STRANMILLIS UNIVERSITY COLLEGE
A College of Queen's University Belfast

RISK MANAGEMENT POLICY & PRACTICE

Version No:	Reason for Update	Date of Update	Updated By
1	Review Timeframe	September 2014	Governance Manager
2	Review	June 2017	Head of Corporate Governance & Planning
3	Review: Updated to expand risk appetite, escalation and de-escalation guidance and to revise the definition of Risk	February 2019	Head of Corporate Governance & Planning (Reviewed by Senior Leadership and Governing Body Committees)
4	Review of Policy, including Risk Appetite	June 2021	Head of Corporate Governance & Planning Senior Leadership Governing Body Committee Chairs
5	Review of Policy, including Risk Appetite	June 2022	Head of Corporate Governance & Planning Senior Leadership Governing Body Committee Chairs

6	Review of Policy, including Risk Appetite	July 2023	Head of Corporate Governance & Planning Senior Leadership Chair of Audit & Risk Assurance Committee
7	Review of Policy, including Risk Appetite	Sept 2024	Senior Leadership Chair of Audit & Risk Assurance Committee
8	Review of Policy, including Risk Appetite	Sept 2025	Corporate Committee Chair of Audit & Risk Assurance Committee

Date for Document Review: Sept 2028

Review / Approval History	Date
Equality Screening	XXX
Corporate Committee	23rd September 2025
Audit, Risk Assurance Committee	XXX
Governing Body	24th September 2024

Summary of Changes

This table details the specific changes from the previous version:

Page Nos:	Reason for Update	Date of Update	Changes Marked
3	Summary of Changes table added	August 2025	No
4	Contents page updated	August 2025	
17	Internal Audit Recommendation – section on Assurance timetable and Reporting Cadence included	August 2025	
22	Internal Audit Recommendation – section on Risk Archive Management included	August 2025	
37	Internal Audit Recommendation – Risk Archive Management Template included	August 2025	

Contents

Risk Management Policy

1. Introduction

1.1 The purpose of this Policy, which forms part of the University College's (the College) internal control and corporate governance arrangements, is to provide a framework for the effective management of risk across the College in pursuing its Mission, Vision and Strategic Aims and Objectives.

1.2 The objectives of the Policy are to:

- continuously develop risk management and raise the profile of the effective management of risk across the College;
- integrate risk management into the culture and decision making of the College;
- manage risk, including the determination of the College's risk appetite and monitoring of its risk profile, in accordance with best practice; and
- create effective risk management processes that will allow the College to make risk management assurance statements to the Sponsor Department, currently the Department for the Economy (DfE), with confidence.

1.3 Risk arises where there is uncertainty of outcome and is anything that could impact on the College's ability to achieve its objectives. It can arise through direct threats, leading to a failure to achieve objectives, or through the failure to fully exploit opportunities that could provide a better way of meeting objectives. Risk management is about identifying risks, assessing their significance and taking appropriate action to manage them. It is a fundamental element of good management practice.

1.4 The management of risks and the maintenance of risk registers at strategic / corporate, operational and programme / project levels should be led from the top and embedded in the normal working routines and activities of the College.

1.5 The management of risk is regularly reviewed and reported to the Governing Body and its Committees in order to monitor the College's risk profile and to gain assurance that risk management is effective and that necessary and timely action is being taken.

1.6 The Audit and Risk Assurance Committee is responsible for appointing Internal Auditors whose activities and reports provide the Committee with an element of assurance including on the effectiveness of the College's risk management arrangements. Internal Auditors are not however a substitute for management ownership of risk management or a substitute for an embedded risk review and management system carried out by staff who have executive responsibility for the achievement of the College's objectives.

1.7 This Policy sets out the principles that will apply to the management of risks by the College. The Governing Body will review the Policy annually and approve changes or improvements to key elements of its processes and procedures.

2. Risk Policy

2.1 Stranmillis College's Mission is 'To transform the lives of children, young people and communities, through excellence in teaching, research and scholarship'

2.2 Much of the College's work is innovative and ground-breaking – and as such involves a certain amount of conscious risk taking.

2.3 The College's Governing Body is committed to ensuring good governance in the delivery of the institution's Mission and Strategic Objectives, including the effective and efficient management of its resources and the high quality of the College's projects and activities. The College will minimise – and were appropriate eliminate, where cost effective and reasonable to do so - risks to the achievement of objectives through an appropriate system of controls, so that residual risk, after mitigating actions, can be borne without serious or permanent damage to the College.

2.4 Through this Policy, the aim is to ensure that risk management is effective and is integrated in the way the College is directed, managed and operates. As an integrated part of the management systems, and through the normal flow of information, this risk management framework will harness the activities that identify and manage the threats and uncertainties faced by the College and systematically anticipate and prepare successful responses.

2.5 The College recognises both its **strategic (corporate) risks**, which will be monitored by the Governing Body, and the **operational and project risks**, which will be monitored by the Senior Leadership Team and Academic Committees and other Governing Body Committees and reported to the Governing Body on a regular basis.

2.6 It is the responsibility of the Governing Body supported by the Audit and Risk Assurance Committee:[1]:

- to lead the assessment and management of risk and take a strategic view of risks in the College;
- to ensure that there are clear accountabilities for managing risks and that staff are equipped with the relevant skills and guidance to perform their roles effectively and efficiently;
- to ensure that roles and responsibilities for risk management are clear to support effective governance and decision-making at each level with appropriate escalation, aggregation and delegation;
- to determine and continuously assess the nature and extent of the principal risks that the College is willing to take to achieve its objectives – its "risk appetite" – and ensure that planning and decision-making appropriately reflect this assessment;
- to agree the frequency and scope of its discussions on risk to review how management is responding to the principal risks and how this is integrated

[1] The Orange Book Management of Risk – Principles and Concepts updated 2023

with other matters considered by the Governing Body, including business planning and performance management processes;

- to specify the nature, source, format and frequency of the risk management information that it requires;
- to ensure that there are clear processes for bringing significant issues to its attention more rapidly when required, with agreed triggers for doing so;
- to use horizon scanning to identify emerging sources of uncertainty, threats and trends;
- to assure itself of the effectiveness of the College's risk management framework;
- to assess compliance with the Committee of University Chairs Code of Governance for Higher Education Institutions and include explanations of any departures within the governance statement of the College's annual report and accounts.

