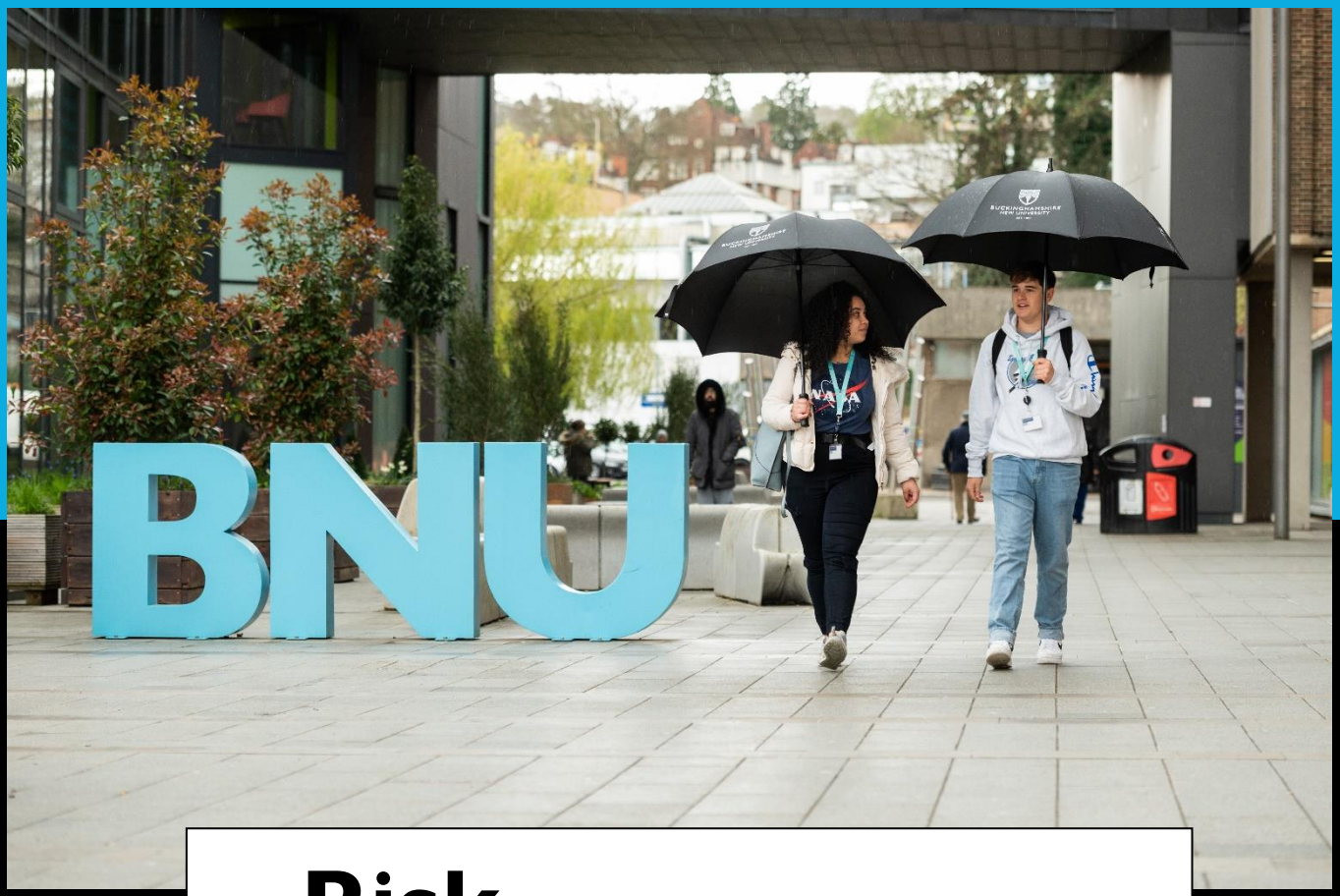
BUCKINGHAMSHIRE
NEW UNIVERSITY
EST. 1891



Risk Management Policy & Procedures

bucks.ac.uk

Contents

Approved by:	**Council**	**Date first published:**	**Jun-2013**
		Date updated:	**Sep-2025**
Owner:	**Director of Strategy, Transformation and Futures**	**Review Date:**	Sep-2028

This document has been designed to be accessible for readers. However, should you require the document in an alternative format please contact the Governance and Compliance team.

1. Overview

1.1 The purpose of this policy is to provide a framework for the effective management of risk across the University in pursuing its Mission, Vision, and Strategic Aims.

1.2 The objectives of the policy are to:

- Continuously enhance and develop the management of risk across the University,
- Ensure risk is managed proactively and supports University wide decision making
- Ensure the University's risk appetite is captured and risk profile is monitored, in accordance with best practice
- Create effective risk management processes that will allow the University to make annual risk management assurance statements with confidence.

1.3 This risk policy ("the policy") forms part of the institution's internal control and corporate governance arrangements.

1.4 The OfS states in its terms and conditions for funding HEIs that there should be effective arrangements for providing assurance to the governing body that HEIs have a robust and comprehensive system of risk management.

