Corporate Ref.	CD 011
Level	Three
Senior Responsible Officer	Director of Communications, Policy & Research
Version	Three
EIA	TBC
Approved by	Audit & Risk Assurance Committee
Approved date	12 October 2022
Superseded version	2
Review date	October 2024

Edinburgh College

For the future you want

Risk Management Policy and Procedure

Corporate Development

1. INTRODUCTION

This policy and procedure details the College's approach to risk management and the evaluation of internal controls, and is part of the College's internal control and Corporate Governance arrangements.

2. 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.

Approach to Risk

Edinburgh College's approach is to minimise the businesses exposure to harmful risk and take advantage of risk opportunities, in particular relation to ethical, social, reputational, compliance, and financial risk.

The College maintains two lines of risk management: Strategic and Operational.

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.

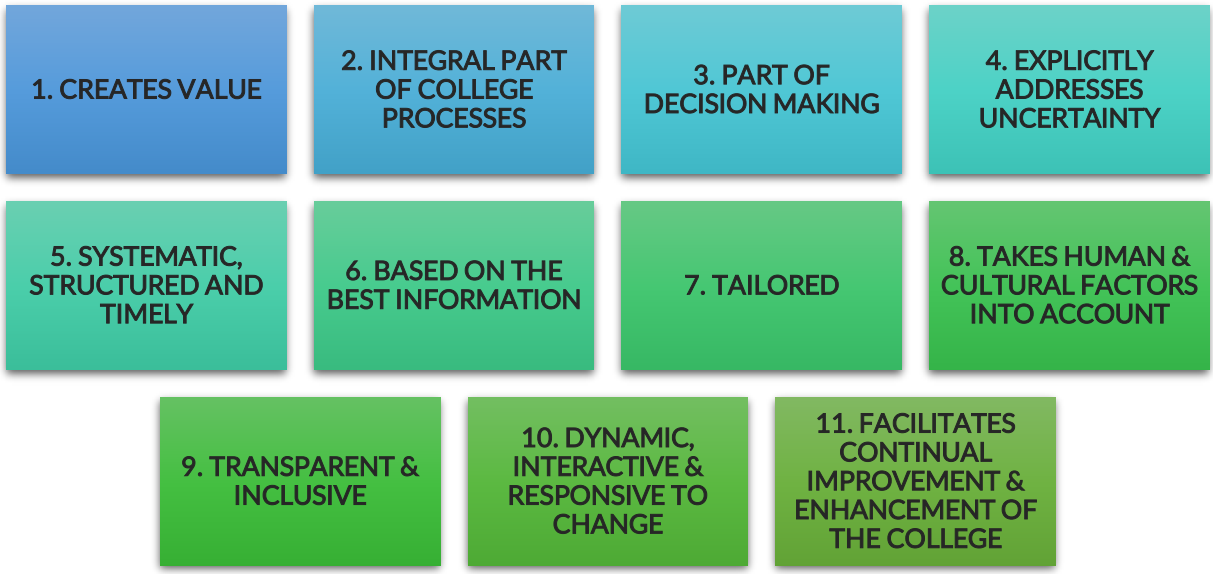
It is also understood that in some cases there is no clear strategic benefit from accepting some risks, e.g. risks that are associated with illegal, unethical or inappropriate and dangerous activity. The College therefore recognises that its appetite and tolerance for risk will always vary according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

3. RISK MANAGEMENT PRINCIPLES AND CULTURE

Edinburgh College follows ISO 31000 principles of risk management (as shown in Figure 1), which provides guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose.

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

Figure 1 - Risk Management Principles



4. THREE LINES OF DEFENCE (ASSURANCE) FRAMEWORK

Edinburgh College adhears to the 'Three lines of defence' model , which is designed to improve the College's approach to internal control, assurance and risk management.