In addition, it is the responsibility of the Governing Body:

- to hold the Principal of the College to account for maintaining a sound system of internal control that supports the achievement of policies, aims and objectives while safeguarding the public and other funds and assets for which it is responsible in accordance with statutes and ordinances and the Partnership Agreement (or any replacement document) with the Department for the Economy (DfE);
- to set the standards and expectations of staff with respect to conduct and probity; and
- to satisfy itself that (less fundamental) Operational / Project risks are being identified, assessed, actively managed and reviewed, with appropriate and effective controls and assurance mechanisms in place.

2.7 It is the responsibility of the Principal, as Designated Accounting Officer, supported by the Audit and Risk Assurance Committee[2]:

- to periodically assess whether the College's values, leadership style, opportunities for debate and learning, and human resource policies support the desired risk culture, incentivise expected behaviours and sanction inappropriate behaviours;
- to ensure that expected values and behaviours are communicated and embedded at all levels to support the appropriate risk culture;
- to designate an individual to be responsible for leading the organisation's overall approach to risk management, who should be of sufficient seniority and should report to a level within the organisation that allows them to influence effective decision-making;
- to establish the organisation's overall approach to risk management;
- to establish risk management activities that cover all types of risk and processes that are applied at different organisational levels;

[2] The Orange Book Management of Risk – Principles and Concepts updated 2023

- to ensure the design and systematic implementation of policies, procedures and practices for risk identification, assessment, treatment, monitoring and reporting.
  Guidance on this, including the format of Risk Registers can be found at Annex 1 and Appendix B, respectively;
- to consider the organisation's overall risk profile;
- to demonstrate leadership and articulate their continual commitment to and the value of risk management through developing and communicating a policy or statement to the organisation and other stakeholders, which should be periodically reviewed;
- to ensure the allocation of appropriate resources for risk management, which can include, but is not limited to people, skills, experience and competence;
- to monitor the quality of the information received and ensure that it is of a sufficient quality to allow effective decision-making;
- to ensure that risk is considered as an integral part of appraising option choices, evaluating alternatives and making informed decisions;
- to be provided with expert judgements through functions to advise on:
  - the feasibility and affordability of strategies and plans;
  - the evaluation and development of realistic programmes, projects and policy initiatives;
  - prioritisation of resources and the development of capabilities;
  - the design and operation of internal control in line with good practice and the nature and extent of the risks that the College is willing to take to achieve its objectives; and
  - driving innovation and incremental improvements.
- to clearly communicate their expectation that risk management activities are coordinated and that information is shared among and across the 'lines of defence' where this supports the overall effectiveness of the effort and does not diminish any of the 'lines' key functions.

The three Lines of Defence are:

1. Management Control / Internal Control Measures;
2. Functions that oversee or specialise in Risk Management; and
3. Internal Audit.

Further guidance on 'the three Lines of Defence' can be found in the HM Treasury Orange Book:

https://www.gov.uk/government/publications/orange-book

University College Specific Commitments

2.8 In managing risk, the College commits to:

- satisfying all mandatory and statutory responsibilities and duties and its own policies and procedures in line with legislation and established good practice, such as that provided in the HM Treasury Orange Book (2023).

- promoting safe working practices thereby ensuring the health, safety and wellbeing of those who provide and / or use its services and the reduction and / or elimination of risk.
- promoting good relations in all of its activities – ensuring that they are inclusive and accessible to the best of its abilities.
- promoting awareness and management of risks through communication and training.
- establishing and regularly reviewing a systematic and consistent approach to risk assessment and risk reduction / elimination.
- prioritising risks and ensuring that their management and reduction is appropriately and proportionately resourced.
- implementing this Policy in line with the Risk Management Strategy – approved and regularly reviewed by the Governing Body.

Risk Appetite

2.9 Risk Appetite is defined as "the amount of risk that an organisation is willing to seek or accept in the pursuit of its long-term objectives[3]."

2.10 This Policy and Statement of risk appetite specifies the amount of risk the College is willing to tolerate or accept in the pursuit of its long-term objectives.

2.11 The College does not have an appetite for high exposure risks but recognises that delivering upon the ambitious strategic aims and objectives outlined in the Corporate Plan 2025-2028 will involve a degree of risk-taking and uncertainty. As such, there is an appetite for higher levels of risk, where justified, in order to deliver upon strategic aims, objectives, and targets. However, it is also important to note that the College's approach to risk taking will continue to be managed within this established Risk Management Policy framework. Consequently, higher levels of risk will only be accepted on the basis of a comprehensive understanding of the exposures involved, potential benefits arising and subject to appropriate mitigation, control responses, and approval arrangements being in place.

2.12 The management of risks in the College is undertaken within a framework comprising:

- Governance processes;
- Risk Policy and Appetite statement;
- Identification, evaluation, management and monitoring of significant risks;
- Assurance and audit processes; and
- The underlying policy and control environment.