1.5 Risk arises where there is uncertainty of outcome and is anything that could impact on the University's ability to achieve its objectives. It can arise through direct threats, leading to a failure to achieve objectives, or through the failure to capture 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 part of best management practice.

1.6 The management of risk at multiple levels needs to be integrated so that the levels of activity support each other. In this way the risk management process of the University will be led from the top and embedded in the normal working routines and activities of the organisation. Risk management becomes an intrinsic part of the way business is conducted.

1.7 The management of risk has to be reviewed and reported on to Council for two reasons:

- to monitor whether the risk profile of the University is changing; and
- to gain assurance that risk management is effective, and to identify when further action is necessary.

1.8 Council needs a means of being assured that risk management is being implemented appropriately. The Audit Committee is responsible for appointing Internal Auditors to obtain this assurance, but it should be noted that the internal auditor is neither a substitute for management ownership of risk management nor a substitute for an embedded review system carried out by staff who have executive responsibility for the achievement of organisational objectives.

1.9 Staff should be aware of the relevance of risk to the achievement of their objectives and training to support staff in risk management should be made available. The policy provides a Guide to risk management, see Appendix 2.

1.10 This policy explains the roles and responsibilities of the Members of Council, the Audit

Committee, the University Strategy Group, Deans/Associate Deans/Directors of Colleges/Directorates, and other key parties. It also outlines key elements of the risk management process and identifies the reporting procedures.

1.11 This latest document builds on the progress made in the development of risk management at the University and its integration with the Business Planning and Performance Measurement indicators. It also reflects changes in the University's management structure introduced as part of the recent organizational change. The University has recategorized risk in to four separate types to enhance clarity, provide focus and support governance: 1. **Strategic Risks**, which impact institutional strategic objectives and are overseen by the Audit and Risk Committee; 2. **Operational Risks**, which affect day-to-day operational effectiveness and are reviewed by the University Strategy Group and Senior Leadership Teams; 3. **Project Risks**, which relate to project delivery and are managed within project teams, with escalation mechanisms in place where risks may impact strategic or operational areas; and 4. **Specialist Risks**, which are a collection of risks associated with compliance that will be monitored and report into the University Strategy Group

1.12 A number of supporting documents are available for information, guidance and re-assurance and are intended for employees and stakeholders. They are:

- Strategic Risk Register – see Appendix 1;
- Guide to Risk Management – guidance and information for all employees - see Appendix 2;
- Glossary of Terms – see Appendix 3; and
- Risk Management Process – guidance on the process - see Appendix 4.

2. Risk Appetite and Tolerance

2.1 In pursuing its Mission, Vision and Strategic Aims the University will assess the level of risk associated with its various activities. Council will determine the appropriate risk appetite for the University, what types of risk will be tolerated and monitor the risk profile of the University to ensure it remains within acceptable levels.

2.2 The University engages in a portfolio of activities, some of which are judged to be low or medium risk and others that are higher risk. There will be occasions when taking high calculated risks will be justified in terms of the benefits expected to accrue to the University. The University will manage the risk associated with individual activities through its risk management processes described in Appendix 4.

2.3 It is recognised as critical that the University preserves its reputation for high quality teaching and research, locally, nationally, and internationally. The University therefore has a low appetite for risk in the conduct of its activities that could put its reputation in jeopardy, could lead to undue adverse publicity or could lead to loss of confidence by its political or industrial partners and funders.

2.4 The University places high importance on compliance and will not knowingly commit breaches in statute, regulation, professional standards, research, commercial contracts or ethics, bribery, or fraud.

2.5 It is important to the University to maintain accreditations related to its courses or operations and does not wish to unwittingly put such accreditations at risk.

2.6 The University aims to maintain its long-term financial viability and its overall financial strength. It will not consider projects where they could lead to breaching its banking covenants or failing to meet its Financial KPIs (Income/Surplus/Debt).

2.7 Activities which are judged to be Exposed or High risk highlighted as Red within the risk profile map, see Appendix 4, should only be activities which are important to the University in achieving its objectives and will be undertaken only where they offer benefits commensurate with the level of net risk involved and do not increase risk to an unacceptable level i.e. where an adverse outcome would seriously jeopardise the overall achievement of the University's Strategic Objectives.

2.8 Where risks are either to be tolerated above the red risk line or where mitigating actions are taken to reduce risks significantly below this level the rationale must be documented in the relevant risk register and evidenced through the appropriate governance framework (e.g. through Programme/Project teams, College Leadership Teams, Directorates, USG or Council minutes), Where the net risk remains red on any risk register these must be reported to the Audit Committee. In a climate of high risk, the university may choose to focus and report solely on its gross risk to avoid misjudging the effectiveness of our mitigations.

2.9 There may well be instances where initiatives are considered to be of sufficient importance to the University to warrant an increased risk exposure. These will typically be opportunities where the university considers a more entrepreneurial approach is warranted or the external environmental changes. These risks will be subject to rigorous review and monitoring by the USG, including inclusion within the SRR and reporting to the Audit Committee and Council.

