



Risk Management Policy

Policy owner:	Registrar & Chief Administrative Officer
Implementation date:	September 2024
Review date:	August 2025
Related policy:	Business Continuity, Interruption and Major Incident Plan

Contents

1.	Introduction	2
2.	Scope	2
3.	Legislative Context	2
4.	Definitions	2
5.	Responsibilities	3
6.	Risk Registers	5
7.	Risk Nomenclature	5
8.	Risk Assessment	7
9.	Risk Appetite	8
10.	RAID Log	8

Version History

Version	Approved by	Revisions made	Date
1	ARC	Full review and re-write	1 September 2024



1. INTRODUCTION

- 1.1 The University of Buckingham is committed to ensuring that it has a comprehensive and robust system of risk management that enables the University to identify obstacles to key objectives and to establish ways of avoiding unnecessary risk and/or mitigating the impact of adverse events that cannot be otherwise avoided.
- 1.2 Risk management encompasses the methods and processes used by the University to take and manage risks in the context of its Strategic Plan. In order to achieve this, the University identifies risks and opportunities related to its overall academic and related business objectives, assess them in terms of likelihood and magnitude of impact, determines a response and monitors progress.
- 1.3 Effective risk management is, therefore, of strategic importance in protecting the reputation and sustainability of the University. It is a university-wide operation and is key to the achievement and implementation of the University's strategic ambitions.
- 1.4 Effective risk management does not entail the elimination of all risk; instead, it is used to inform business decisions and aid successful operations.

2. SCOPE

- 2.1 This policy forms part of the University's internal control and governance arrangements and applies to all staff.

3. LEGISLATIVE CONTEXT

- 3.1 In accordance with the Higher Education and Research Act (2017), the Office for Students' *Regulatory Framework* Conditions of Registration E1 and E2 require the University to uphold, through its governing instruments (E1) and its practices (E2), the public-interest principle that the University operates comprehensive corporate risk management and control arrangements (including for academic risk) to ensure the sustainability of the provider's operations, and its ability to continue to comply with all of its conditions of registration.

4. DEFINITIONS

- 4.1 Risk is the possibility that an action or event will adversely affect the University's ability to meet its objectives.
- 4.2 Opportunity is the possibility that an action or event will beneficially affect the University's ability to meet its objectives.
- 4.3 Risk management is the process by which risks are identified, assessed, prioritised and managed in order to support well-informed decision-making and maximise the realisation of opportunities across the University.



- 4.4 Gross risk is risk that is known or believed to be present before any mitigation measures have been applied.
- 4.5 Net risk (sometimes called residual risk) is any risk that remains after mitigation measures have been applied.
- 4.6 Inherent risk is risk that will always be present despite mitigation measures having been applied.
- 4.7 Risk appetite is the level of risk that the University is willing to pursue or retain in the management of risks and the pursuit of opportunities.

5. RESPONSIBILITIES

5.1 Council

- 5.1.1 In accordance with Article 5 of the University's Royal Charter and Power 4.13 of the Scheme of Delegation, the Council is charged with ensuring the provision of a system for risk management and control.
- 5.1.2 Statute 16.3(c) and Power 7.1 of the Scheme of delegation empower the Council to be the University's legal authority and, as such, to ensure that the University upholds its legal rights and fulfils its legal responsibilities.
- 5.1.3 Pursuant to risk management, the University's legal responsibilities include adherence to the Office for Students Conditions of Registration E1 and E2, which require the University to uphold, through its governing instruments (E1) and its practices (E2), the public-interest principle that the University operates comprehensive corporate risk management and control arrangements (including for academic risk) to ensure the sustainability of the provider's operations, and its ability to continue to comply with all of its conditions of registration.
- 5.1.4 Council will review the University's risk management framework and Risk Register on an annual basis.
- 5.1.5 The Council has delegated the responsibility for the routine review of the University's risk management framework and Risk Register to the Audit and Risk Committee.

5.2. Audit and Risk Committee

- 5.2.1 In accordance with Power 4.13 of the Scheme of Delegation, the Audit and Risk Committee (ARC) is delegated the responsibility for ensuring the provision of a system for risk management and control. ARC will report to Council on business operations and advise the Council of any emerging concerns.