The model identifies organisational arrangements and clear lines of accountability, which are responsible for providing assurance with regard to the management of key business areas and risks. The model can be summarised as follows:

First Line	Second Line	Third Line
Risk Ownership	**Risk Oversight**	**Risk Assurance**
Operational management • Functions that own and manage key operational business areas and risks • Provide strategy for controls • Identify, assess, control and mitigate risk • Security is designed into the system	**Work closely with first line** • Functions that oversee or specialise in monitoring key business areas, risk management, quality control, and compliance • Identifying known and emerging issues • Identifying shifts in the College's implicit risk appetite	**Independent assurance function** • Functions that provide internal and external audit and independent assurance of key business areas and risks • Report to external parties and Board of Management

	• Assisting management in developing processes and control to manage risk and issues	

5. ROLES AND RESPONSIBILITIES

Lines of Responsibility

- The Chair and Committee members of the Board of Management and the Principal have the responsibility for overseeing risk management within the College.
- The Principal and the Executive Team have the responsibility to oversee, support, and implement policies approved by the Board of Management which improves risk management across the College.
- The Senior Management Team have functional responsibility to manage and mitigate against those risks under their responsibility, individually and collectively. They are also responsible for producing and reviewing subsidiary operational risk registers detailing the top risks in their area of operations. This includes implementation of the management of these risks.
- 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
    - Secretary to the Group
- All staff are responsible for encouraging and embedding good risk management practice within their area of activity.

Role of Board of Management

The Board of Management has a fundamental role to play in the management of risk. Its role is to:

- provide risk oversight of the College's risk framework, its risk policies and procedures, and its management of strategic risks
- set the tone (risk appetite and risk tolerance) for risk management within the College
- know about the most significant risks facing the organisation
- ensure that risk is being managed effectively and solutions to risk mitigation are implemented

Role of Executive Team

- Implementation of the Risk Management Policy
- Promotion of a holistic approach to risk management
- Report new significant risks which develop within their area of responsibility to the Risk Management and Assurance Group
- Report any risk which no longer exists to the Risk Management and Assurance Group
- Report any risk which cannot be controlled at local level to the Risk Management and Assurance Group
- Ensure there are appropriate levels of risk oversight and awareness throughout the organisation
- Maintain functional control of risks within area of responsibility

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

- To review new risks or failures of existing control measures
- To review the 'probability' and 'impact' scoring of strategic level risks on a regular basis
- To review the adequacy of internal control systems designed to minimise risk
- To receive the reports from the Risk Management and Assurance Group and make appropriate recommendations, which will effectively improve systems of control

Role of Risk Management and Assurance Group

- To identify and analyse the top risks faced by the College and review the Strategic Risk Register
- To regularly review and monitor the 'probability' and 'impact' of top college risks and report progress to the Audit and Risk Assurance Committee
- Review of operational risk registers for all College departments/teams each calendar year
- Overall co-ordination of College Risk Management

- To maintain the Board of Management's confidence that risk is being managed effectively within the organisation and that solutions to identified risks are appropriate and in place

Role of Senior Management Team

- Co-ordinate and ensure that the day-to-day operational objectives are implemented in line with the Risk Management Policy and Procedure
- Be aware of risks which fall into their area of responsibility, the possible impacts these have, manage, and mitigate risks occurring and monitor outcomes against the risks identified ensuring that procedure notes detail corrective action to minimise future risk
- Report systematically and promptly to Executive Team and Risk Management and Assurance Group of any perceived new risks or failures of existing control measures
- Report to the Risk Management and Assurance Group on current 'active' risks highlighting mitigating actions and effect towards risk reduction via relevant operational risk register
- Ensure the operational risk register is kept up to date

Role of Risk Champion

- 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 register is complete and up to date and that risks are not being overlooked or ignored
- Provide feedback where they believe risks are not clearly described or are not directly linked to one or more stated objectives
- All risks should have an owner, ensure during reviews that risks are assigned to the appropriate person (typically the owner of the objective/s) and that the owner clearly understands the risk and what is being done about it
- Ensure that the assessment of the inherent/residual risk score is reasonable/ accurate
- Where applicable, ensure that further controls identified for risks are implemented and that an owner is appointed to implement controls with a clear target date
- Carry out spot-checks between formal reviews of the risk register to ensure owners fully understand their role/responsibility to the risk and that they are managing them