3. Roles and Responsibilities of the Council and its Committees

3.1 The role of Council is to:

- Ensure that risk management policies, procedures, methodologies, and tools are put in place with input from the Audit Committee and the USG and approve the University's Risk Policy.
- Oversee risk management within the University and its subsidiary companies and delegate part of this work, as appropriate, to the Audit Committee, see 3.2 below.
- Determine the appropriate risk appetite for the University and its subsidiary companies by determining the levels of risk that will be tolerated for each area of risk.
- Approve major decisions affecting the risk profile of the University and its subsidiary companies.
- Monitor the risk profile of the University to ensure it remains within an acceptable level.
- Ensure there is a risk assurance process in place to independently test whether the risk policies, procedures and related controls are functioning as intended.
- Review the Strategic Risk Register at least annually and the risk profile of the University at each of its meetings to satisfy itself that strategic risks are being actively managed in line with the policy.
- Review the annual report of the Audit Committee to Council and approve changes to the risk policy proposed by the Audit Committee.

3.2 The Audit Committee's responsibilities are:

- To monitor and review the effectiveness of risk management arrangements and, in particular, to review the external auditors' management letter, the internal auditors' annual report and management responses.
- Review the Strategic Risk Register at each of its meetings to understand any changes to risk ratings in order to monitor net risk and ensure risks are controlled within tolerance levels.
- Report to Council on the effectiveness of the risk management process and make recommendations to Council on any changes to the policy and processes.

Note: The Audit Committee should not itself own or manage risks and is, as with internal audit, not a substitute for the proper role of management in managing risk.

3.3 The Resources Committee's responsibilities are:

- When recommending core resource strategies and budgets provide an indication of the level of risk-taking or aversion that will inform the overall risk appetite and exposure that is determined by Council.
- Alert Council to any specific areas of concern in relation to strategic risks that arise from the work of the Resources Committee.

Note: Subsidiary companies will report to Council through their Boards of Directors on the effectiveness of their risk management processes, ensuring that all identified risks are being actively managed.

4. Roles and Responsibilities of the University Strategy Group

4.1 The University Strategy Group (USG) has ultimate responsibility for this policy and for ensuring that it is appropriately implemented throughout the University. The Vice-Chancellor has overall responsibility for risk management within the institution and this policy, and the Pro Vice-Chancellors, Deans of Colleges and Directors of Services are responsible for risk management and the policy's implementation within their areas of responsibility.

4.2 USG should manage the strategic risks of the University by:

- Identifying, evaluating, monitoring, and controlling the strategic risks faced by the University. The approved new list of strategic risk areas is provided with the full description of the risk and latest ratings within the Strategic Risk Register (SRR) in Appendix 1.
- Ensuring the process for updating the SRR is carried out effectively and in a timely way.
- Reviewing the SRR on a monthly basis to update its gross likelihood score to ensure that mitigating actions are controlling net risk within the tolerance levels for each risk and where this is not the case implementing additional mitigating actions in order to 'manage down' the likelihood of a risk occurring or reduce its impact to reduce net risk to within the tolerance levels for that risk.

4.3 SMT and USG should ensure that there is effective reporting of risks throughout the University and, through the Clerk to Council, ensure that the Strategic Risk Register is updated prior to, and is available in a timely manner, for Audit Committee and Council meetings.

5. Roles and Responsibilities of Deans of Colleges and Directors of Services/Directorates

5.1 Each Dean/Director will maintain a college/directorate's operational risk register. This will involve identifying, assessing, monitoring, and controlling the risks within their area of responsibility. The college/directorate's operational risk registers will be the subject of regular review (every 60 days) and discussion with USG line managers and between the Deans/Directors and Finance and HR business partners. Deans/Directors are responsible for ensuring that where a net risk rating is above the tolerance level for that risk this is escalated for the attention of the USG member (Strategic Risk owner) responsible with details of any further mitigating actions that are being put in place. The registers will be updated at regular intervals throughout the year and provided to Directorate of Strategy & Transformation.

5.2 The business planning and budgeting process is used to set objectives, agree action plans, and allocate resources to Schools and Directorates. The process of allocating operational resources and the approval of project and other capital bids requires identification and consideration of risks and controls. Progress towards meeting business plan objectives is monitored regularly. For major projects or areas of high or complex risk exposure, the compilation of a risk register may be necessary.

6. Roles and Responsibilities of Directorate of Strategy and Transformation (DrST)

6.1 Directorate of Strategy and Transformation (DrST) will maintain the University's Strategic Risk Register (SRR) and Specialist Risk Register and will be responsible for its update prior to review by the USG. To enable the update to take place, the owners of each risk and action leads will be responsible for providing any updates to their risk assessors on the mitigating actions. The risk assessors will also be responsible for discussing and agreeing with DrST any changes to the risk ratings; both likelihood and impact for gross (or raw) ratings and the same for net (residual) risk ratings taking account of the mitigating actions that have been implemented.

