Corporate Ref.	CD 011
Level	Tier 3
Senior Responsible Officer	Chief Operating Officer
Version	4
EIA	3 July 2024
Approved by	Audit & Risk Assurance Committee
Approved date	2 October 2024
Superseded version	3
Review date	October 2026

Risk Management
Policy and Procedure

Version Control

Version	Author	Date	Changes
4	Portfolio Manager	27/09/2024	Transfer to new template and overall review.

1. Introduction

This policy and procedure outlines 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 seeks 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.
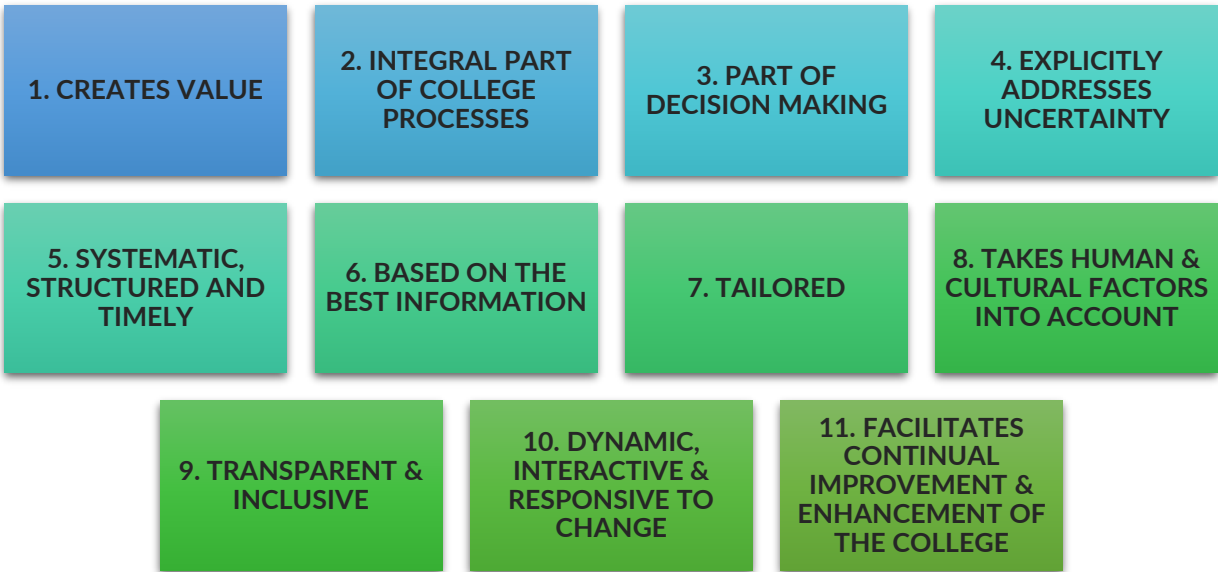
It is also understood that in some cases there is no clear strategic benefit from accepting some risks, e.g. risks associated with illegal, unethical or inappropriate, or dangerous activity. The College therefore recognises that its appetite and tolerance for risk will always vary according to the activity 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 organisation 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 its 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 the Board of Management 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 and 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.
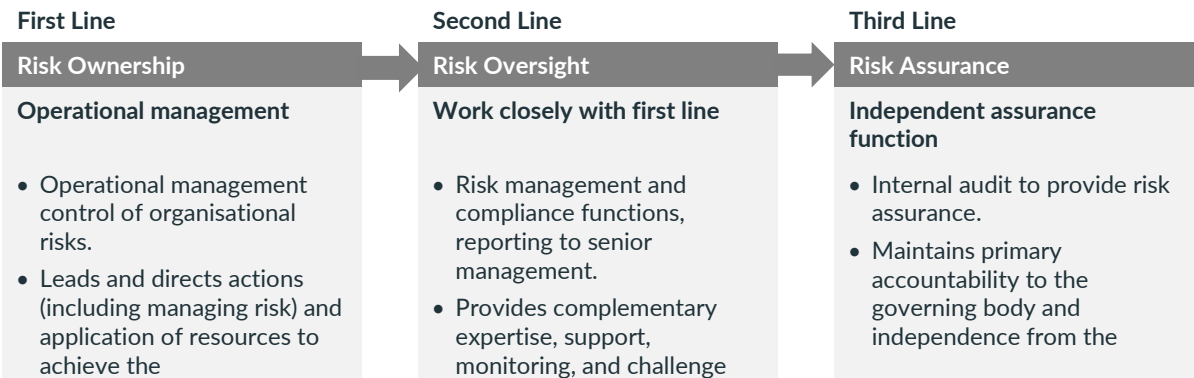
Both the strategic and operational risk registers are regularly updated and reviewed by the RMAG, the Audit and Risk Assurance Committee, and the Board to ensure effective oversight and management of risks at all levels of the College.