5.2.2 The University's risk management framework and Risk Register will be considered by ARC at least quarterly. In doing so, the ARC will scrutinise and evaluate the management of risk and make a recommendation to the Vice-Chancellor and Registrar as to whether the Risk Register and associated actions are appropriate.

5.3. Executive Group

5.3.1 The Executive Group will consider strategic, academic and non-academic risks across the University and maintain oversight of risk management operations. They will review the University's Risk Register at least quarterly.

5.4. Compliance and Risk Steering Group

5.4.1 The Compliance and Risk Steering Group monitors and oversees the university's risk management, audit and business continuity plans on a day-to-day basis, championing their implementation and alignment to strategic aims.

5.4.2 The group reports directly to the Executive Committee and is responsible for number of sub-groups including, the Health and Safety Committee, the Visa Compliance Working Group, the Prevent Working Group and the Data Governance Group.

5.5 Deans and Heads of Department

5.5.1 The role of the Dean or Head of Department is to maintain and monitor a local Risk Register and apply good risk management practice within their management purview.

5.5.2 Where new risks are identified at local level, the relevant Dean or Head of Department is responsible for determining any need to escalate to the University Risk Register in consultation with the Compliance and Risk Steering Group..

5.6 Risk Owners

5.6.1 A Risk Owner can be any member of university staff assigned as such through the University's Risk Registers.

5.6.2 Risk Owners must monitor and manage the risk(s) assigned, liaising with colleagues as appropriate, and taking action to mitigate the effects.

5.6.3 Risk Owners should be aware of the current risk environment and record any change or new risk in the relevant Risk Register liaising with their Dean or Head of Department, or the Compliance and Risk Steering Group, as appropriate.



5.7 Internal Auditors

- 5.7.1 The University's Internal Auditors offer impartial and independent assurance regarding the University's risk management, governance, and internal control processes, ensuring they are appropriately structured and functioning effectively.

6. RISK REGISTERS

- 6.1 Risks that are considered germane to the University's strategic objectives and/or could impact its ability to operate effectively are identified in the University Risk Register.
- 6.2 Council will receive and scrutinise the University Risk Register annually.
- 6.3 ARC will receive and scrutinise the University Risk Register at each meeting and will be responsible for updating Council accordingly.
- 6.4 Each of the University's Faculties and Directorates are required to maintain a local Risk Register. Local Risk Registers will be scrutinised regularly by the Compliance and Risk Steering Group and be available to the ARC for review.
- 6.5 Where new risks are identified at local level, the relevant Dean or Head of Department is responsible for determining any need to escalate to the University Risk Register in consultation with the Compliance and Risk Steering Group.
- 6.6 For the University's Risk Register template, please see Appendix 1.

7. RISK NOMENCLATURE

- 7.1 Risks should be recorded in the applicable Risk Register(s) in accordance with the following schema.

7.2 Risk Identifier

- 7.2.1 An alphanumeric code of three components where component 1 = a letter to identify the department or area, component 2 = a letter to identify the risk category and component 3 = the number of the risk.

7.3 Risk Category

- 7.3.1 A single word description identifying the nature of the risk. The University's designated risk categories are: Strategic; Market; Financial; Academic; Student Experience; Compliance & Legal; Estates & Infrastructure; Data; Human Resources; Management; Operational; Projects; Reputational. Where risks fall into multiple categories, risk owners can use their discretion to determine the most applicable categorisation in consultation with the Compliance and Risk Steering Group.



7.4 Risk Description

7.4.1 A generic description of the risk as might apply to all universities.

7.5 (Gross) Likelihood

7.5.1 An assessment of the current potential likelihood of the risk – without controls – using the Risk Assessment Matrix as a guide to scoring.

7.6 (Gross) Impact

7.6.1 An assessment of the current potential impact of risk – without controls – using the Risk Assessment Matrix as a guide to scoring.

7.7 Gross Risk

7.7.1 A multiplication of likelihood and impact.

7.8 Risk Controls

7.8.1 The strategies, policies, procedures and processes in place to manage the risk.

7.9 Risk Owner

7.9.1 For the University Risk Register, the risk owner must always be a member of the Executive Group; for local Risk Registers, risk ownership may be delegated to line managers as appropriate.