6.2 DrST will be responsible for identifying any matters shown on operational and project risk registers which could impact strategic risks in terms of their ratings. Where mitigating actions result in net risk which is not within the tolerance level for that risk the risk owner is responsible for identifying additional mitigating actions in order to 'manage down' the likelihood of a risk occurring or reduce its impact so as to reduce the net risk to within the tolerance levels for that risk. These additional actions will be clearly differentiated in the register until they have been implemented, at which point the ratings for the risk will be reassessed. Once this process is complete, the SRR will be reviewed by USG and a final version produced to reflect any changes arising from the review prior to submission to the Audit Committee.

6.3 The above procedure is followed in the case of Operational Risk Register and Project RAID Logs.

7. Risk Management Process

7.1 Deans and Directors will review the operational risk registers of Colleges and Directorates regularly and USG will review and report on strategic and specialist risks through their termly reporting cycle and provide an assessment of strategic risks to each meeting of the Audit Committee.

7.2 Subsidiary companies will report through their respective USG members.

8. BNU Risk Framework

Risk Registers				
	Strategic	**Operational**	**Project**	**Specialist**
Description	Risks affecting achievement of strategic objectives	Risks affecting day to day operations and KPI deliveries	Risks affecting delivery timelines and project objectives	Dedicated focus on niche/ expertise risks
Owner	USG	UMG assisted by SLT	Project Manager	Individual risk owners
Governance	Audit & Risk Committee	USG	Directorate of Transformation & Futures	USG
Frequency	Every 30 days	Every 60 days	Frequency as determined by project governance board	Every 30 days
Risk Areas	Financial Sustainability and Student Recruitment Regulatory and Compliance Reputation and Brand Infrastructure and Business Continuity	Student Experience (academic quality, support services) Teaching and Learning (curriculum delivery, regulations) Infrastructure and Facilities (campus safety and security, space utilisation) HR relations/Capacity Delivery – Delivery Capabilities (staffing shortages, workplace culture, training gaps) Financial Sustainability Governance and Compliance	Budget and Resource Scope, Delivery and Quality Stakeholder Engagement and Change Resistance Implementation Failures	Compliance and Accreditation Information Security Research and Development Equity, Diversity, and Inclusion Sustainability
Approach	Formal, structure, risk appetite levels embedded	Continuous monitoring, reliability on collaboration and feedback, quick adaptability to challenges, "Just Do It" mitigation approach	Stakeholder engagement, frequent reviews within teams and Demand board	Plan ahead & review at stages, defined timelines

Prepared by:	Risk and Business Officer & Head of Transformation	Date:	May 2025
Final Approval by:	Audit & Risk Committee, June 2025 Council, July 2025		
Review Date:	June 2028		

Appendix 1 Strategic Risk Register August 2025

Strategic Risks			
Impacts the **entire university** or multiple directorates	**Scale for Risk Rating** (Likelihood x Impact)	**Likelihood**	**Impact**
Threatens the university's mission, reputation, or long-term goals.	1 to 5 - Low	1. Very low	1. Very low
Could cause significant financial loss at the institutional level.	6 to 15 - Medium	2. Low	2. Low
Requires **executive or council-level decisions**.	16 to 20 - High	3. Moderate	3. Moderate
Risks **non-compliance** with governing regulations	21 to 25 - Exposed	4. High	4. High
Causes **widespread disruption** beyond one directorate (if cannot be captured in the Specialist risk register)		5. Very high	5. Very high

Risk Areas
Risk Area One: Financial Sustainability and Student Recruitment
Risk Area Two: Regulatory and Compliance
Risk Area Three: Reputation and Brand
Risk Area Four: Infrastructure and Business Continuity

Review Date: August 2025

STRATEGIC RISK REGISTER						
Risk	**Risk Owner**	**Risk Impact**	**Risk Likelihood**	**Risk Score**	**Risk Trend**	**Mitigation**
Risk Area One: Financial Sustainability and Student Recruitment						
Parent Risk 1: Failure to gain financial independence from partners There is a risk that the University's continued reliance on external partners for income generation may limit its financial autonomy and strategic flexibility, potentially undermining long-term financial sustainability.	**USG**	**4**	**4**	**16**	↑	1.Internationalisation recruitment strategy : Continue to pursue a strategic and considered expansion in the international student market, extra CAS allocations. 2.Use the Financial Independence Group to govern all financial independence plan projects 3.Analysis of the needs of our student personas 4.BNU flexible: launch a selection of evening and weekend course provision 5.BNU Online: Nine post graduate hybrid/online courses to be launched for September 2026 6.TNE : Expand transnational education avoiding high risk, high volume agreements 7.Review and optimise estate utilisation - an

						estates masterplan is a strategic initative and will be created. 8. Directorate reviews within the professional services
1.1 Failure to capitalise on growth markets There is a risk that BNU may not effectively identify, prioritise, or invest in emerging growth markets such as digital education, international student pathways, or degree apprenticeships. This could lead to missed opportunities for sustainable income diversification and reinforce reliance on existing, potentially less scalable partnerships.						
1.2 Inability to reduce cost base There is a risk that BNU's operational inefficiencies may constrain efforts to reduce the University's overall cost base. This could limit the ability to reallocate resources toward strategic priorities such as income diversification, digital innovation, and long-term financial independence from delivery partners.						
Risk Area Two: Regulatory and Compliance						
Parent Risk 2: Breach of OfS regulations from gaps in policies, governance, processes, and failure to adapt to regulatory changes. There is a risk that gaps in policies, governance, and processes, combined with a failure to respond effectively to changes in sector regulations, may lead to non-compliance, resulting in potential sanctions, reputational damage, and loss of funding for BNU.	**USG**	**5**	**4**	**20**	↔	1.Creation of partner quality framework 2. Continue to engage proactively and transparently with the OfS 3.Review and update institutional policies 4.Monitor and assure quality of external returns