2.13 In setting its risk appetite, the Governing Body acknowledges that there is a certain amount of risk in all of the College's activities and that it may not be possible or desirable to completely eliminate such risks. The priority is to minimise exposure to reputational, compliance and financial risks, while

[3] There are various definitions of Risk Appetite. The above has been taken from the Institute of Risk Management – Risk Appetite and Tolerance Guidance Paper (2011)

acknowledging that there are opportunities to take measured risks, for example, in the area of innovation in curriculum and research, where there is a potential high risk of failure. The Governing Body must be assured however, that such ‘opportunity’ risks are carefully managed with robust controls and that where necessary, contingency arrangements are put in place.

2.14 The Governing Body also acknowledges that project risk appetite may need to differ from the risk appetite applied to routine business and therefore this will be considered on a project-by-project basis.

2.15 The Governing Body’s appetite for risk across its activities is provided in the following table.

The overarching definitions are taken from the Risk Appetite Guidance Note at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1012891/20210805_-_Risk_Appetite_Guidance_Note_v2.0.pdf

The Risk Appetite assessment categories are as below:

- **Averse**; Avoidance of risk and uncertainty in achievement of key deliverables or initiatives is key objective. Activities undertaken will only be those considered to carry virtually no inherent risk.
- **Minimal**; Preference for very safe business delivery options that have a low degree of inherent risk with the potential for benefit / return not a key driver. Activities will only be undertaken where they have a low degree of inherent risk.
- **Cautious**; Preference for safe options that have a low degree of inherent risk and only limited potential for benefit. Willing to tolerate a degree of risk in selecting which activities to undertaken to achieve key deliverables or initiatives, where we have identified scope to achieve significant benefit and / or realise an opportunity. Activities undertaken may carry a high degree of inherent risk that is deemed controllable to a large extent.
- **Open**; Willing to consider all options and choose one most likely to result in successful delivery while providing an acceptable level of benefit. Seek to achieve a balance between a high likelihood of successful delivery and a high degree of benefit and value for money. Activities themselves may potentially carry, or contribute to, a high degree of residual risk.
- **Eager**; Eager to be innovative and to choose options based on maximising opportunities and potential higher benefit even if those activities carry a very high residual risk.

and are supported by descriptions across a range of areas.

Strategic Risk Appetite Descriptions	
Compliance, Regulation & Ethics	**AVERSE** The College places high importance on maintaining the highest standards of integrity, compliance, and ethics, including in respect to Child Protection and Safeguarding. As such, the College has no appetite for any breaches in statute, regulation, professional standards, research ethics, bribery, or fraud, including systems and processes.
Information & Security	**AVERSE** The College is committed to maintaining the highest standards of Security, including physical security, cyber security and compliance with General Data Protection Regulation requirements to prevent unauthorised and / or inappropriate access to its estate, and unauthorised access to and disclosure of its information assets.
Teaching and Learning	**OPEN** The College is committed to delivering the highest quality teaching and learning for all of its students as well as developing enhanced / innovative approaches to teaching and learning. This will involve further investment in teaching and learning facilities / infrastructure and continual updating and refreshing of the curriculum. In delivering its objectives, the College recognises the need to identify solutions to meet increasingly diverse student needs and to further its work with professional bodies and others to ensure success The College recognises that this may involve an increased degree of risk in developing education and in this respect a moderate level of risk is acceptable, subject always to ensuring that potential benefits and risks are fully understood before developments are authorised and that appropriate measures are in place to mitigate risk.
Research and Knowledge Transfer	**OPEN** The College is committed to ambitious and performance-driven progress in research and knowledge exchange including: - promoting new fields of research in the Education field and building research capacity; - developing further strategic academic collaborations and partnerships nationally and internationally; - facilitating enhanced research opportunities, performance and funding; - supporting innovation and increasing the number of postgraduate students engaged in research.

	The College recognises that this will involve an increased degree of risk in developing research. In this respect, a moderate level of risk is acceptable, as long as Funding Rules and Ethics are not compromised, risks are fully understood and appropriate measures are in place to mitigate risk.
Internationalisation	**OPEN** The College has a reputation in the international arena, is committed to international growth and will continue to assess further international partnerships where appropriate as well as increasing the internationalisation of its research / knowledge exchange activities and the international mobility of students and staff. The College recognises that this will involve an increased degree of risk in developing international activities. The College is comfortable in accepting a moderate level of risk subject to ensuring that the potential benefits and risks are fully understood before developments are agreed and that appropriate measures to mitigate the risks have been implemented.
Student Experience	**MINIMAL** The College is committed to further development of facilities and support arrangements for the student learning and living experience and in ensuring that programmes are accessible to students from all backgrounds. The College will therefore maintain a generally low (minimal) appetite for any risks which threaten the delivery of objectives in this area.
Reputation	**MINIMAL** The College has an established track record for learning, teaching, research, Lifelong Learning and student experience. As such, there is a low (minimal) appetite for any risks which would impact negatively upon the College's reputation, 'brand', ethical standing, or heritage which could lead to undue adverse publicity, or could lead to loss of confidence by stakeholders, including its Sponsor Department, currently the Department for the Economy (DfE).
Financial Performance and Sustainability	**MINIMAL** The College aims to maintain its long-term viability and its overall financial strength. It has a sound financial base, it has Financial Regulations in place, has diversified its sources of income over and above that provided by its Sponsor Department. It has also demonstrated effective control of budgets and maintains a focus on delivering Value for Money (VfM). The College has a low (minimal) appetite for any risks which will impact upon the achievement of its financial targets. The College will ensure that potential benefits and risks are fully understood before developments are agreed and that appropriate measures to mitigate risk are established.

