

Risk management policy and procedure

1 Scope

- 1.1 This policy and procedure is a corporate policy and applies to:
- 1.2 All employees of the University of Northampton
- 1.3 Members of the University's Board of Governors
- 1.4 Directors and employees of the University's wholly-owned subsidiary companies
- 1.5 Whilst the University expects its employees and staff to comply with this policy, it does not confer contractual rights or form part of any contract of employment and may be amended or replaced at any time

2 Purpose

- 2.1 The ultimate purpose of this policy and procedure is to help the University achieve its strategy and objectives, improve performance and make sound decisions. The further purposes are:
- 2.2 To set the requirements for how risk is managed by the University
- 2.3 To describe how risks are identified, assessed, responded to, monitored and reported
- 2.4 To promote awareness of risks and risk management
- 2.5 To provide assurance to the Board of Governors about the effective management of risk

3 Definitions

- 3.1 Risk: an uncertain event or factor that can affect the achievement of business objectives. It will have an impact on the University for example in terms of financial performance, brand and reputation, or ability to do business. The impact of a risk can be positive or negative
- 3.2 Risk appetite: the amount of risk the University is willing to seek or accept in pursuit of its strategy
- 3.3 Risk management: systematic process of identifying, assessing, and mitigating risks
- 3.4 Control/controls: any process, policy, device, practice, or other action that modifies risk

4 Policy statement

- 4.1 This policy statement sets out the requirements for risk management at the University
- 4.2 **Strategic alignment:** Identifying and managing risk is an ongoing process linked to achieving the University's strategy and objectives
- 4.3 **Accountability from the top:** The Board of Governors is responsible for ensuring that a sound system of risk management is in place and is maintained. The Board determines the University's overall risk appetite and the risk appetite for individual issues the Board judges significant
- 4.4 **Leadership:** All members of the University Leadership Team (ULT) are responsible for ensuring that this policy and procedure is adopted, and that appropriate time and resource is made available to support ongoing risk management activity in their respective areas
- 4.5 **Ownership:** All risks have an owner who is responsible for proactive engagement with the management of the risk. Faculties and Professional Services own their risks and are responsible for consistently performing

their own risk identification, assessment, monitoring, reporting, and risk management activities

- 4.6 **Review:** Local risk registers are reviewed quarterly. There is a regular University-wide consolidation and review by ULT of the risks escalated to it. Ad hoc reviews are conducted when internal or external developments warrant
- 4.7 **Consistency:** Risks must be assessed using the criteria provided in this document. This facilitates the consolidation of risk information at University level. Consistent tools and templates provided by the Governance, Compliance and Risk team are used across the University
- 4.8 **Driving improvement:** For each risk it reviews, ULT monitors the status of the risk and progress against actions identified to improve controls
- 4.9 **Transparency and openness:** Risks must be reported and escalated in accordance with this policy and procedure
- 4.10 **Effectiveness review:** The Audit and Risk Committee is responsible for reviewing the effectiveness of the University's approach to risk management