2.1 Non-Compliance with statutory and regulatory returns There is a risk that inadequate data and reporting processes could cause late or inaccurate submission of statutory returns (HESA, OfS, SLC, Prevent Duty, etc.), leading to regulatory penalties, funding delays for the University. NB: Expect likelihood score to decrease over the next few weeks with mitigations. Ofs is recognising BNU shift in attitude towards retrospective failures						5. OBC Risk Oversight – Maintain ongoing monitoring of OBC risk, with the primary focus now transitioning to LLST. 6. Business Management Audit Outcome – Positive audit results indicate that the risk level is lower than originally assessed, reducing overall exposure. 7. Programme and VLE Compliance Audits – PVC (Academic) and PVC (Pedagogy) to undertake formal audits of programmes and the Virtual Learning Environment (VLE) to ensure compliance with Office for Students (OfS) standards. 8. VLE Implementation – Continue the phased implementation of the VLE as a targeted control measure to address compliance and quality assurance requirements. Project progressing well.
Risk Area Three: Reputation and Brand						
Parent Risk 3: Reputational damage from failure to manage risks associated with external collaborations and affiliations There is a risk that inadequate oversight, due diligence, or governance of external collaborations, affiliations, and commercial partnerships may lead to reputational harm, negatively affecting BNU's credibility, stakeholder trust, and ability to attract students, staff, and funding.	**USG**	**4**	**3**	**12**	↓	1.Proactive management of academic and commercial collaborations 2.Creation of new and enhanced due diligence processes for partnerships and initiatives to have robust assessment at every stage. Partner Quality framework was shared at Council and further being developed. 3.Leverage the employee forum to inform council appointments and some internal communications. Employee Forum keeps a live conversation going around any risks and opportunities from strategic decisions. 4. Press Office is 24/7 - some notable articles in WonkHE. Develop and deliver strong internal communications to pre-empt and manage media narratives
3.1 Inadequate oversight of external partnerships leading to reputational harm There is a risk that inadequate oversight and management of external partnerships and						

affiliations may lead to reputational harm for the University, impacting stakeholder trust and future collaboration opportunities.						
3.2 Insufficient due diligence on external partners causing reputational damage There is a risk that insufficient due diligence and ongoing management of external partners and affiliations could result in reputational damage, negatively affecting student recruitment, stakeholder confidence, and the University's standing in the higher education sector.						
Risk Area Four: Infrastructure and Business Continuity						
Parent Risk 4: Failure to ensure business continuity and resilient infrastructure There is a risk that inadequate planning, outdated infrastructure, or insufficient disaster recovery arrangements could disrupt BNU's critical operations and services, leading to prolonged downtime, loss of data, and negative impacts on staff, students, and stakeholders.	**USG**	**5**	**3**	**15**	↑	1.Continue to raise awareness about information security in the University - mandatory training and awareness campaign - a new course has been rolled out since previous register 2.Alternative comms channels in the event of an outage 3.Development of failover site at Aylesbury to protect data and increase BC/DR resilience 4.Student Record System project is underway and progressing well - Phase 1 near completion and identified areas of improvement needed 5.Roll out of a Security Operations Centre (SOC) service for monitoring the cyber threats

Appendix 2 Guide to Risk Management

What is risk management?

Though the Higher Education Funding Council for England (HEFCE) has been replaced by the Office for Students, HEFCE, in its circular 01/28 "Risk management - a guide to good practice for higher education institutions" still provides a useful framework for higher education institutions to understand approaches to risk management. The circular defined risk as "the threat or possibility that an action or event will adversely or beneficially affect an organisation's ability to achieve its objectives"..

This definition links risk to achieving the BNU's objectives and identifies that risk management is not just about recognising and mitigating a negative risk but also enables the identification of risk-taking opportunities that may lead to positive benefits.

Risks at BNU are identified as:

- Strategic Risks
- Operational Risks
- Project Risks and
- Specialist Risks

HEFCE defines risk management as "a process which provides assurance that objectives are more likely to be achieved; damaging things will not happen or are less likely to happen; and beneficial things will be or are more likely to be achieved."

The risk management method enables:

- the identification of risks
- the evaluation of risks
- the setting of acceptable risk thresholds/appetite level
- the identification and mapping of controls against those risks
- the identification risk indicators that give early warning that a risk is becoming more serious or 'crystallising'.

Where risks are identified and the current level of risk is assessed to be too high, internal ‘controls’ are used to reduce the risk level to one that we are able to tolerate.
Internal controls are a range of:

- strategies, regulations, procedures, policies and guidance that the University, Schools and Directorates use to govern their work.
- any additional controls or mitigating actions taken to deal with a particular situation.

