious – Medium	Open – Medium- High	Eager - High
Cyber & Information Governance	Cyber-attack/ GDPR breach		IT – Technology Improvement	IT - Technology Advancement
Regulatory & Compliance	Regulatory breach		Policy improvement change	
Finance		Financial management	Commercial opportunities	
Reputation			Managing consequences	Taking opportunities
Workforce	Workforce wellbeing	Workforce development		
Quality Service	Student outcomes		Curriculum opportunities	
Commerciality				Realising potential

Definitions.

Risk **appetite** is: “The amount and type of risk an organisation is willing to pursue or retain to achieve its long-term objectives”.

- Risk **tolerance** is: “the boundaries of risk taking outside of which the organisation is not prepared to venture in pursuit of its long-term objectives.”
- An element of risk taking is always necessary in order **to achieve objectives.**
- A risk appetite statement should act as a framework to enable **evidenced** risk-based decision making.

Cyber and Information Governance Risk Appetite Statement.

Relating to the threat of a cyber-attack or loss of data confidentiality through malicious activity.

Edinburgh College recognises the growing threat and increasingly sophisticated nature of cyber-attacks whilst being responsive to a changing landscape to maintain the highest possible cyber controls.

While innovation and growth may bring about new technological risks, there is very little or no appetite for technological innovation, advancement and investment which will knowingly expose the College to increased risk of malicious attack or data breach without appropriate controls in place.

Risk appetite: averse

There are no positive outcomes from a successful cyber-attack or GDPR event. No deliberate breach of compliance is acceptable.

Technological Development

The College has a greater appetite for IT and digital innovation with defined mitigations in place, to achieve our goal of becoming a high performing digital organisation. The Board will work closely with the IT and Learning Technology departments to ensure that all appropriate mitigations are in place, and we are not unnecessarily exposed, and the risk remains as low as possible and managed within our risk appetite.

Risk appetite: open - eager

Innovation and growth necessarily will bring new technological and information risks. We will seek technological advancement to become a high-performing digital organisation.

Regulatory Risk Appetite Statement.

While we recognise that human error and oversights can occur in spite of systems and processes to ensure compliance, we would not be actively seeking to take risks which would expose us to a serious breach of regulatory or statutory duty such as health and safety, information security, safeguarding.

Risk appetite: averse

No deliberate significant breach of compliance is acceptable.

The College is operating in an area of potentially high regulatory and policy change and there may be opportunities to establish ourselves as a key influencer on behalf of Edinburgh and other colleges. We are therefore seeking to develop relationships with policymakers such as the SFC and be in a position to challenge and negotiate for change where we feel it will benefit our outcomes, such as student experience.

Risk appetite: open

Some risk taking is necessary with the potential for legal or regulatory challenge. We accept the potential for regulatory challenge where we can justify it.

Financial Risk Appetite Statement.

It is necessary to take some considered risk in order to innovate and tackle the financial challenges ahead. We need to invest to support our objective of delivering an exceptional student experience. We also need to maintain our estate and continually improve the digital infrastructure.

We are operating in an environment which imposes financial constraints beyond our control. The College is willing to take financial risks if they are well planned, compliant and position the College well for greater capacity in delivering its strategic goals.

A sustainable financial approach needs to adapt to accommodate different funding models and the need to take new commercial opportunities which may be more within our control and will support our aspirations for innovation and growth. Strategic financial decisions will not be taken without considering and communicating operational impacts.

Risk appetite: open

Some risk taking is necessary but should be carefully considered and controlled.

Reputational Risk Appetite Statement.

The College is prepared to take appropriate risk with regard to innovation in order to achieve our strategic goals and we accept that this may incur increased scrutiny and challenge. Our focus is on the longer-term reputation of the College as it aims to deliver its strategy for the future.

We will make and communicate potentially difficult decisions in a carefully considered way and are confident in our ability to robustly defend and explain the rationale behind those decisions, which are made in the interest of long-term outcomes and benefits to our students and other stakeholders.

Risk appetite: open –	eager

Limited / controlled publicity cannot be avoided where we want to grow and innovate. We will actively promote innovations and be prepared to justify them externally if necessary.

Quality Service Risk Appetite Statement.

Student outcomes.
A quality service embraces the entirety of student experience, and the College has a very low risk appetite for making decisions that would adversely impact student outcomes.