5 Risk governance

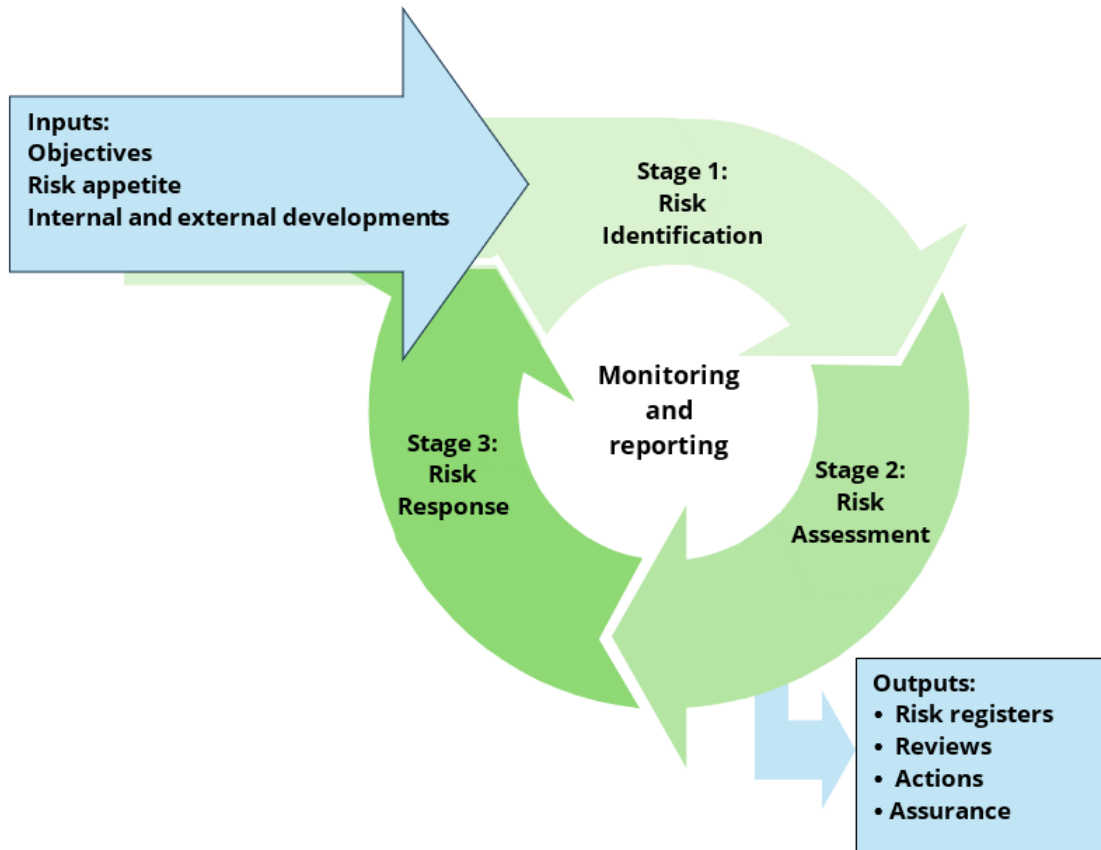
- 5.1 'Risk governance' describes the structure and accountabilities that support the development and implementation of risk management. Risk governance ensures that there is accountability for risk management and appropriate transparency of risk
- 5.2 Risk management is a both a 'top down' and a 'bottom up' process. It is described in brief below and in detail in sections 7 to 15
- 5.3 Local risk registers are used for departments to identify and assess risk. Local risk registers are reviewed regularly. The results of local reviews are collated by the Governance, Compliance and Risk team and reviewed

by the University Leadership Team (ULT)

- 5.4 ULT discusses risk regularly, both by discussing the University-level risk register and as part of its ongoing consideration of University business. ULT as a group, and its individual members, are expected to identify risks and raise these for assessment and response
- 5.5 Each risk has an identified owner. Risks on the University risk register are owned by a member of the University Leadership Team and this responsibility cannot be delegated
- 5.6 ULT reports on risk to the Audit and Risk Committee and the Board of Governors

6 Risk management procedure overview

- 6.1 The inputs are:
 - 6.1.1 Objectives
 - 6.1.2 Risk appetite
 - 6.1.3 Internal and external developments
- 6.2 There are three elements of monitoring and reporting:
 - 6.2.1 Stage 1 is risk identification
 - 6.2.2 Stage 2 is risk assessment
 - 6.2.3 Stage 3 is risk response
- 6.3 The outputs are:
 - 6.3.1 Risk registers
 - 6.3.2 Reviews
 - 6.3.3 Actions
 - 6.3.4 Assurance
- 6.4 The following graphic illustrates the risk management procedure described above.