The aim of risk management is to ensure that these controls are effective in identifying, monitoring, and controlling the risks the University faces in its day-to-day activities or any future ventures. What follows are a series of steps that are recommended as good practice in risk management, and which are already followed at a strategic level at the University.

Identify the risks and decide upon an appropriate management medium

This is where the range of risks that may affect a particular new activity, existing operational activity or projects is listed. These risks may be identified as part of an existing planning framework, using for instance

SWOT analysis, or within the project initiation phase. The subsequent management of these risks may also be developed as objectives and review within those plans. At a strategic level, risks are identified and managed using the format shown in Appendix 1 of this document.

Major capital projects should maintain a risk register and Colleges, Directorates and project managers also find this to be an appropriate medium. What is however important is that a method of identifying and managing risks is agreed in accordance with this policy and that the method used is appropriate to the structure, culture, complexity and criticality of the area or project concerned. Where there is doubt, a member of the Senior Management Team or Strategy and Transformation Team will be able to give advice.

Identify risk owners

Risk owners are individuals who assess and monitor a particular risk. Risk owners for those risks that affect the whole University level tend to be members of the University Strategy Group. At a college, directorate, or project level it will be necessary to determine where the risk lies, i.e. is it an operational/strategic/specialist risk or is it a risk that affects the whole college. It is then possible to identify who the risk owner should be. Risk owners should be identified in risk registers or other plans and documentation.

Evaluate the risks

Having identified the risks and the risk owner, the risk should then be evaluated for impact and likelihood and a guide is provided at the end of this document showing the scales used by the University Strategic Group in the strategic and specialist risk assessment (SRR, SpRR), where impact and likelihood range from 1 to 5, giving a maximum 'score' of 25 when these are multiplied together.

The same evaluation of risk takes place at college and directorate level for operational risks. For individual projects, RAID logs will be used and monitored by the Project Manager.

This is an appropriate method to assess the impact and likelihood of the risk emerging, and taking account of the level of risk exposure that the risk owner is willing to tolerate, but without the need to engage in a complex scaling of financial impacts that is applied in our strategic risk register.

A RAG (Red, Amber, and Green) rating can be used as an indication of the level of confidence that an action plan will meet its objectives, or in the case of an operational risk to indicate whether the risk is controlled at an acceptable level given the potential impact. This is a subjective assessment but can be validated on the basis of the assurances used by the area in making the assessment. A reasonable guide to the RAG system of assessment would be where:

- Red = Not on target to deliver objective or a risk of significance that is unacceptably high; additional actions, not yet fully planned, will be required to recover this and the position will need regular monitoring.
- Amber = Objective is not yet on track or risk is still not fully controlled, but actions are planned or underway that will recover or achieve that position.
- Green = On target to achieve this objective or control this risk with existing controls or actions.

Set acceptable levels of risk

The overall level of risk or 'exposure' that an organisation or part of an organisation is prepared to tolerate needs to be determined. This level may be different for different risks and the level may change depending

on circumstances. Once determined, risk thresholds provide triggers for action, changes in monitoring regime and can help determine what information is escalated to senior management or board level.

Identify suitable responses to risk (Risk Treatment)

During this stage a range of practical responses to each significant risk in the plan or the risk register should be identified. There may be a number of responses in each case.

There is a range of responses (controls) to a risk:

- Reduce or Treat: taking action to reduce either the likelihood of the risk crystallising further, or its impact.
- Accept or Tolerate: when the likelihood and impact are low producing a total risk score below 7, or when it would be too expensive to mitigate a risk.
- Transfer: transferring the risk to a third party, e.g. insurance.
- Terminate: identifying actions to eliminate the risk such as withdrawing from the activity.
- Contingency: having a plan of action to be implemented when a risk crystallises further or passes through a risk threshold or goes beyond the global threshold.
- Prevent: identifying measures to prevent a risk having an impact on an organisation.

What is most important is that the response should be proportional and suited to the risk.

Implement controls or actions

During this stage the most appropriate responses to each risk should be selected and implemented. The risks that have the highest priority should be dealt with first. Once implemented the responses should be monitored to see if there are any knock-on effects on other activities and amended as necessary. Responsibility for risks and the responses to risk should be clearly allocated in order to ensure the responses reduce the overall risk exposure. It should be noted here that the implementation of responses or controls may have financial costs and adequate resources should be made available.

Gain assurances about effectiveness – risk reporting

Having taken action or put controls in place, they should be monitored for effectiveness at a frequency that is suited to the risk exposure. Again, some guidance is provided in the risk scoring guide at the end of this document. Where other planning frameworks are used it may be that you are monitoring performance against target objectives that were originally identified within a SWOT analysis or risk identification session.

Clearly, where monitoring reveals that the situation has not improved, or indeed has worsened; additional actions or controls should be instigated. Conversely, monitoring may reveal an improvement and some or all controls may be relaxed accordingly.

Embed and review

Having gone through all the stages above the management of risk should become part of the way the organisation works, appearing in a range of planning, strategic, project and operational documents either explicitly or implicitly.