People and Culture	**MINIMAL** The College aims to value, support, develop and utilise the full potential of all its staff and students and to provide a stimulating, harmonious and safe place to work and study. It places importance on a culture of academic freedom, equality and diversity, dignity and respect and collegiality. The College has a low (minimal) appetite for any deviation from its standards in these areas.
Major Project and Change Activities	**OPEN** Major change activities are required periodically to develop the College, and to adapt to changes in the regulatory and technological environment and generally in the nature and conduct of the College's activities. The College expects such changes to be managed according to best practice in project and change management. The College has a low appetite for any deviation from its standards in this area. However, a moderate (open) level of risk may be accepted as long as the benefits are justified and appropriate measures to mitigate the risk are established.
Business Continuity	**MINIMAL** The College places high importance on maintaining continuity of all aspects of its operations and has a low (minimal) appetite for any adverse risks, incidents, or events which could negatively impact upon the College's brand or upon the normal operations.
Environment and Social Responsibility	**CAUTIOUS** The College aims to make a significant, sustainable, and socially responsible contribution to society both locally, nationally and internationally through its research, education, knowledge exchange, and operational activities. It recognises that this should involve a low-moderate (cautious) level of risk, which is acceptable, subject always to ensuring that potential benefits and risks are fully understood before developments are authorised and that appropriate measures to mitigate risk are established.

Professor Jonathan Heggarty	Date: September 2025
Principal & CEO	Review Date: September 2026
	For distribution to: All Staff

Annex 1

EFFECTIVE RISK MANAGEMENT – PRINCIPLES AND PROCESSES

Definition of Risk

Risk is defined as: The likelihood of outcome, whether positive opportunity or negative threat, of action, inaction, or events. Risk to the achievement of objectives will be assessed in respect of the combination of the likelihood of something happening, and the scale of potential impact.

Effective Risk Management:

- covers all risks, including governance, management, fraud, quality, reputational and financial, focusing on the most important risks. A comprehensive List of example risk categories is included at **Appendix A;**
- produces a balanced portfolio of risk exposure;
- is based on a clearly articulated policy and approach;
- requires regular monitoring and review, giving rise to action where appropriate;
- needs to be managed by an identified individual and involve the demonstrable commitment of Governors and staff;
- is integrated into normal business processes and aligned to the strategic objectives of the College.

Benefits

The process of identifying risks and the introduction of internal controls to help mitigate such risks helps to support effective business planning, avoids excessive risk taking and helps to improve the Institution's ability to respond quickly and effectively to opportunities and threats in the internal and external environment. Risk management is central to the achievement of objectives, whether at strategic, operational or project level.

Compliance and Reporting

Under the terms of the Partnership Agreement (or any replacement document) with the Department for the Economy (DfE), the College must ensure that there are appropriate arrangements in place to promote effective risk management, control and governance. This is a condition of the award of Grant.

The Code of Good Practice for Audit and Risk Assurance Committees sets out the minimum reporting requirements. Audit and Risk Assurance Committees must produce an Annual Report to the Governing Body, including an opinion on the adequacy and effectiveness of the system of risk management, internal control and governance.

The Accounts Direction from DfE also requires the College to issue a Governance Statement as part of the audited financial statements. This statement must include an account of the risk management arrangements in place and how risk assessment and internal control is embedded in the Institution's operations.

Assurance Timetable and Reporting Cadence

To enhance transparency and governance, the following assurance process shall be embedded:

Operational risk reviews shall be undertaken on a quarterly basis across all departments to ensure timely identification, assessment, and management of emerging and residual risks. These reviews serve as a preparatory mechanism for the Senior Leadership Team's scheduled evaluation of the Corporate Risk Register, enabling informed decisions regarding the escalation of significant operational risks or the removal of resolved risks from the Corporate Register. This process ensures that the Corporate Risk Register remains a dynamic and accurate reflection of the College's strategic risk profile, and supports effective governance and assurance reporting to the Governing Body and Audit and Risk Assurance Committee.

Formal reviews will occur:

- Quarterly at the Senior Leadership Team level
- Biannually at the Governing Body and Audit and Risk Assurance Committee

Each review will generate:

- Updated risk registers (departmental and corporate)
- Summary reports highlighting risk movements, emerging risks, and mitigation effectiveness

Reports will be used to inform:

- Departmental assurance reporting
- Annual ARAC opinion on the adequacy and effectiveness of risk management
- Strategic planning and resource allocation

Risk Management Principles

- The College will not commit to any new project or activity until a thorough and effective risk assessment has been carried out.
- The College will maintain an effective control framework, designed to contain risks where cost-effective to do so – and to manage risks effectively.
- All College staff will have commensurate responsibility for identifying and managing risk to the achievement of objectives.
- Risk management will be collaborative and informed by the best available information and expertise.
- The authority to take decisions involving risk will be commensurate with the level of risk – and will be clearly defined and communicated by management.
- Major external risks or threats to the College will be identified and monitored on a regular basis – and contingency plans made to effectively and proportionately respond in the event of such threats materialising.
- Where appropriate, risks should be minimised by the securing of appropriate insurances or indemnity from third parties with whom the

College is collaborating, including those with whom there is a contract to provide services.

- As part of the assessment of risks, dates and timelines for review will be established and adhered to and there will be a clearly identified individual Risk Owner.
- Risk will be a standing item on the agenda of the Governing Body, its Sub-Committees and Senior Management Committees.
- In keeping with the College's wider policies, risk assessment will include, wherever possible, consideration of the views of relevant stakeholders.

Risk Management Process

The risk management process is aligned to the Planning Process because of the linkage to the achievement of objectives. All objectives, corporate or otherwise, including project objectives must be assessed by management for risk to their achievement.

A format for recording risks in a Risk Register is attached at **Appendix B** and includes a summary analysis format as part of the presentation / reporting of risks. The Risk Register follows the risk management process as described below and has been designed with reference to the HM Treasury Orange Book - Management of Risk - Principles and Concepts (2023).