Risk appetite: averse

We do not seek to take risks that could adversely impact student outcomes.

Curriculum.
To deliver its strategy, and long-term sustainable outcomes, we are prepared to innovate and make changes to reflect learner and sector needs, which will incur a higher element of risk.

We accept that an element of risk-taking is necessary to achieve long-term goals in terms of delivering curriculum, especially in the context of current financial pressures. Therefore, our curriculum will be reviewed and designed in line with our growth goals and with consideration to employment potential.

Risk appetite: open

We acknowledge there may need to be short term impact in order to achieve longer term rewards, such as curriculum changes.

Workforce Risk Appetite Statement.

Workforce wellbeing.
Our workforce is fundamental to creating an excellent student experience, both in terms of learning and support. The College values its staff and will not seek to deliberately take risk which would adversely impact them.

Risk appetite: averse

We want to avoid any adverse impact on workforce wellbeing.

Workforce development.
The need to innovate, change and adapt to meet long-term strategic goals in the face of financial, governmental and union pressures means that we need to recruit and retain the right skillsets to deliver an excellent and inspiring student experience. We aim to manage this in a way that protects and respects workforce wellbeing and creates a safe workplace culture and a workforce which enables us to deliver our strategy.

Risk appetite: cautious

Some risk is acceptable in order to innovate and develop skills and capacity.

Commerciality Risk Appetite Statement.

The College aims to create a culture and capability that will drive significant revenue growth, aligned to our overall strategic growth aspirations.
We therefore acknowledge that realising commercial potential and maximising opportunities will bring about increased risk exposure, which we are willing to accept, with due consideration of regulatory or ethical consequences.

Risk appetite: eager

Investment and innovation are key to growing alternative income streams.

13. APPENDIX 2 – Probability Factor Scoring

EVENT LIKELIHOOD	% CHANCE OCCURRING	RESULT	ASSIGNED SCORE
Event is expected in most circumstances	>90%	Almost Certain	5
Event will probably occur in most circumstances	51% - 90%	Likely	4
Event should occur at some time	31% - 50%	Possible	3
Event could occur at some time	10% - 30%	Unlikely	2
Event may occur only in exceptional circumstances	<10%	Rare	1

14. APPENDIX 3 – Impact Factor Scoring

ACTIONS	1 INSIGNIFICANT	2 MINOR	3 MODERATE	4 MAJOR	5 CATASTROPHIC
Management Time	Resolution would be achieved during normal day-to-day activity	Resolution would require coordinated input from one or more sections	Resolution would require input from other members of Leadership Team	Resolution would require the mobilisation of a dedicated project team	Resolution would require input from Senior Executive and expert external assistance.
Health & Safety	On-site exposure immediately contained	On-site exposure contained after prolonged effect	On-site exposure contained with outside assistance	***Prolonged/*** Major incident with serious casualties	Major incident with multiple fatalities
Reputation	Letter to local press	Series of articles in local press	Extended negative media/sector media coverage	Short-term negative national media coverage	Extensive and sustained negative national media coverage
Regulatory/ Legal action	Minor breaches by individual member(s) of staff	No fine and no disruption to teaching/ normal business processes	Fine – but no disruption to teaching/ normal business processes	Fine – and disruption to teaching/normal business processes	Extensive fine and significant disruption to teaching. Normal business processes over extended period

Staff (Morale, Recruitment Retention)	No evidence of adverse staff reaction	Staff complaints/ possible comment by union members	General discontent evident across multiple groups of staff	Significant adverse impact, significant concerns to College	Disaster Management Process required. Trade Unions in conflict mode
Management Effort	An event which can be absorbed through normal activity	An event, the consequences of which can be absorbed but management effort required to minimise the impact	A significant event which can be managed under normal circumstances	A critical event which, with proper management, can be endured	A disaster with the potential to lead to the collapse of the business of the College

End of document

AUDIT AND RISK ASSURANCE COMMITTEE
02 OCTOBER 2024
PAPER I

Title	Annual Report on Cyber-Attacks and Data Breach Incidents
Appendices	Appendix 1: Data Breach Reporting Thresholds Appendix 2: Security Operations Centre Reporting
Disclosable under FOISA	Yes ☒ / No ☐
Primary Contact	Mike Jeffrey, Vice Principal: Corporate Development
Date of Production	13/09/2024
Action Required	For Approval ☐ / For Discussion ☒ / For Information ☒
Aligned to Strategic Risk	Yes ☒ / No ☐ *(If 'yes' please complete Section 5.3)*

1. RECOMMENDATIONS

The Audit and Risk Assurance Committee are asked to NOTE and DISCUSS the following annual report on cyber-attacks and personal data breach incidents.