7.10 (Net) Likelihood

7.10.1 An assessment of the current likelihood of the risk – with existing controls – using the Risk Assessment Matrix as a guide to scoring.

7.11 (Net) Impact

7.11.1 An assessment of the current potential impact of risk – with existing controls - using the Risk Assessment Matrix as a guide to scoring.

7.12 Net Risk

7.12.1 A multiplication of likelihood and impact.

7.13 Change since last review

7.13.1 An arrow to indicate the direction of travel. If this is a new risk, remove the arrow and type "N/A - NEW RISK".



7.14 Actions

7.14.1 The strategies, policies, procedures and processes that need to be put in place (or refined if they are already in place) to better manage the risk.

7.15 Deadline

7.15.1 The timescale within which the actions must be taken, RAG rated to show progress.

7.16 Risk Appetite

7.16.1 An assessment of the level of risk the University is willing and able to accept – using the Risk Appetite Matrix as a guide to scoring.

8. RISK ASSESSMENT

8.1 Risks should be assessed for likelihood and impact in accordance with the following matrix:

		IMPACT					
LIKELIHOOD		Very little impact on operations	Some impact on operations	Operations will be impacted to an extent	Significant impact on operations	Existential / catastrophic impact on business operations and delivery of objectives	
		1	2	3	4	5	
	Almost Certain	5	5	10	15	20	25
	Highly Likely	4	4	8	12	16	20
	Likely	3	3	6	9	12	15
	Possible	2	2	4	6	8	10
	Rare	1	1	2	3	4	5

Figure 1: Risk Assessment Matrix

9. RISK APPETITE

9.1 The University recognises that it is neither possible nor desirable to avoid all risk and that substantial organisational benefits may flow from a balanced approach to assessing the anticipated benefits and the potential scale or likelihood of harm. The University is cognisant of the value of continuing to pursue activities that entail risk where this is accepted as part of achieving its strategic ambitions, albeit subject to heightened due diligence and scrutiny.



- 9.2 The University is likely to maintain a high appetite for risk in matters of freedom of speech, academic freedom, critical inquiry, open debate and progressive as well as strategic growth provided that suitable and proportionate measures to mitigate the impact and likelihood of any potential risks in these areas are implemented.
- 9.3 The University is likely to maintain a low appetite for risk in situations where there exists a potential for significant and enduring reputational harm as a result of non-compliance with regulation, substantial and enduring impairment to its research or teaching endeavours, considerable financial loss or significant deviations from financial projections, loss of life or harm to students, staff or other stakeholders and/or involvement in illegal or unethical activities.
- 9.4 The University's approach to risk appetite should be assessed in accordance with the following matrix:

APPROACH TO RISK	DESCRIPTOR		
	Driven	5	High risk, high reward approach where innovation is key
	Open	4	All options considered with the one deemed to be most likely to succeed selected
	Cautious	3	'safe' option with limited reward
	Minimal	2	'very safe' option with minimal reward
	Averse	1	Object is to avoid risk

Figure 2: Risk Appetite Matrix

9.5

10. RAID LOG

- 10.1 Supplementing the University's Risk Registers, RAID logs are utilised for the purpose of logging, documenting and tracking the risks, assumptions, issues and dependencies inherent in the management of a particular domain or project.
- 10.2 For the purposes of developing and maintaining the University's RAID Logs, entries should be recorded in accordance with the following schema.

10.3 Risk

- 10.3.1 A risk is an exposure to an uncertain future event that may impact delivery. The University's RAID Logs capture risk categories from the applicable Risk Register and assign them to one or more of the issues arising.



10.4 Assumption

10.4.1 An assumption is a supposition that a piece of information is true, because there is no evidence at hand that shows otherwise. Assumptions should be regularly tracked and reviewed, with risks, issues, dependencies and actions updated as they ebb and flow over time.

10.5 Issue

10.5.1 An issue is a problem that has occurred (or is occurring) and needs to be clearly identified. It may affect the domain or project in various ways, such as delaying progress, adding complexity, requiring additional resources and generating risk. Issues should be regularly evaluated for their severity and impact and tracked as to how they are being managed and resolved.

10.6 Dependency

10.6.1 A dependency is a related item that is required to be in place in order for actions against identified issues to be proceed unimpeded. Dependencies should be regularly tracked, and actions updated as they ebb and flow over time.