Key Points to Note in Relation to Risk Registers

- It is important to keep Risk Registers up-to-date in order to reflect the current control environment and further management actions being taken to manage the risks to an acceptable level.
- Risks with an inherent score falling within the 'green zone' do not need to be included in the Risk Register.
- Risks with a residual score of zero should be removed from the Risk Register if management is content that such risks have been dealt with. If circumstances change, the risk may be included again in the Risk Register as appropriate.
- Do not confuse routine activities with the **key** controls that are in place to manage the risks. It is also important to include both preventative and reactive controls. *Preventative Controls* include any policy, procedure, practice, process, technology, technique, method, or device that modifies or manages risk. *Reactive controls* relate to contingency measures that will be taken in the event of the risk materialising.
- Risk treatments or further actions being taken to manage the risk eventually become controls or modify existing controls, once they have been implemented.
- Where a target date is missed – the reason for slippage must be recorded along with a revised target date.
- Sources of assurance relate to how you are informed / how you know that the controls that are in place are working effectively. Identification of assurance provision for key controls helps to reinforce management's responsibility for the design and operating effectiveness of controls within the College – particularly in relation to identified risks thereby providing

greater assurance to the Principal regarding the overall management of the specific risks.

Step 1: Identifying and Defining the Risk

Identifying risks is the first step in the process of building the College's risk profile. This should be a continuous process, routinely generated through discussion with staff at Team / Committee meetings and when reviewing progress against Business Plans. Risks should be directly related to objectives, and a certain amount of horizon scanning may also be necessary to identify potential new risks.

A range of techniques can be used for identifying specific risks that may potentially impact on one or more objectives. The following factors, and the relationship between these factors, should also be considered:

- tangible (e.g. Budget shortfalls) and intangible (e.g. regulatory change) sources of risk
- changes in the internal and external context or environment
- uncertainties and assumptions within options, strategies, plans, etc.
- indicators of emerging risks
- limitations of knowledge and reliability of information
- any potential biases and beliefs of those involved

Risks should be identified whether or not their sources are under the College's direct control. Even seemingly insignificant risks on their own have the potential, as they interact with other events and conditions, to cause great damage or create significant opportunity.

It is important that the essence of the risk is clearly articulated in a Risk Statement to ensure that the management of the risk is focused in the right area. The statement should be stated in terms of the cause of the risk and its impact and not simply the failure to deliver a specific objective. An example risk statement is provided in **Appendix B.**

Step 2: Assessing the Inherent Risk

The inherent risk assessment is the level of risk before any controls to address that risk have been put in place. It is important that this assessment is undertaken so that the College knows what the exposure would be if controls were to fail. The inherent risk should be assessed in respect of the combination of the likelihood of something happening, and the impact if it does actually materialise. Guidance on assessing the level of inherent risk is attached at **Appendix C.**

Step 3: Risk Analysis and Evaluation

Risk analysis supports a detailed consideration of the nature and level of risk. The analysis can be undertaken with varying degrees of complexity, depending on the purpose of the analysis, the availability and reliability of evidence and the resources available.

Risk evaluation should involve comparing the results of the risk analysis with the nature and extent of the risks that the College is willing to take – the Governing Body's risk appetite – to determine where and what additional action is required. Options may involve one or more of the following:

- avoiding the risk of feasible, by deciding not to start or continue with the activity that gives rise to the risk.
- taking or increasing the risk in order to pursue an opportunity.
- retaining the risk by informed decision.
- changing the likelihood, where possible.
- changing the consequences, including planning contingency activities.
- sharing the risk e.g. through commercial contracts.
- transferring the risk e.g. via insurance.

The outcome of risk evaluation should be recorded in risk registers, communicated and validated at appropriate levels of the College. The risk register should be regularly reviewed and revised based on the dynamic nature and level of the risk faced.

Step 4: Controlling the Risk

This stage of the process is about identifying the controls that are currently in place to manage the risk. Such controls should give reasonable assurance of confining the risk within the risk appetite agreed by the Governing Body. The purpose of controls is normally to constrain or reduce the risk to an acceptable level, rather than to eliminate it.

Step 5: Assessing the Residual Risk

The residual risk assessment takes account of the controls that are already in place to manage the risk. This risk assessment will also consider the combination of the likelihood of something happening, and the impact if it does actually materialise.

Step 6: Considering What Further Actions Are Necessary to Manage the Residual Risk

The adequacy of the controls can only be considered once the residual risk is identified. At this stage it is important to consider what further options are appropriate in order to further treat or reduce the risk / manage the residual risk to an acceptable level. This should be viewed in the context of the risk appetite and tolerability levels decided by the Governing Body as set out in the Risk Management Policy at paragraph 2.15.

Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived in enhancing the achievement of objectives against the costs, efforts or disadvantages of proposed actions. Justification for the design of risk treatments and the operation of internal control is broader than solely economic considerations and should take into account all of the College's obligations, commitments and stakeholder views.

As part of the selection and development of risk treatments, how the chosen option(s) will be implemented should be specified, including the rationale for the selected option(s) and the expected benefits to be gained.

The proposed actions should be recorded in the Risk Register alongside target dates for implementing such actions and the name of the post holder responsible for taking each action forward.

It should be noted that some risk is unavoidable and it is not within the College's ability to manage the risk to a tolerable level, in which case this should be clearly identified in the Risk Register. The need for contingency arrangements should also be considered in the event of the risk materialising.

It should also be noted that some risks may not be the responsibility of the College, in which case ownership for such risks should be transferred, where possible. Nevertheless, the College will wish to seek assurance from the other party, for example in a contract situation that the third party has processes in place to manage those risks.