2. PURPOSE OF REPORT

The Audit and Risk Assurance Committee indicated it would welcome an annual report on data breach incident and cyber-attacks to help members understand the source, frequency and whether any specific trends existed. This report is intended to provide information in accordance with ARAC's request.

In line with the rest of the sector, cyber security at Edinburgh College has been improving since the Scottish Government published its Public Sector Action Plan on Cyber Resilience, but there is no room for complacency. Phishing, social engineering and ransomware are still the top concerns, although human error and accidental data breaches by staff are more common.

Separately, under the UK General Data Protection Regulation (GDPR), Edinburgh College has a legal duty to investigate any security incident which may affect the confidentiality, integrity or availability of personal data; evaluate whether a data breach has occurred; and (if of sufficient seriousness) report it to the ICO and the individual(s) affected within 72 hours of discovery. Failure to report a breach when required to do so can result in a fine of up to €10m or 2% of turnover. A significant personal data breach can result in a fine of up to €20m or 4% of turnover.

3. KEY INSIGHTS

The sections below provide an annual overview of cyber-attacks, and data beaches, at Edinburgh College over the past 12 months.

3.1 Cyber-Attacks

The most prevalent security incidents observed in the last period have been:

- **Student devices on college Wi-Fi networks connecting to suspicious domains**—a common issue given the widespread device usage, and

- **Anomalous logon events from staff accounts**, including unfamiliar sign-ins and access attempts from unexpected locations.

While many of the detected incidents were false positives, any genuine security threats identified were localised and contained. Early detection through 24/7 monitoring by the Security Operations Centre (SOC), combined with multi-factor authentication (MFA) protocols, significantly limited attackers' ability to compromise college systems, even when they possessed valid credentials.

Notably, no significant, high-impact external cyber-attacks were recorded during this session. While a few phishing attempts bypassed mail filters, none resulted in account takeovers or system exploitation. This is a strong indication that our ongoing initiatives, such as mail filtering, attack surface reduction, and vulnerability management, are effective in mitigating risks.

Over recent months, there has been a noticeable decrease in the total number of security alerts, yet escalations remain present. This suggests that while incidents may be reducing in volume, the remaining threats are either more severe or require deeper investigation. This indicates a possible trend of increasingly sophisticated or persistent attack methods, but also that we are successfully tuning out the "noise" of low-level tickets in the SOC's workload, potentially improving SOC efficiency and focusing resources on higher-priority incidents.

A lower volume of alerts should not lead to complacency. Recent threat intelligence confirms that attackers need only one opportunity to breach defences, emphasising the importance of continuous monitoring and ongoing improvement in our security measures.

3.2 Personal Data Incidents & Data Breaches

Data Breach Definition
The Information Commissioner's Office (ICO) defines a data breach as:

"A security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is:

- *lost, destroyed, corrupted or disclosed;*
- *if someone accesses the data or passes it on without proper authorisation; or*
- *if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed".*

Under the UK General Data Protection Regulation (GDPR) Edinburgh College has a legal duty to investigate any security incident which may affect the confidentiality, integrity or availability of personal data; evaluate whether a data breach has occurred; and (if of sufficient seriousness) report it to the ICO and the individual(s) affected within 72 hours of discovery.

Edinburgh College's Data Protection Policy; Information Security and Breach policy; mandatory GDPR training module, and employee induction direct staff to the DataProtection@Edinburghcollege.ac.uk inbox and data incident reporting form, for the purposes of reporting data incidents/suspected data breaches.

Incidents and Breaches

Over the period October 2023 to 31st August 2024 (inclusive) the College's Information Management Team (IMT) was notified of, and investigated, 26 data incidents to evaluate whether personal data breaches had occurred (in line with the breach definition provided by the ICO).

The IMT determined that:

- 22 of these incidents technically comprised a data breach; and
- 4 manifestly did not qualify as a data breach.

The college's Data Breach Reporting Procedure sets out a scoring matrix which the IMT uses to consistently evaluate whether or not a confirmed breach is reportable to a). the Information Commissioner's Office b). the individuals affected ("data subjects").