Risk management arrangements at the strategic level are reviewed and reported to Council on an annual basis including a review of the strategic risk register. Colleges and Directorates should consider their own arrangements on a similar basis, perhaps as part of their business planning process.

If you have questions or concerns in relation to risk management, please contact Strategy and Transformation, or a member of USG who will be happy to guide or assist you.

Guide to impact and likelihood scores.

Impact

Scale	Description	Definition
1	Very low	Will have little or no impact on achieving outcome objectives
2	Low	Will have a minor impact on achieving desired results, to the extent that one or more stated outcome objectives will fall below goals but well above minimum acceptable levels
3	Moderate	Will have a moderate impact on achieving desired results, to the extent that one or more stated outcome objectives will fall well below goals but above minimum acceptable levels
4	High	Will have a significant impact on achieving desired results, to the extent that one or more stated outcome objectives will fall below acceptable levels
5	Very high	Will have a severe impact on achieving desired results, to the extent that one or more of its critical outcome objectives will not be achieved

Likelihood

Scale		Description	Definition
1		Very low	Highly unlikely, but it may occur in exceptional circumstances. It could happen, but probably never will.
2		Low	Not expected, but there's a slight possibility it may occur at some time.
3		Moderate	The event might occur at some time as there is a history of casual occurrence at the University &/or similar institutions.
4		High	There is a strong possibility the event will occur as there is a history of frequent occurrence at the University &/or similar institutions.
5		Very high	Very likely. The event is expected to occur in most circumstances as there is a history of regular occurrence at the University &/or similar institutions.

Monitoring Guide

Total Score	Description	Definition
0 to 5	Low	Should not require much attention, but be reviewed annually
6 to 15	Medium	Should be monitored and reviewed on a quarterly basis
16 to 20	High	Should be monitored monthly and be reviewed on a quarterly basis
21 to 25	Exposed	Should be constantly monitored and reviewed monthly

Likelihood	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Impact				

Appendix 3 Glossary of Terms

Audit Committee	A committee appointed to support the Council in monitoring the corporate governance and control systems in the organisation including risk management.
Exposure	The consequences, as a combination of impact and likelihood, which may be experienced by the organisation if a specific risk is realised.
Gross or Raw Risk	The exposure arising from a specific risk before any (or Inherent Risk or Current Risk) action has been taken to manage it.
Internal Control	Any action, originating within the organisation, taken to manage risk. These actions may be taken to manage either the impact if the risk is realised, or the likelihood of the realisation of the risk.
Likelihood	The condition of being likely or probable; probability.
Monitoring Indicators	Any measure that tell us whether the mitigating actions are having the desired effect. e.g. KPIs
Net or Residual Risk	Also called Target Risk. The exposure arising from a specific risk after mitigating action has been taken to manage it and making the assumption that the action is effective. (Note this is reflected on the SRR as a Mitigated Risk Rating.)
Probability	The probability of something happening reflects how likely it is to happen, sometimes expressed as a fraction or a percentage, with 0 probability meaning the event is certain not to happen, and 1 meaning the event is certain to happen. 0.5 or 50% probability means the event is as likely to happen as not.
Risk	Uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. It is the combination of likelihood and impact, including perceived importance.
Risk Action Lead	The person responsible for implementing a mitigating action.
Risk Appetite and Tolerance	The amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time.
Risk Assessment	**T**he evaluation of risk with regard to the impact if the risk is realised and the likelihood of the risk being realised (See Gross Risk and Net Risk).
Risk Management	All the processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress.
Risk Management Assurance	An opinion, based on evidence gained from review of the effectiveness of an organisation's management of risk.
Risk Owner	The person who is ultimately responsible for managing the risk.
Risk Profile	The documented and prioritised overall assessment of the range of specific risks faced by the organisation.
Risk Trend	How the level of risk changed since the last assessment – increased, unchanged, decreased.

Appendix 4 Risk Management Process

The risk management process involves identifying, analysing, assessing, prioritising, managing, monitoring and reporting on risks. The approach to each step and the methods and tools used are described below.

1. Identification of Risks

The identification of risks is derived from both a 'top down' (USG) and a 'bottom up' (College and Directorate) process of risk assessment and analysis resulting in coverage of the whole University. The focus is on identifying 'key' or 'significant' risks that would impact on the achievement of key objectives. Risks can be identified by anyone, at anytime and anywhere and be put forward for evaluation.

2. Risk Analysis

The information that is gathered about the risk is analysed and a description of the risk produced to ensure a clear understanding of the root cause of the risk and consequences if it is realised.

3. Risk Assessment and Profiling

The evaluation of risk with regard to the impact if the risk is realised and the likelihood of the risk being realised. This is carried out using a 5x5 matrix using the following definitions:

Likelihood	Impact
1 Very Low	1 Very Low
2 Low	2 Low
3 Moderate	3 Moderate
4 High	4 High
5 Very High	5 Very High

A risk rating is then derived by multiplying the likelihood of the risk occurring by the impact of the risk if it is realised. The scale for the risk rating is then determined from the table below.