7 Inputs to the risk procedure

- 7.1 Objectives: Risk should be considered in relation to achieving objectives. These include the University's strategic objectives and the objectives of individual functions. This ensures that risk is linked to performance
- 7.2 Risk appetite: This helps to frame the way we approach and respond to risks. It must be considered when deciding the approach to a risk response and individual mitigation actions. The Board of Governors has ultimate responsibility for determining risk appetite.
- 7.3 Internal and external developments: These may impact the seriousness of risks and influence mitigation strategies

8 Risk identification (Stage one)

- 8.1 The first stage of the risk procedure is the identification of potential risks, which are the uncertain events or issues that could impact the achievement of business objectives
- 8.2 Risk identification is a continual process, which is embedded in our ongoing operations. It critical to the achievement of our objectives. By increasing our awareness of the risks we face, we will be better placed to address them proactively
- 8.3 All types of risks should be considered, including those with high impact but low probability
- 8.4 For risk identification and all subsequent stages of the process, the online risk register provided by the Governance, Compliance and Risk team must be used. This ensures that the key information is documented. Use of a consistent template ensures that risk management is University-wide and risks can be escalated and deescalated appropriately

9 Risk assessment (Stage two)

- 9.1 The aim of risk assessment is to prioritise risks and identify those that require further management attention. This is done by using risk assessment criteria to assess the severity of the risk, producing a risk score
- 9.2 The University's risk impact scores are as follows:

9.3 Financial impact

Financial impact is an assessment of impact on operating profit over a 4-year period. These scores are used for reporting at ULT and Board level. Where these

values are too high for a business area, it may be appropriate for lower values to be used for in business area risk reporting. Please liaise with the Governance, Compliance and Risk team to develop and document these.

Financial scores and impacts in £'000 are as follows:

- 1: <£300k
- 2: £300K - <£500K
- 3: £500K - <£1m
- 4: £1m - <£5m
- 5: More than £5m

This information is also represented in the table below:

Score	Impact in £'000
1	<£300K
2	£300K - <£500K
3	£500K - <£1m
4	£1m - <£5m
5	More than £5m

9.4 Reputation

Reputation scores and impacts are as follows:

- 1: Internal – defined as 'Internal - minor impact on stakeholders within UON'
- 2: Intra-group – defined as 'Internal - major impact on stakeholders within UON'
- 3: Local third party - defined as 'External – Impact on local stakeholders'
- 4: National - defined as 'External – Impact on national stakeholders'

5: International - defined as 'External – Impact on international stakeholders'

This information is also represented in the table below:

Score	Description	Definition
1	Internal	Internal – minor impact on stakeholders within UON
2	Intra-Group	Internal – Major impact on stakeholders within UON
3	Local Third Party	External – Impact on local stakeholders
4	National	External – Impact on national stakeholders
5	International	External – Impact on international stakeholders

9.5 Likelihood

- 1: Remote. Frequency of occurrence = <Once in 20 years. Probability of occurrence = <10% chance
- 2: Less likely. Frequency of occurrence = <Once in 15 years. Probability of occurrence = >10% chance and <40% chance
- 3: Equally likely as unlikely. Frequency of occurrence = <Once in 10 years. Probability of occurrence = >40% chance and <60% chance
- 4: More likely. Frequency of occurrence = <Once in 5 years. Probability of occurrence = >60% chance and <90% chance
- 5: Almost certain. Frequency of occurrence = One or more a year. Probability of occurrence = >90% chance

This information is also represented in the table below:

Score	Description	Frequency of occurrence	Probability of occurrence
1	Remote	<Once in 20 years	< 10% chance
2	Less likely	<Once in 15 years	>10% and <40% chance
3	Equally likely as unlikely	<Once in 10 years	>40% and < 60% chance
4	More likely	<Once in 5 years	>60% and <90% chance
5	Almost certain	One or more a year	>90% chance

Therefore, the following risk scores are possible:

- 1 – 6
- 8 – 10
- 12
- 15
- 16
- 20
- 25

This is also represented in the table below:

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

9.6 Part of risk assessment is documenting the existing controls to manage the risk, its potential impact and the likelihood of it occurring

9.7 Control opinions are assessed as follows. 'Effective' in this context means that risk is being managed to the agreed level