This breach evaluation matrix has been adopted by a number of colleges across Scotland who are members of the Data Protection Officer Shared Service provided by HEFESTIS Ltd.

To date, zero breaches have been determined as reaching the threshold for reporting to the Information Commissioner's Office and similarly no breach has been evaluated as reaching the higher-threshold for reporting to the affected data subject(s). Each decision is recorded on a case- by-case basis on the college's data incident recording tracker.

Edinburgh College's independent Data Protection Officer introduced, in session 2021-22, a new standardised response form providing those reporting breaches with a summary of the incident; containment actions taken; notification recommendation (to ICO and affected individuals); an evaluation of the cause of the incident, and recommended corrective actions.

Table 1: Recorded data breaches at Edinburgh College (by ICO Classification)

Data Breach (ICO Classification)	18 June to Sep 2019	19 Oct to Sep 2020	20 Oct to 9 Sep 2021	21 Oct to 5 Sep 2022	Oct 22 to 29 Sep 2023	Oct 23 to 31 Aug 2024	Annual Change +/-
Data emailed to incorrect recipient (A)	13	12	8	7	11	13	+2
Failure to use bcc (B)	4	6	0	1	1	3	+2
Unauthorised access (C)	3	1	0	0	1	1	No change
Data of wrong data subject shown in client portal (D)	3	2	1	0	0	0	Nil
Other cyber incident (E)	2	0	4	2	0	4	+4
Data posted or faxed to incorrect recipient (F)	2	0	0	0	0	0	Nil

Alteration of personal data (G)	2	0	1	0	1	0	-1
Loss/theft of paperwork or data left in insecure location (H)	1	3	0	0	0	0	Nil
Failure to redact (I)	1	4	4	4	0	0	Nil
Verbal disclosure of personal data	1	0	0	0	0	1	**+1**
TOTAL:	**32**	**31**	**19**	**14**	**14**	**22**	**+8**

Source of breaches & trends
As outlined below, over the period October 2023 to 31st August 2024 the principal source of data breaches at Edinburgh College has been human error. A limited narrative for the main data breaches is provided below.

This aligns with national trends, where ***non*** 'cyber security [cyber-attack]' incidents accounted to 73% of all personal data breaches reported to the Information Commissioner's Office (ICO) over the period 1st January 2024 to 31st March 2024 (latest reported figures).

Incorrect email recipients (13 data breaches)
As outlined in Table 1, 13 (**59%**) of 22 recorded data breaches at Edinburgh College were the result of personal data being emailed to the incorrect recipient when sending emails; by point of comparison this accounted for the greatest number of data breaches reported to the ICO over the period 1st January 2024 to 31st March 2024.

The college has initialised warning messages on all outgoing emails (to external email addresses), reminding senders that their email was being directed outside the organisation; and this message is reinforced in the college's mandatory GDPR training and directly with staff who have committed a data breach of this nature.

Failure to use BCC (3 data breaches)
Three breaches resulted from members of staff using the "TO" field rather than the "BCC" field. On all three occasions, emails were sent to recipients requesting them to delete the original email. Processes have also been put in place to ensure the BCC field is used in future when sending emails to multiple recipients. DPO advised all correct actions were undertaken to contain these incidents.

Unauthorised access (1 data breach)
One breach resulted from a member of staff accidentally sending a message using another member of staff's account (due to member of staff not logging out of pc). IT detected no malicious activity and account password was changed. DPO advised all correct actions were undertaken to contain the incident.

Other cyber incident (4 data breaches)
One breach resulted in the deletion of some staff records due to a software bug in iTrent. College received confirmation that the bug has now been fixed. In addition, all deleted documents were duplicates and no loss of data had occurred. DPO advised the College had undertaken all correct actions to mitigate any ongoing

impact and prevent a future occurrence.

One breach resulted in staff being able to view an email from an Outlook account that was accessible to all members of staff. IT confirmed deletion of the email. DPO advised all correct actions were undertaken to contain the incident.

One breach resulted from a member of staff using AI to analyse personal data. All chats and added/uploaded data were removed from the AI platforms used. Curriculum areas have been advised not to use Open AI products (temporarily) until appropriate guidance is in place. DPO advised all correct actions were undertaken to contain the incident.