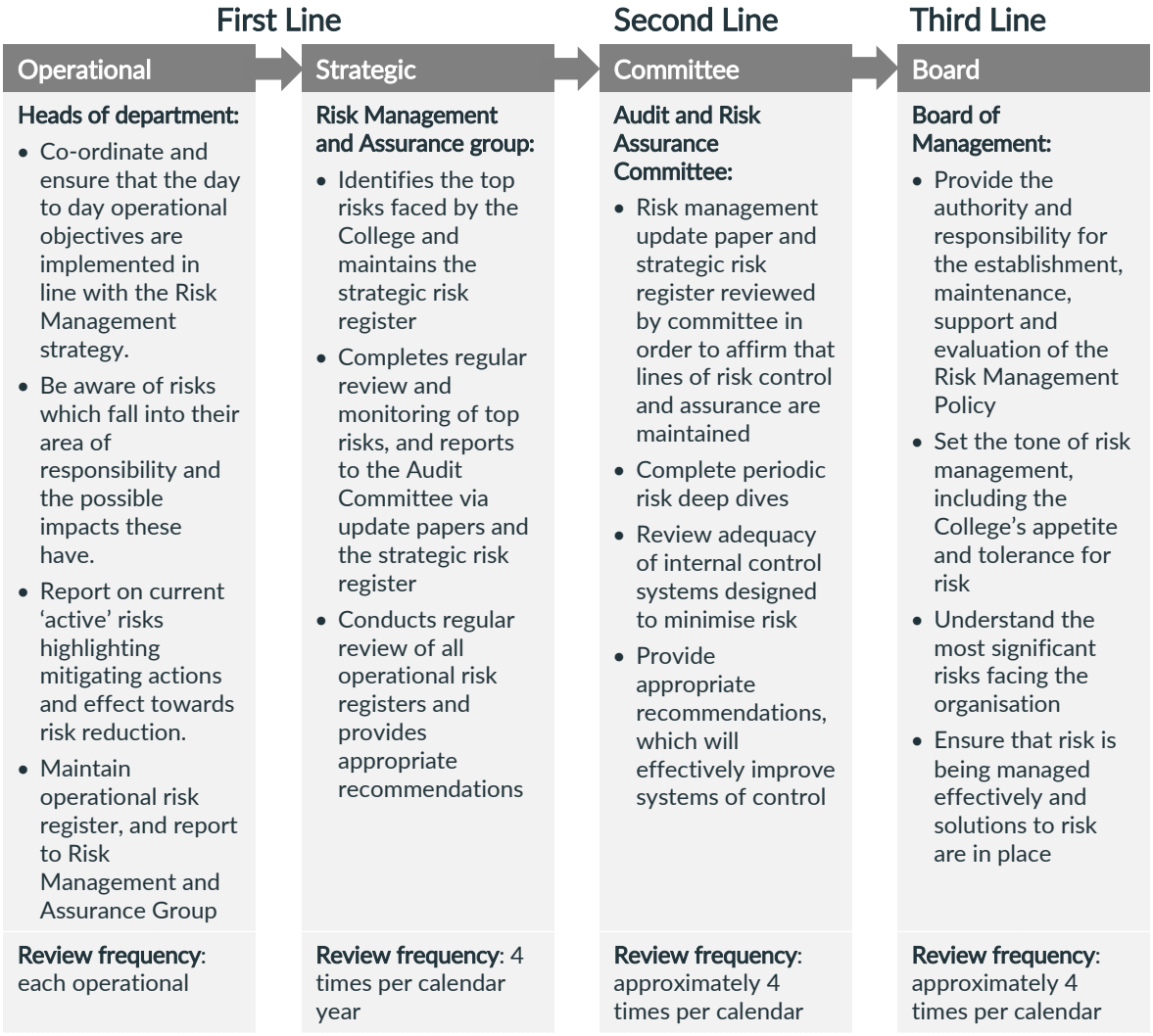
Role of College Staff

- 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 any perceived new risks or failures of existing risk control measures

6. REGISTERS AND REPORTING

Edinburgh College maintains risk registers at strategic and departmental (operational) levels. These risk registers record details of all identified risks along with their analysis and plans for risk treatment.