Terminating the risk will be a last resort. For example, in a project management situation if it becomes clear that the project cost / benefit relationship is in jeopardy a decision may be taken to cease the project. This will be a matter for the Project Board and the Governing Body to consider.

Risk Monitoring

Monitoring should play a key role before, during and after implementation of risk treatment. Ongoing and continuous monitoring should support understanding of whether and how the risk profile is changing and the extent to which internal controls are operating as intended to provide reasonable assurance over the management of risks to an acceptable level in the achievement of the College's objectives.

Principal (Corporate risks) should be subject to "deep dive" reviews by the Governing Body and / or the Audit and Risk Assurance Committee, with those responsible for the management of risks and with appropriate expertise present at an appropriate frequency depending on the nature of the risk and the performance reported.

Risk Archive Management

To support strategic oversight and continuous improvement, the College will establish and maintain a Risk Archive to document risks that have been removed or closed.

The archive will include:

- Risk title and description
- Original and residual risk scores
- Closure rationale and date
- Responsible owner and mitigation history

The archive will be reviewed annually to identify risk movement trends, recurring themes, and areas of systemic vulnerability.

Archived risks may be reactivated if conditions change or new evidence emerges.

This archive will be maintained by the Director of Corporate Services and Development and reported to the Audit and Risk Assurance Committee as part of the annual assurance cycle. The template for Risk Archive Management is contained in **Appendix D**

Escalation and De-Escalation of Risks

Risk Owners should bring to the attention of the Principal for consideration of escalating a risk from an Operational / Divisional Risk Register to the Corporate Risk Register if any of the following circumstances apply:

- The risk becomes unmanageable;
- The residual risk is outside of the Risk Appetite boundaries agreed by the Governing Body;
- The risk has the potential to impact significantly on the achievement of a Strategic Objective;
- The risk remains very high after control measures have been implemented;
  The risk impacts on more than one Departmental area / project or programme.

A risk may be considered by the Governing Body for de-escalation from the Corporate Risk Register where it is decided that the risk rating has decreased significantly and is within the Governing Body's Risk Appetite in relation to the risk in question.

Irrespective of whether the risk is escalated for inclusion in the Corporate Risk Register, the risk should remain on the Operational / Divisional Risk Register for continued monitoring and action as required.

Roles and Responsibilities

Audit and Risk Assurance Committee and the Governing Body

Leading the assessment and management of risk is a role for the Governing Body, supported by the Audit and Risk Assurance Committee. The Corporate Risk Register will be reviewed at all Audit and Risk Assurance Committee and Governing Body meetings throughout the year at which assurance will be sought that all necessary controls are in place and these are operating effectively and that, where appropriate further action is being taken in a timely manner to manage risks to an acceptable level. Similarly, the Education Committee, Finance and General Purposes Committee and HR and Remuneration Committee will consider the Operational / Divisional Risk Registers in relation to the key areas reporting to the respective Committees on a regular basis. A record of these considerations will be contained within the Minutes.

The Principal and Senior Management

The Principal, with the support of Senior Management colleagues will be responsible for ensuring that the Risk Management Policy is implemented across the College and that it is embedded and operating effectively. Discussion on Risks will feature on the Agenda of all Senior Management Committees and will be recorded in the Minutes.

Senior Managers with cross-cutting responsibilities, may decide to maintain a Directorate Risk Register rather than individual Risk Registers within their area of responsibility, to ensure proper oversight of risks across different areas, while ensuring that risks continue to be managed at the appropriate level.

Departmental Heads

All Departmental Heads will be responsible for engaging with their staff to identify, assess and review risks on a regular basis and to ensure that the Operational / Divisional Risk Registers are up-to-date and used to inform discussion. A record will be kept of these discussions.

Departmental Heads will also be responsible for reporting those risks to the Principal that may require entry to the Corporate Risk Register. An audit trail of such discussions will be maintained.

Internal Audit

Internal Audit will, as part of its programme of reviews, provide annual assurance to the Governing Body on Risk Management and its effective implementation.

Appendix A

Example Risk Categories | The Orange Book

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

Governance risks – Risks arising from unclear plans, priorities, authorities and accountabilities, and / or ineffective or disproportionate oversight of decision-making and / or performance.

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

Legal risks – Risks arising from a defective transaction, a claim being made (including a defence to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets (for example, intellectual property).

Property risks – Risks arising from property deficiencies or poorly designed or ineffective / inefficient safety management resulting in non-compliance and / or harm and suffering to employees, contractors, service users or the public.

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

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

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

Technology risks – Risks arising from technology not delivering the expected services due to inadequate or deficient system / process development and performance or inadequate resilience.

Information risks – Risks arising from a failure to produce robust, suitable and appropriate data / information and to exploit data / information to its full potential.

Security risks – Risks arising from a failure to prevent unauthorised and / or inappropriate access to the estate and information, including cyber security and non-compliance with General Data Protection Regulation requirements.

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

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

Failure to manage risks in any of these categories may lead to financial, reputational, legal, regulatory, safety, security, environmental, employee, customer and operational consequences.

Appendix B

*Divisional / Corporate Risk Register

Risk Assessment Matrix

			IMPACT		
LIKELIHOOD	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
5 Almost Certain	M (5)	H (10)	H (15)	E (20)	E (25)
4 Likely	M (4)	M (8)	H (12)	H (16)	E (20)
3 Possible	L (3)	M (6)	M (9)	H (12)	E (15)
2 Unlikely	L (2)	M (4)	M (6)	M (8)	H (10)
1 Rare	L (1)	L (2)	M (3)	M (4)	H (5)

QUARTERLY RISK SUMMARY

Worked Example

Risk No.	Actual Impact on KPIs (To be reported every 6 Months)	Risk Statement	Inherent Assessment	Residual Assessment	In Quarter Change	Effectiveness of Controls
	Not / Unlikely to be Achieved 🔴 Likely to be Achieved but with some Delay 🟠 Achieved 🟢		Extreme 🔴 High 🟠 Medium 🟡 Low 🟢		Same → Higher ↑ Lower ↓	Very Good 🔵 Good 🔵 Weak 🟠 Insufficient ⚪
R 1	🟢	Theft of intellectual property, including fabrication or plagiarism of research or scholarly work could lead to	🟠	🟢	→	🔵

		loss of data, publications, funding and reputation.				