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	• Risk management and compliance functions, reporting to senior management. • Provides complementary expertise, support, monitoring, and challenge	• Internal audit to provide risk assurance. • Maintains primary accountability to the governing body and independence from 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.

related to the management of risk.

- Provides analysis and reports on the adequacy and effectiveness of risk management (including internal control).

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.

EDI Risk
Management Consid

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.
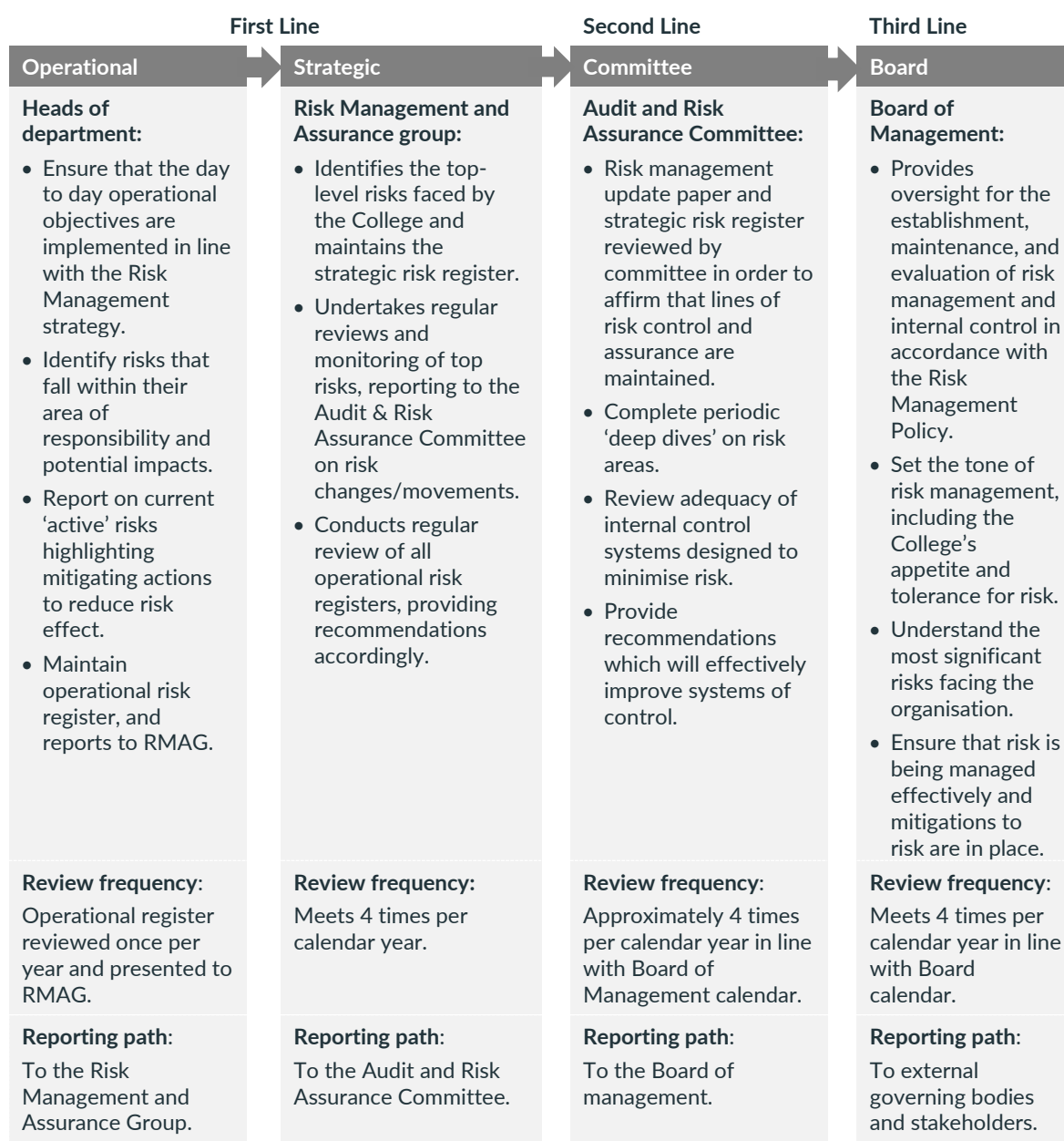
Role of College Staff