The following diagram demonstrates the risk management reporting path within the three lines of defence:



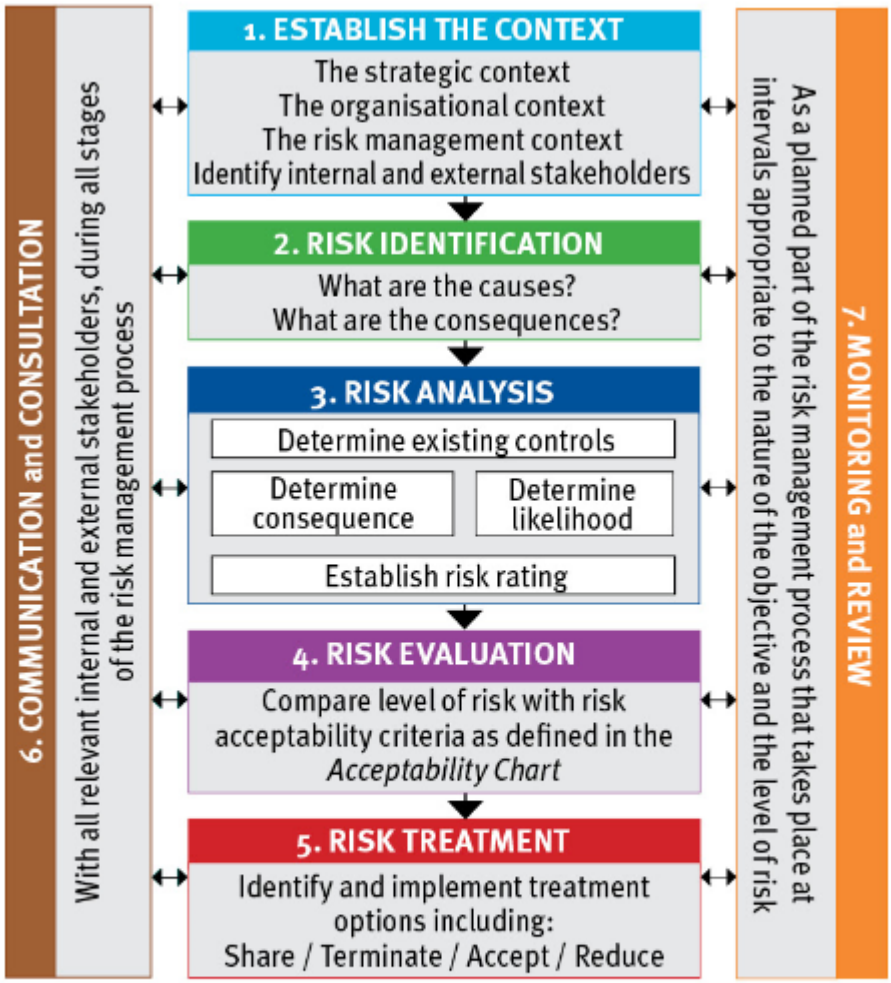
register reviewed once per year		year in line with Board of Management calendar	year in line with Board of Management calendar
Reporting path: Heads present the operational risk registers to the Risk Management and Assurance Group	**Reporting path**: Risk management update paper, including the strategic risk register, presented at each Audit and Risk Assurance Committee meeting	**Reporting path**: Board of management Risk management update paper, including the strategic risk register development for the Board in line with instructions / recommendations provided by the Committee	**Reporting path**: External governing bodies and stakeholders

7. RISK MANAGEMENT PROCEDURE

This risk management procedure seeks to help deliver objectives, promote sound decision-making, and prioritise resources (as shown in Figure 2).