Risk Register: Worked Example:

1	2	3	4		5	6		7	8
Risk No	**Objective(s)**	**Risk**	**Assessment**		**Controls in Place**	**Assessment**		**Action Planned and Responsibility** **Target Date**	**Risk Owner**
			Inherent			Residual			
			Impact	Likelihood		Impact	Likelihood		
R1	**Aim 2:** to produce research publications of world-leading and internationally excellent standard	Theft of intellectual property, including fabrication or plagiarism of research or scholarly work could lead to loss of data, publications, funding and reputation.	**3**	**3**	- Regulations Governing the Allegation and Investigation of Misconduct in Research - Code of Ethics in Research - Research Office - Data Protection Policy - Disciplinary Procedure	**3**	**2**	• Policy Scoping Exercise • Training • Establishment of Working Group to develop policy and guidelines on Intellectual Property **By xx/xx/xxxx**	Director of Scholarship & Research

					- Regular review of Risk Register			**Director of Scholarship & Research/Other Post holder**	

Sources of Assurance – These should not rely solely on internal sources.

For example:

Quarterly Research and Scholarship Reports to the Education Committee of the Governing Body.

The outcome of Internal Audit reviews.

Confirmation of compliance with Codes of Practice.

Objectives In Full In Respect of Each Risk:

June 2025 I = 3, L = 2 **(M 6)**	March 2025 I = 3, L = 2 **(M 6)**	Jan 2025 I = 4, L = 3 **(H 12)**			

Risk Appetite Levels				
Adverse (A)	**Minimal (M)**	**Cautious (C)**	**Open (O)**	**Eager (E)**

The Risk Appetite assessment categories are as below:

- **Averse**; Avoidance of risk and uncertainty in achievement of key deliverables or initiatives is key objective. Activities undertaken will only be those considered to carry virtually no inherent risk.
- **Minimal**; Preference for very safe business delivery options that have a low degree of inherent risk with the potential for benefit/return not a key driver. Activities will only be undertaken where they have a low degree of inherent risk.
- **Cautious**; Preference for safe options that have low degree of inherent risk and only limited potential for benefit. Willing to tolerate a degree of risk in selecting which activities to undertake to achieve key deliverables or initiatives, where we have identified scope to achieve significant benefit and/or realise an opportunity. Activities undertaken may carry a high degree of inherent risk that is deemed controllable to a large extent.
- **Open**; Willing to consider all options and choose one most likely to result in successful delivery while providing an acceptable level of benefit. Seek to achieve a balance between a high likelihood of successful delivery and a high degree of benefit and value for money. Activities themselves may potentially carry, or contribute to, a high degree of residual risk.
- **Eager**; Eager to be innovative and to choose options based on maximising opportunities and potential higher benefit even if those activities carry a very high residual risk.

Appendix C

Risk Type (with associated impact)