One breach resulted from documents being accidentally accessed and deleted from a Public Teams site. The site was changed to private and access limited to invited members. All deleted files were retrieved from the recycle bin and no sensitive information was accessed. DPO advised all correct actions were undertaken to contain the incident.

Verbal disclosure of personal data (1 data breach)
One breach resulted from a member of staff leaving a message for a student on the wrong mobile number. iTrent was updated with correct mobile number and student contacted to explain what had happened. Processes put in place to ensure any further messages left on answer machines would contain no personal data and ask the recipient to call the College. DPO advised all correct actions were undertaken to contain the incident.

4. IMPACT AND IMPLICATIONS

Annual reporting of trends in cyber-attacks and personal data breaches will enable the college's Senior Management Team, and Audit & Risk Assurance Committee, to identify areas of significant risk and respond and resource accordingly. Identification of these trends will enable operational teams, including the IT Digital Infrastructure team and Information Management Team to prioritise activities to mitigate risk, including appropriate staff training.

The occurrence of successful, significant cyber-attack, and/or significant personal data breach - could potentially lead to sanctions (and reputational damage). Potential sanctions under the UK GDPR include:

- A warning in writing in cases of first and non-intentional non-compliance;
- regular periodic data protection audits;
- a fine up to 10,000,000 EUR or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater;
- a fine up to 20,000,000 EUR or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.

5. ALIGNMENT TO STRATEGIC PLAN / KPIs / RISK REGISTER

5.1 Alignment to Edinburgh College Strategic Pillars *[Indicate with an 'X' which Strategic Pillar this paper supports]*:

Curriculum Strategy	☐	Finance Strategy	☐	People Strategy	☐
Commercial Strategy	☐	Digital Strategy	☒	Other	☐

5.2 Relevant Key Performance Indictors *[Indicate with an 'X' which performance indicators this paper supports]*:

Student Success	☐	Credit Target	☐	Equality, Diversity & Inclusion	☐
Student Satisfaction	☐	Adjusted Operating Position (AOP)	☒	Staff Costs	☐
Student Retention	☐	Non-SFC Income	☐	Staff Engagement	☒
Student Enrolments	☐	Gross Carbon Footprint	☐	Partner Engagement	☐

5.3 Alignment to the Top-Level Risk Register *[Strategic risk information should be copied directly from the most recent TLRR]*:

Strategic Risk(s)	**Risk Score***		
(24) Cyber security breaches within the college **Executive Lead:** Chief Operating Officer **Lead Committee:** Planning and Resources Committee	Inherent (Gross) Risk		
	Probability	*Impact*	*Score*
	5	5	25
	Residual (Net) Risk		
	Probability	*Impact*	*Score*
	4	5	20
	Movement (since last review)		⇔
(25) Fineable breach of GDPR or Privacy and Electronic Communications Regulations **Executive Lead:** VP Corporate Development **Lead Committee:** Planning and Resources Committee	Inherent (Gross) Risk		
	Probability	*Impact*	*Score*
	4	5	15
	Residual (Net) Risk		
	Probability	*Impact*	*Score*
	3	4	12
	Movement (since last review)		⇩