The steps outlined in this section should be considered when updating/developing the relevant Risk Register template document.

Figure 2 - ISO31000: 2009 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, departmental priorities, current objectives, scope and activity.

If considering operational risks then think in terms of what could impact the day-to-day processes, people or systems currently in place.

If considering project or programme risks think in terms of what could impact 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, e.g. what, when and how something could happen that represents a source of potential harm to the College.

It is important that any risk assessment is as objective and balanced as possible. Make use of information that is already being collated, discuss with colleagues, and try to identify any similar risks already being considered.

Here is a list of useful questions to apply when considering risk identification:

- Is there any risk to compliance, statutory, regulatory, policy and contractual requirements?
- Is there any danger of litigation to the College, its staff, or students?
- 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 with staff, students, stakeholders, or communities?
- Is there a lack of control or management oversight of the identified issue that can be improved?
- Are there any targets or objectives that are not being met or won't be met?
- Does the risk pose a financial problem to the organisation?

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 protective equipment, lifting and handling, equipment, warning signs and task design
- **Procedural Controls** – such as policies, procedures, clinical protocols
- **Professional Controls** – such as compliance with external regulatory standards, national and local guidelines, quality standards

Controls are ineffective without the necessary information, instruction, guidance, and training. Therefore, consider the adequacy of any training, equipment, staffing or resources.

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 of high risk (Red), moderate risk (Amber) and low risk (Green).

Scoring is documented within risk registers and is reviewed by the register owners and the relevant boards, committees, and groups as necessary.

RAG classifications are applied to risk based on the following two themes:

1. The **PROBABILITY (likelihood)** of the risk occurring if the existing controls fail, or if effective safeguards cannot be applied. *See Appendix 1 – Probability Factor Scoring for further details on how to score risk probability.*
2. The **IMPACT (consequence)** of the risk occurring. This is measured in terms of the actual or potential severity of physical injury, impact on services or goal achievement, or overall impact for the College. *See Appendix 2 – Impact Factor Scoring for further details on how to score risk impact.*

Probability and Impact are each scored from **1 – 5** and are then combined to produce an overall risk score. **Probability x Impact = Risk Score**

Probability and Impact should be continuously monitored and adjusted to give an accurate and honest appraisal of the risk. (Risks should be scored as is, not what we want them to be).

The below risk matrix demonstrates how RAG classifications are applied based on the risk score:

RAG SCORE KEY	LEVEL OF RESPONSIBILITY
0 – 10 LOW RISK	**Minimal concern or on Target - Under Management Control** **When Green**, controls and assurances are adequate/effective in proportion to the risk
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 risk