Scale for Risk Rating
1 to 5 - Low
6 to 15 - Medium
16 to 20 - High
21 to 25 - Exposed

Once the risk assessment is complete for all risks on a register then the ratings can be mapped onto a risk and tolerability matrix as illustrated below to show the risk profile. The following example is based on the SRR for August 2025 using the gross risk ratings.

BNU RISK PROFILE: GROSS RISK RATINGS **August 2025**						
Likelihood	5	5	10	15	20	25
	4	4	8	12	16 (Risk1)	20 (Risk 2)
	3	3	6	9	12 (Risk 3)	15 (Risk 4)
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
	Impact					

4. Risk Action Planning

For each risk a decision needs to be made as to whether to treat, transfer, terminate or tolerate the risk.

Treat – It is usually possible to mitigate a risk by 'managing down' the likelihood, the impact, or both. Any control measures must reflect the potential frequency, severity and financial consequences of the risk event. These risks are then managed through the development of appropriate risk mitigation plans. There is a requirement to measure progress with mitigating actions and to highlight to management when mitigating actions are off track.

Transfer – Some risks can be transferred to another body or University i.e. insurance, contractual arrangements, outsourcing etc. It is however important to note that some risks e.g. reputation can never be transferred.

Terminate – It may be able possible to eliminate a risk by ending all or part of a particular activity or project.

Tolerate – Some risks may have to be tolerated as they are inherent in the activity and cannot be treated, transferred or terminated. In addition there are some risks over which we can have no control and some for which any management actions would be prohibitive in terms of resource. The important point is that these risks are identified, are clearly understood and are acknowledged. If the risk is tolerated then the situation must still be monitored to make sure that the risk does not move beyond an acceptable level of likelihood or impact. Where a risk is beyond the management's control and has a high impact then a contingency plan should be created, e.g., a disaster recovery plan for IT to enable business continuity.

As part of the reporting process risk owners must escalate any risks that are rated red (Exposed) and where they exceed the agreed tolerance levels and no further mitigating action has been identified.

The USG member responsible for the area must then decide what action to take which may mean managing the risk directly and including the on the SRR/SpRR. This process will enable the movement of risks between risk registers so that risks are managed at the appropriate level.

Appendix 5: Equality Impact Assessment

1. What is changing and why?				
The Risk Policy was last updated in 2023 and the current revision contains management team name changes (USG instead of UET) and Directorate name changes. New categories of risks are identified and added along with their management i.e., Strategic, Operational, Specialist and Project Risks. along with their management. The rest of the text is exactly as it was before.				
2. What do you know?				
3. Assessing the impact				
	Could benefit	**May adversely impact**	**What does this mean?** *Impacts identified from what you know (actual and potential)*	**What can you do?** *Actions (or why no action is possible) to advance equality of opportunity, eliminate discrimination, and foster good relations*
a) How could this affect different ethnicities? *Including Gypsy, Roma, Traveller, Showmen and Boaters, migrants, refugees and asylum seekers.*	☐	☐	It will not affect anyone in this group differently from anyone in any other group. Managing risk in the University is equally beneficial to all.	
b) How could this affect cisgender and transgender men and women (including maternity/pregnancy impact), as well as non-binary people?	☐	☐	It will not affect anyone in this group differently from anyone in any other group. Managing risk in the University is equally beneficial to all.	
c) How could this affect disabled people or carers? *Including neurodiversity, invisible disabilities and mental health conditions.*	☐	☐	It will not affect anyone in this group differently from anyone in any other group. Managing risk in the University is equally beneficial to all.	
d) How could this affect people from different faith groups?	☐	☐	It will not affect anyone in this group differently from anyone in any other group. Managing risk in the University is equally beneficial to all.	

e) How could this affect people with different sexual orientations?	☐	☐	It will not affect anyone in this group differently from anyone in any other group. Managing risk in the University is equally beneficial to all.	
f) How could this affect different age groups or generations?	☐	☐	It will not affect anyone in this group differently from anyone in any other group. Managing risk in the University is equally beneficial to all.	
g) How could this affect those who are married or in a civil partnership?	☐	☐	It will not affect anyone in this group differently from anyone in any other group. Managing risk in the University is equally beneficial to all.	
h) How could this affect people from different backgrounds such as: socio-economic disadvantage, homeless, alcohol and/or substance misuse, people experiencing domestic and/or sexual violence, ex- armed forces, looked after children and care leavers.	☐	☐	It will not affect anyone in this group differently from anyone in any other group. Managing risk in the University is equally beneficial to all.	
i) How could this affect people with multiple intersectional experiences?	☐	☐	It will not affect anyone in this group differently from anyone in any other group. Managing risk in the University is equally beneficial to all.	

4. Overall outcome				
No major change needed ☒	Adjust approach ☐	Adverse impact but continue ☐	Stop and remove ☐	
5. Details of further actions needed				
None				
6. Arrangements for delivery and future monitoring				
None				
7. EIA Completed by:	Jeeva Jacob	Risk and Business Officer	**Date**	**20/05/2025**
8. Signed off by:	Sandy Gill	Head of Transformation	**Date**	**12/06/2025**