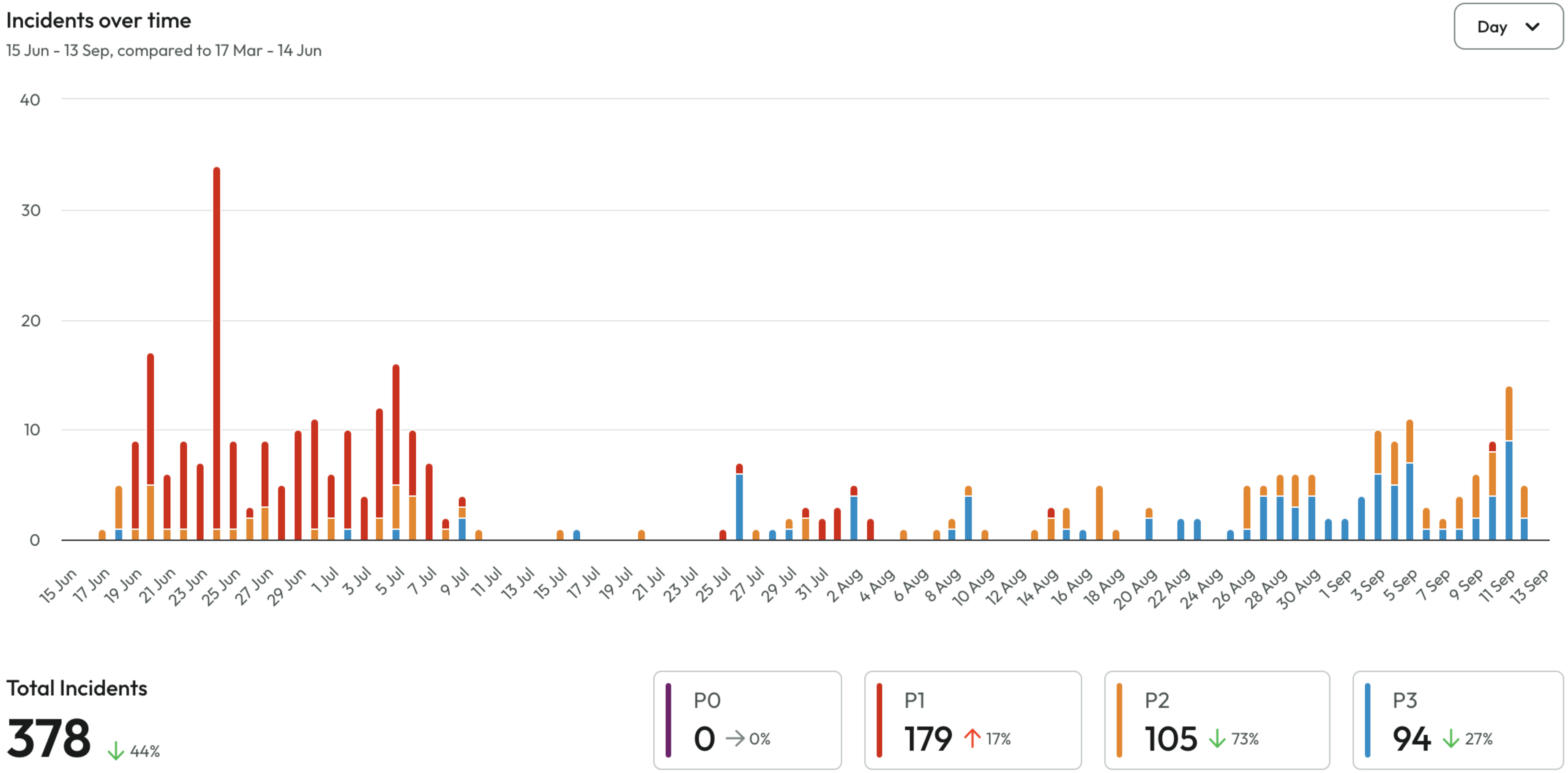
**Risk Score Key: 0-10 Low Risk; 11-15 Moderate Risk; 16-25 High Risk. [Further information on risk scoring can be found in the EC Risk Management Policy & Procedure]*

Appendix 1: Data Breach Reporting Thresholds

ICO Definition of ICO/Data Subject reporting thresholds

Likely to result in risk to people's rights and freedoms:	**Likely to result in high risk to people's rights and freedoms:**
"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."	Must inform those concerned directly and without undue delay (as soon as possible) A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Again, you will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again, the risk is higher

Appendix 2: SOC REPORT LAST 90 DAYS



Incidents over time

15 Jun - 13 Sep, compared to 17 Mar - 14 Jun

Total Incidents

378 ↓ 44%

P0

0 → 0%

P1

179 ↑ 17%

P2

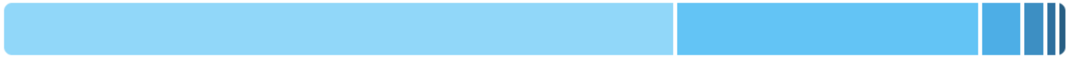
105 ↓ 73%

P3

94 ↓ 27%

Resolution overview

15 Jun - 13 Sep, compared to 17 Mar - 14 Jun



●	Out of Scope MDR	243	64.3%	↑ 48%
●	Benign True Positive	109	28.8%	↓ 70%
●	Analytic Under Review	14	3.7%	↑ ∞
●	True Positive (Malicious)	7	1.9%	↑ 600%
●	Closed By Customer	3	0.8%	↑ ∞
●	Unresolved	2	0.5%	↑ ∞