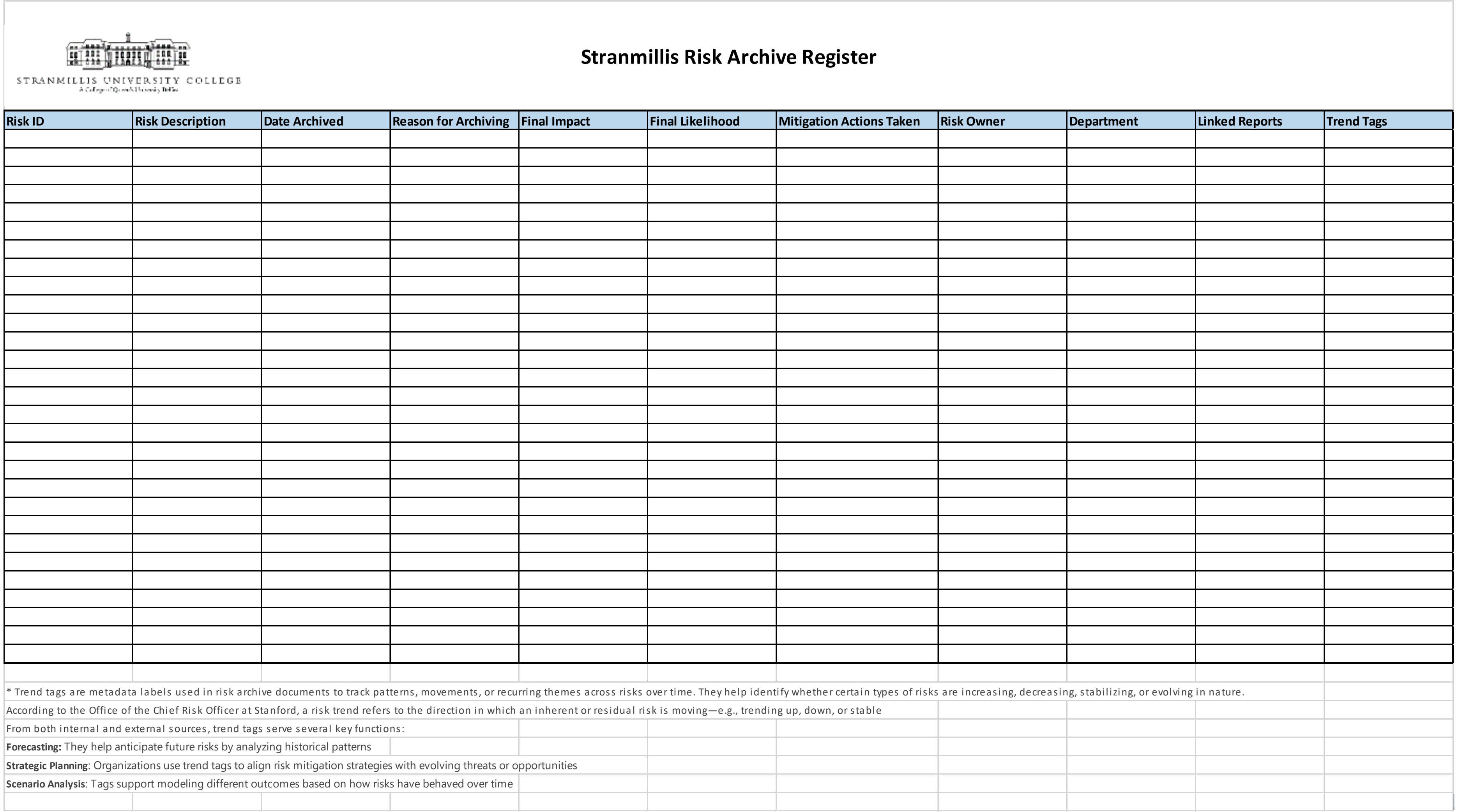
Impact	Impact on individual(s) – staff or public.	Statutory Duty.	Business / Operational	Buildings/ Engineering/ Environmental	Quality of Service	Finance
5 Catastrophic:	• Irreversible multiple injury or Death	• Multiple breach of statutory legislation and prosecution.	• Litigation > £500k expected. • National Media Interest • Severe loss of confidence and reputation	• Critical Environmental Impact. • Service closed for unacceptable period.	• Severe impact on customer satisfaction. • Gross failure to meet professional / national standards	• Significant financial impact (over 5% of total directorate budget) • Theft / loss >£250k
4 Major	• Major injury/ill health (reportable) • Major clinical intervention • Permanent incapacity	• Multiple breach of statutory legislation and improvement notice issued.	• Litigation >£250k to <£500k expected. • Adverse publicity • Impact on reputation	• Major/significant environmental impact • Severe disruption to service	• Major impact on customer satisfaction. • Failure to meet professional / national standards	• Major financial impact (between 2% - 5% of total directorate budget. • Theft / loss between £100k - £250k

3 Moderate	- Temporary Incapacity - Short term monitoring - Additional medical treatment up to 1 year - Extended hospital stay.	- Single breach of statutory legislation and Improvement Notice issued.	- Litigation >£50k - <£250k possible. - Potential for adverse publicity, avoidable with careful handling - Potential to impact on reputation.	- Moderate environmental impact - Moderate disruption to services	- Formal complaint expected. - Failure to meet internal standard	- Moderate financial impact (between 1% and 2% of total directorate budget) - Fraud/Theft / loss between £50k - £100k
2 Minor	- First Aid/ self-treatment - Minor injury - Minor ill health up to 1 month - Near miss (small cluster)	- Breach of statutory legislation.	- Litigation <£50k - Impact on reputation – internal awareness,	- Localised environmental impact - Disruption to service perceived as inconvenient	- Possible complaint. - Single failure to meet internal standard.	- Minor financial impact (up to 1% of total directorate budget) - Fraud/Theft / loss between £1k - £50k
1. Insignificant	- Near miss (single) - No adverse outcome - No injury or ill health	- Near breach of statutory legislation. - Minor breach of guidance or legislation.	- Possible litigation due to settlement is <£5k.	- Minimal impact to environment. - Minimal disruption.	- Customer initially unhappy. - Minor non-compliance with internal standard.	- Theft / loss up to £1k.

Likelihood Descriptor	**Probability /** Likelihood (of event or incident occurring over lifetime of Corporate Plan)
5 Almost Certain	The event is expected to occur.
4 Likely	The event is likely to occur.
3 Possible	There is a reasonable chance of the event occurring.
2 Unlikely	Not expected, but there is a slight possibility it may occur at some time.
1 Rare	The event will occur only in exceptional circumstances.

Prioritisation		
Colour	Timescale for action	Timescale for review
RED (Extreme)	Action immediately	Review within 1 month
AMBER (High)	Complete Action within 3 months where possible	Review within 3 months
YELLOW (Medium)	Complete Action within 6 months where possible	Review within 6 months
GREEN (Low)	Complete Action within 12 months where possible or accept risk	Review controls within period of corporate plan

Appendix D



STRANMILLIS UNIVERSITY COLLEGE
A College of Queen's University Belfast

Stranmillis Risk Archive Register

Risk ID	Risk Description	Date Archived	Reason for Archiving	Final Impact	Final Likelihood	Mitigation Actions Taken	Risk Owner	Department	Linked Reports	Trend Tags

* Trend tags are metadata labels used in risk archive documents to track patterns, movements, or recurring themes across risks over time. They help identify whether certain types of risks are increasing, decreasing, stabilizing, or evolving in nature.

According to the Office of the Chief Risk Officer at Stanford, a risk trend refers to the direction in which an inherent or residual risk is moving—e.g., trending up, down, or stable

From both internal and external sources, trend tags serve several key functions:

Forecasting: They help anticipate future risks by analyzing historical patterns

Strategic Planning: Organizations use trend tags to align risk mitigation strategies with evolving threats or opportunities

Scenario Analysis: Tags support modeling different outcomes based on how risks have behaved over time