- 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		Second Line	Third Line
Operational	**Strategic**	**Committee**	**Board**
Heads of department:	**Risk Management and Assurance group:**	**Audit and Risk Assurance Committee:**	**Board of Management:**
• 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 highlighting mitigating actions to reduce risk effect. • Maintain operational risk register, and reports to RMAG.	• 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. • Conducts regular review of all operational risk registers, providing recommendations accordingly.	• 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. • Review adequacy of internal control systems designed to minimise risk. • Provide recommendations which will effectively improve systems of control.	• 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 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
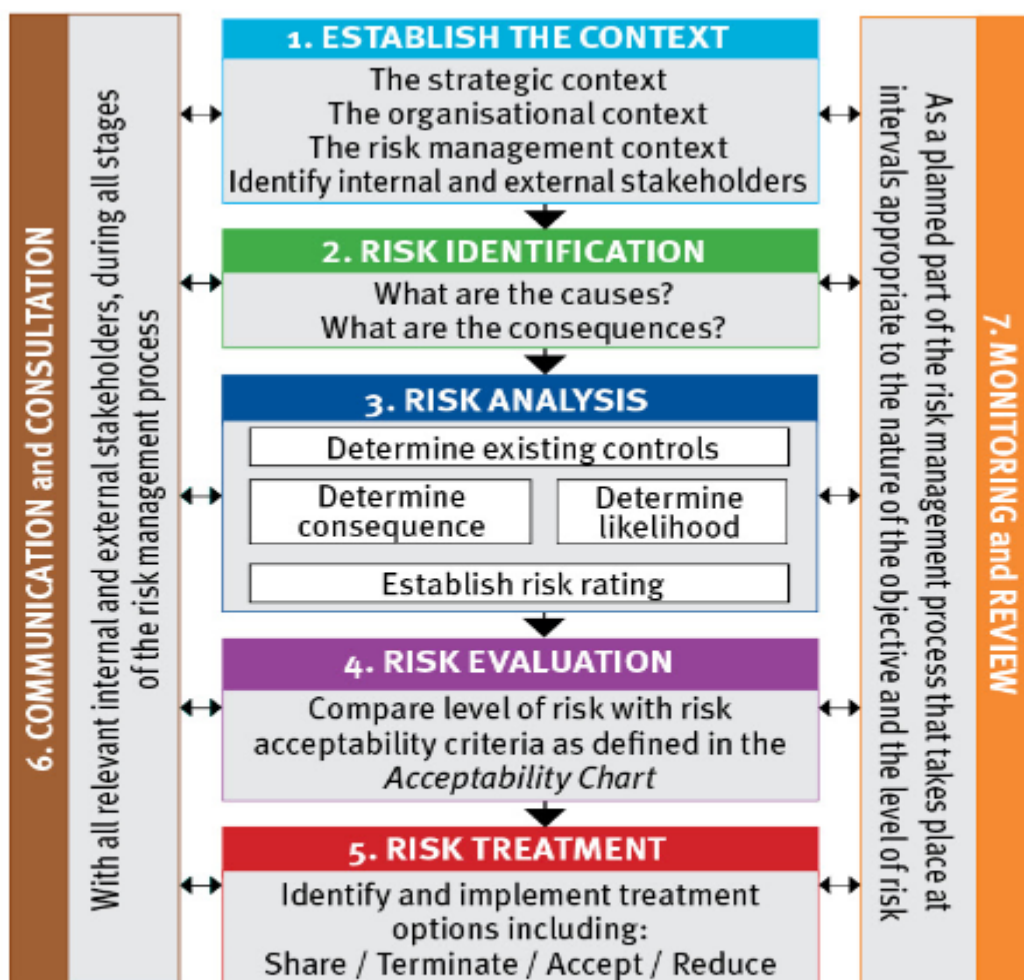
- Process based on ISO 31000: 2009
- Risk can be described as anything; event, practice, process, activity, etc. that could hinder or help achievement of stated goals or objectives