- Good: Effective control framework assessed and agreed, proportionate to the risk. All required controls are fully in place and appropriately tested on an ongoing basis
- Satisfactory: Effective control framework assessed and agreed, proportionate to the risk. All required controls are generally functioning as intended but some changes necessary to achieve the appropriate level of control. Control weaknesses are relatively minor and not urgent
- Improvement: Effective control framework assessed and agreed, proportionate to the risk. All required controls are not functioning as intended and need to be improved to achieve the appropriate level of control. Control weaknesses are serious and require urgent resolution
- Unsatisfactory: Effective controls have not been agreed and/or established and/or are not functioning as designed. Control weaknesses are significant and must be resolved with high priority

This information is also represented in the table below:

Good	Effective control framework assessed and agreed, proportionate to the risk. All required controls are fully in place and appropriately tested on an ongoing basis
Satisfactory	Effective control framework assessed and agreed, proportionate to the risk. All required controls are generally functioning as intended but some changes necessary to achieve the appropriate level of control. Control weaknesses are relatively minor and not urgent
Improvement	Effective control framework assessed and agreed, proportionate to the risk. All required controls are not functioning as intended and need to be improved to achieve the appropriate level of control. Control weaknesses are serious and require urgent resolution
Unsatisfactory	Effective controls have not been agreed and/or established and/or are not functioning as designed. Control weaknesses are significant and must be resolved with high priority

9.8 Alongside controls, sources of assurance are also be documented in the risk register. Separate guidance is available on identifying and documenting sources of assurance

10 Risk response (Stage three)

10.1 Having assessed the severity of the risk, this stage considers whether the current level of risk is acceptable or whether further actions are required to manage the risk

10.2 If further action is required, clear actions with action owners and due dates must be agreed

10.3 The target risk score must be documented. The target risk score is the acceptable score for an individual risk. The target risk score must be

appropriate with regards to the University's stated risk appetite as set by the Board of Governors

11 Monitoring and reporting

11.1 The key parts of the University's ongoing monitoring and reporting of risk are:

11.1.1 Risk registers

11.1.2 Risk reviews

11.2 These are outlined in sections 12 and 13 below.

12 Risk registers

12.1 Having worked through the three stages described above, the risk register is the principal output. Risk registers are the University's means of documenting, managing and monitoring risk. They provide evidence of our risk management activities and a source of reporting about risk

12.2 The University has an overall strategic risk register, and local risk registers

12.3 The strategic risk register is focused on the identification and management of 'game changing' strategic and operational risks to the University

12.4 Each faculty and professional service must hold a local risk register

12.5 Local risk registers may also be kept where the risks do not sit under a particular faculty or professional service, for example a cross-University project or change programme

13 Risk reviews

13.1 Risk reviews are carried out in accordance with a calendar issued by the Governance, Compliance and Risk team

Local risk register reviews

- 13.2 The Dean or Director is responsible for ensuring that a review of the local risk register takes place at least each quarter. Where there are significant changes, a more frequent review is expected in response. This will help to ensure that the University level risk register is up to date
- 13.3 Local risk register reviews should normally take place via a meeting. Where risks have cross-university significance or themes, it may be appropriate to carry out the review through a suitable committee, for example the Health, Safety and Security Committee could review the health and safety risk register. For other risk registers a departmental or management meeting will be more suitable
- 13.4 Local risk register reviews must consider:
- 13.5 Whether all risks that 'keep you awake at night' are appropriately captured
- 13.6 Whether any risk must be escalated to ULT in accordance with the escalation criteria set out in section 15 below
- 13.7 Whether a risk can be removed from the local risk register
- 13.8 Alignment with the University's risk appetite
- 13.9 Risk register reviews must involve the relevant Dean or Director and must be approved by them
- 13.10 Risk register reviews must be documented. The following must be flagged:
- 13.11 New risks
- 13.12 Changes since the previous review
- 13.13 Misalignments or potential misalignments between risk appetite and risk score
- 13.14 Risks for escalation to the ULT risk register
- 13.15 Risks deescalated or closed since the last review

13.16 Completed risk register reviews must be submitted to the Governance, Compliance and Risk team in accordance with the published risk reporting schedule