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 risk

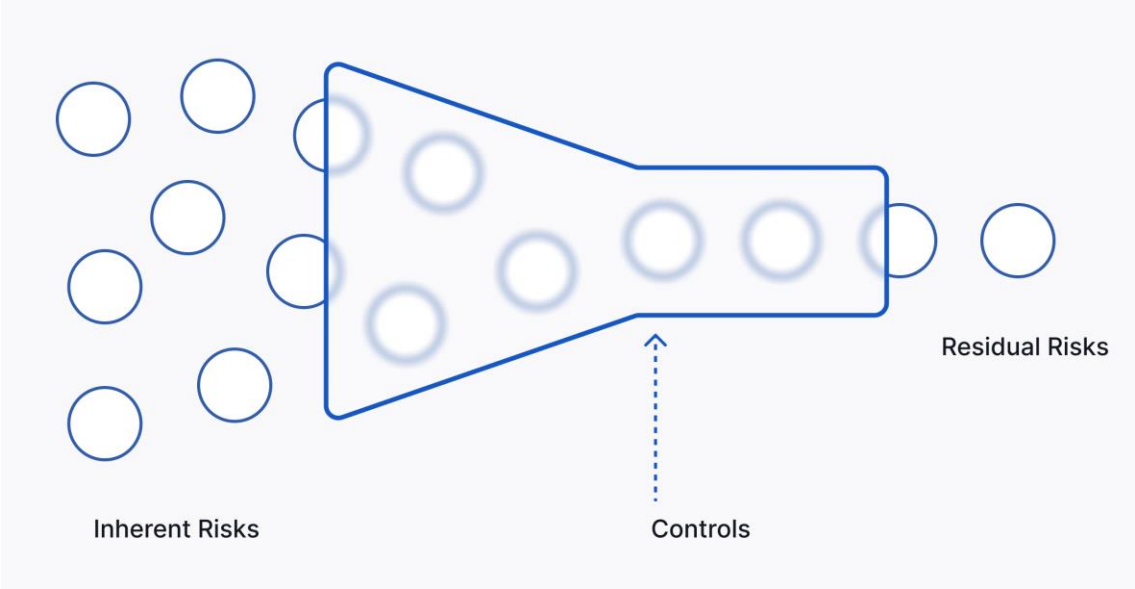
When it comes to risk analysis, there are two types of score assessments made for each identified risk.

Inherent risk vs. residual risk (See Figure 3)

1. **Inherent risk** is the amount of risk that exists in the absence of controls. In other words, before the College implements any counter-measures, the risk they face is the inherent risk.

2. **Residual risk** is the risk that remains after controls have been put in place. It's the risk that remains after the College has taken proper precautions.

Figure 3 - Inherent risk vs. Residual Risk



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

STEP 4 - EVALUATION

Risk evaluation is the process of assessing a risks potential significance and the level of oversight that should be applied.

Significance

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

1. **Acceptable** - The risk does not necessarily require further treatment or monitoring as the actions and mitigations in place are sufficient to adequately control the risk.
2. **Unacceptable** – The risk will require further treatment to reduce its severity / probability to a more acceptable level. Risks in this category will require treatment, as outlined in Step 5.

Oversight

The following are the levels of risk oversight 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 Top-Level Risk Register.
2. **Operational** – Risks at this level are more specific to a business area of the College and therefore require oversight at a department level via an Operational Risk Register.

When risks are identified and recorded it is expected that decisions are made in management forums to determine whether the risk is recorded on the departments operational risk register or if the risk needs to be escalated to the strategic top-level risk register.

STEP 5 – RISK TREATMENT

Based on the outcomes of your evaluation in Step 4 the following treatment options should be considered:

- **Share:** if practical, share some of the risk with partnerships, suppliers or insurers.
- **Terminate:** cease or take steps to cease the activity causing the risk altogether. Proper operational approvals should be obtained.
- **Reduce:** the most common treatment, reduce the risk by applying additional treatments until the risk becomes acceptable, realised, or redundant.
- **Accept:** some risks may be unavoidable in which case future actions should focus on minimising the impact to the College when the risk is realised. (e.g. Brexit)

Action will be taken as soon as possible, at all levels of the organisation as appropriate, to eliminate or reduce the risk. Each risk must be allocated a risk owner who will be responsible for taking appropriate action to minimise its impact.

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 activities and understanding; and when identifying emerging possible threats.

STEP 7 – MONITORING AND REVIEW

Monitoring and review periods should be a planned part of the risk management process and should take place at intervals appropriate to the nature of the objective and the 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 throughout the year.

Strategic Level Reporting

The top-level risk register for the College is monitored and updated by the Risk Management and Assurance Group four times each calendar year.

A risk management update, along with a copy of the top-level risk register, is submitted to the Audit and Risk Assurance Committee and Board of Management for review and feedback.

The College also references the 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 Risk Management and Assurance Group once per calendar year.

8. APPENDIX 1 – 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

9. APPENDIX 2 – 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 co-ordinated 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