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 and 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.
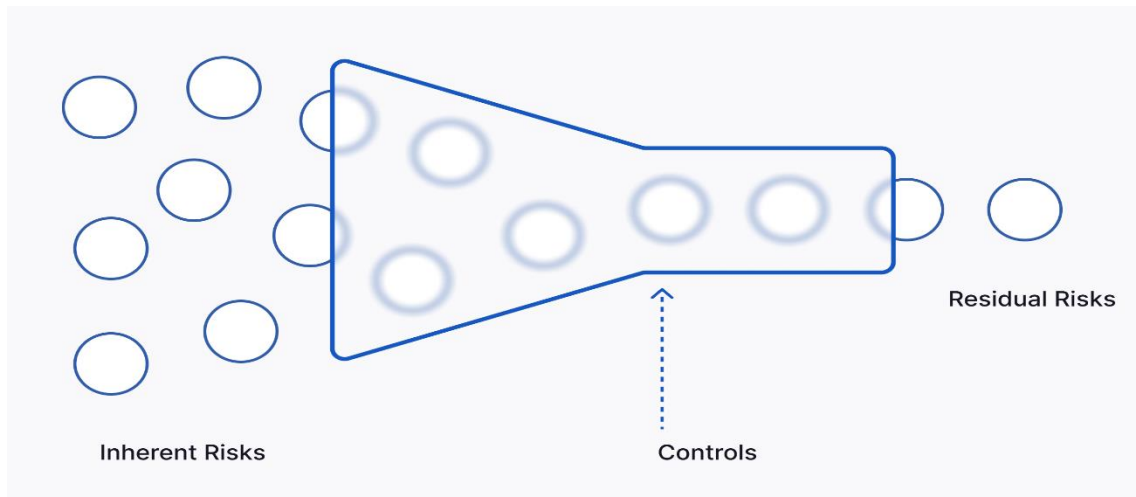
Inherent risk and residual risk (Refer Figure 3):

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 risk treatment involves lowering the risk exposure until it becomes acceptable or redundant. This can be achieved through both reactive measures, which reduce the impact if the risk occurs, and preventative measures, which reduce the likelihood of the risk happening in the first place.

- **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 assigned a risk owner responsible for taking appropriate action to minimise its impact on the College or faculty/department. The key treatment options and the individuals responsible for implementing them should be recorded in the relevant operational and strategic risk registers.

STEP 6 – Communication and consultation

Effective communication of risk management activities and outcomes across the College is essential to support informed decision-making, enhance risk management practices, and identify emerging threats.

Where the residual risk score remains higher than the College's risk appetite after treatment, additional controls should be implemented, where possible, to reduce the risk to an acceptable level.

Additionally, there is a formal risk escalation process in place. This ensures that unresolved or significant risks are reported by managers to the Senior Management Team (SMT), escalated to the Risk Management and Assurance Group (RMAG), and, if necessary, presented to the Board for further consideration and action.

STEP 7 – Monitoring and review

Monitoring and review periods should be integrated into the risk management process and conducted at intervals appropriate to the objectives and level of risk.

This process should also encompass a review of actual incidents and near misses to assess whether the current risk ratings and controls are adequate.

Additionally, it is important for management to evaluate continuous improvement aspects of risk management, ensuring that a culture of risk management is embedded within the College.

Risk deep dive reviews

The Audit and Risk Assurance Committee and the Board of Management will systematically conduct deep dive reviews into risk areas they deem appropriate throughout the year. Additionally, project risk reporting may be incorporated into these reviews to ensure comprehensive oversight of potential risks associated with ongoing projects.

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 to 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 to 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:	Adverse

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:	Adverse

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:	Adverse

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:	Adverse

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 and 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