Strategic risk reviews by ULT

13.17 ULT review the risk register regularly

13.18 ULT risk register reviews must:

13.19 Review progress on actions identified to manage risks. Ensure that risk owners are held to account

13.20 Discuss and agree which risks will be referred to the Audit and Risk Committee

13.21 Review risks referred upwards to the ULT risk register and agree whether to keep or deescalate to a local risk register

13.22 Agree which risks are sufficiently mitigated that they can be deescalated to a local risk register

13.23 Agree the closure of risks on the ULT risk register

13.24 Assess incidents of breach or near breach of the risk appetite, and reports these to the Audit and Risk Committee, either stating a) how the risk will be managed to bring it back into line with risk management, or b) making a recommendation to increase the risk appetite and stating the rationale for this

13.25 ULT also:

13.26 Reviews ad-hoc risk reports as required

13.27 Reviews the University's risk profile. The risk profile is a graphical representation of the relative positioning of risks in terms of their likelihood and impact

13.28 Understands how the risk profile has changed between reporting periods

13.29 Compares the current risk profile to the University's risk appetite

13.30 Holds an annual risk workshop to understand, review and update the University's risk profile

13.31 Considers risk as part of its discussions

Audit and Risk Committee risk review

13.32 The Audit and Risk Committee:

13.33 Receives and reviews the risk report from ULT

13.34 Satisfies itself that risks are being actively managed and appropriate controls are in place

13.35 Monitors the most significant risks to the University and the effectiveness of their mitigation

13.36 Satisfies itself that the University's approach to risk management is adequate and effective

13.37 The Audit and Risk Committee agrees its report on risk to the Board of the Governors

Board of Governors risk review

13.38 The Board of Governors:

13.39 Receives the risk report from the Audit and Risk Committee along with the Committee's opinion on the matters described above

13.40 Advises the executive on its level of assurance

13.41 Sets and monitors the University's risk appetite

14 Responsibilities

14.1 This section sets out the responsibilities of staff members and groups for risk management.

14.2 Risk Owners

14.3 Ensure that the risks you own are monitored and regularly reviewed.

Reviews will consider:

14.4 Changes to the existing controls

14.5 Further actions

14.6 Progress against actions previously agreed

14.7 Make recommendations on changes to the risk score for consideration by ULT

14.8 Make recommendations on escalation, de-escalation or closure

14.9 Report as required on the status of the risks you own

14.10 Deans and Directors

14.11 Demonstrate ownership of the local risk register in their faculty or professional service

14.12 Coordinate and manage the information in the local risk register, ensuring its integrity

14.13 Identify, assess and agree the response for new risks. Ensure that risks in their area of responsibility are identified, assessed, managed and reported

14.14 Agree the escalation of a risk from a local risk register for consideration for the strategic risk register

14.15 Agree the closure of risks on their local risk register

14.16 Ensure compliance with this policy and process

14.17 Act as first point of contact with the Governance, Compliance and Risk team on risk management

14.18 Ensure that risk register reviews are carried out and risks are updated in a timely manner

14.19 Remain aware of any supplemental or custom risk management practices used in the areas in their remit. Engage with the Governance,

Compliance and Risk team to ensure these comply with this policy and procedure. Advise ULT accordingly to inform its risk reviews

14.20 Other local risk register owners

14.21 Where a local risk register is not owned by a Dean or Director, a nominated owner must be identified. The owner must carry out the same tasks as the Deans and Directors which are described above

14.22 University Leadership Team

14.23 Set the tone at the top for risk management behaviours

14.24 Identify, assess and agree the response for new risks

14.25 Review and discuss the strategic risk register as described in section 13

14.26 Agree an owner for each risk on the strategic risk register. The risk owner must be at an appropriate level of seniority and accountability to carry out the responsibilities described above

14.27 Review ad-hoc risk reports as required

14.28 Agree which risks will be referred to the Audit and Risk Committee for review

14.29 Agree which risks will be deescalated to a local risk register

14.30 Agree the closure of risks on the strategic risk register

14.31 Carry out a risk workshop at least annually

14.32 Audit and Risk Committee

14.33 Satisfy itself that risks are being actively managed and appropriate controls are in place

14.34 Monitor the most significant risks to the University and the effectiveness of their mitigation

14.35 Satisfy itself that the University's approach to risk management is adequate and effective. Advise the Board on this

14.36 Advise the Board on the University's overall risk appetite, and the risk appetite for individual issues the Board judges significant

14.37 Advise the Board on major decisions affecting the University's risk profile or exposure

14.38 Recommend to the Board the annual statement of risk management and internal controls for inclusion in the Annual Report and Accounts

14.39 Board of Governors

14.40 Determine the University's overall risk appetite and the risk appetite for individual issues the Board judges significant

14.41 Ensure that sound systems of risk management and internal control are in place and are maintained

14.42 With the Audit and Risk Committee, monitor the principal risks and the operation of controls. This responsibility is shared with the Audit and Risk Committee which reports to the Board

14.43 Approve the Risk Management Policy and Procedure

14.44 Approve the annual statement of risk management and internal controls through its approval of the Annual Report and Accounts

14.45 Governance, Compliance and Risk Team

14.46 Responsible for the development and coordination of risk management activity across the University

14.47 Provide assistance and consultation on risk and risk management

14.48 Provide advice about the application of this policy and procedure

14.49 Own the risk management policy and procedure, ensuring that a review takes place at least every three years and that changes are referred to the Board of Governors for approval

14.50 Issue a risk reporting schedule at least annually. The schedule outlines the reporting requirements

- 14.51 Provide University-level risk reports to ULT, the Audit and Risk Committee and the Board of Governors
- 14.52 Receive and collate information from reviews of local risk registers, using this to prepare University-level risk reports, including the risk profile
- 14.53 Regularly monitor the actions required to address the risks which have been escalated to ULT, following up with risk owners as necessary
- 14.54 Recommend escalation and de-escalation of risks
- 14.55 Prepare ad hoc risk reports to ULT
- 14.56 Facilitate risk workshops for ULT and the Board of Governors

15 Escalation

- 15.1 ULT is the escalation point for risks from local risk registers
- 15.2 Each risk owner is responsible for considering whether a risk requires escalation to ULT. Deans and Directors are responsible for approving escalation
- 15.3 Risks must be escalated to ULT where the following is true:
 - 15.3.1 Current risk impact score is greater than or equal to 12.
 - 15.3.2 This is calculated by the highest impact score (financial or reputational) multiplied by the likelihood score
 - 15.3.3 Financial or reputational impact of 5
 - 15.3.4 Represents a significant threat from a University perspective, rather than a localised impact specific to the department/project/function
 - 15.3.5 A response will be more effectively co-ordinated at a ULT level rather than being managed locally
- 15.4 ULT members who wish to report a risk outside the formal reporting process should raise this at any ULT meeting or contact the Associate

Director Governance, Compliance and Risk. Other staff members should speak to their line manager

15.5 Where a risk has been identified by a manager, that person will assess the risk using the criteria set out in this procedure and consider whether it should be escalated to the relevant Dean or Director for inclusion in the local risk register or for further escalation

16 Risk Nominees

16.1 Deans, Directors and other ULT members may choose to appoint a risk nominees or nominees. They may choose to delegate any of their responsibilities under this policy and procedure to a nominee, except that ULT members must not delegate overall responsibility for a risk on the University risk register. Delegation to nominees should be documented using the online risk register or by sending an email to the nominee copied to the Associate Director Governance, Compliance and Risk

17 Associated documents

17.1 Online risk register user guide

17.2 Risk Appetite Procedure and Risk Appetite Statement

17.3 Guidance:

- How to identify and assess emerging risks
- How to assess controls and control opinion
- How to identify and document sources of assurance
- How to complete the target risk score
- How to assess risk appetite

18 Equality Impact Assessment

An Equality Impact Assessment is in place for this policy and procedure

Date: January 2025

Reviewer: Associate Director GCR

19 Ownership and approval

Policy owner: Associate Director Governance, Compliance and Risk

Approved by: Board of Governors

Date of approval: 26 March 2026

Date of next review: March 2029

20 Version control

Version: 1.1

Date: 26/03/2026