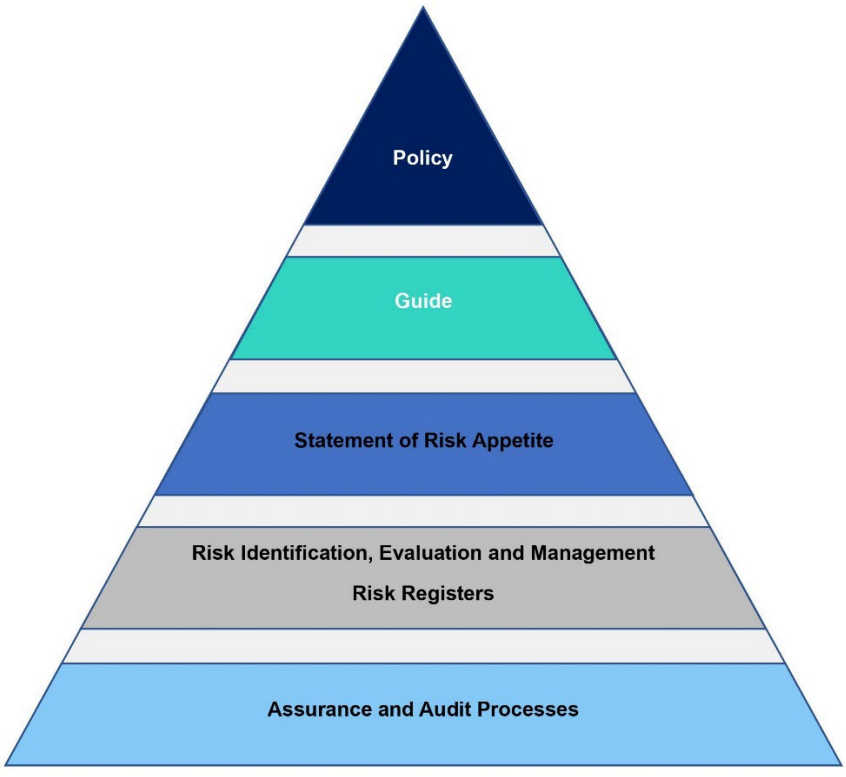
# Risk Management Guide

## Purpose of the Guide

1. This document supplements the Risk Management Policy of the University of Greenwich. It explains why risk management is an important element of the University's governance arrangements, and how the various committees, management groups and individuals in the University who have risk management responsibilities under the Policy should carry these out.

2. Risk Management is not the same as risk assessments in terms of the health and safety of staff, students and visitors. Separate guidance is available on health and safety risks.

3. The Risk Management Guide is part of the Risk Management Framework of the University, which consists of the following elements:
   a. Governance processes;
   b. The Risk Management Policy and this Risk Management Guide;
   c. The University's Statement of Risk Appetite;
   d. The identification, evaluation and management of significant risks, through the regular review of the Strategic Risk Register, the risk registers for strategic plan sub- and enabling strategies, Faculty and Directorate risk registers, and risk registers for major projects;
   e. Assurance and audit processes;
   f. The underlying policy and control environment; and
   g. Business Continuity Planning and Emergency Response Planning.



## Definitions

4. Some important definitions used in the Risk Management Framework are:

   i. Risk: "is the effect of uncertainty on objectives - usually expressed in terms of causes, potential events, and their consequences" (HM Government, *The Orange Book: Management of Risk – Principles and Concepts*, 2020)

   ii. Risk Management: all activities co-ordinated by the University which are designed and operated to identify, assess, respond to and report the uncertainties which may impact on the University's ability to achieve its objectives.

   iii. Risk appetite: the amount and type of risk that an organisation is prepared to seek, accept or tolerate.

   iv. Risk tolerance: the maximum level of residual risk which an organisation is prepared to tolerate after risk treatment (mitigations).

   v. Mitigation: controls and actions that are taken, or which could be taken, to address risks faced either by reducing the likelihood that they will occur, or by managing their impact if they do occur.

   vi. Control: a risk mitigation which is ongoing and will run continuously until changed (e.g. the regular review of student number forecasts).

   vii. Action: a risk mitigation which is SMART (specific, measurable, achievable, realistic and time-bound).

   viii. Raw risk: the risk of something happening before any controls or actions are applied to mitigate the risk.

   ix. Sources of Assurance: ways (preferably external) in which the controls on a risk are confirmed as actually taking place and being effective.

   x. Residual risk: the level of risk remaining after the application of controls and actions to mitigate the risk.

## Why we need to manage risk

5. Taking risk is an essential part of the direction and control of the University. Understanding and reacting appropriately to the risks involved in all the University's operations, both academic and supporting activities, is an essential part of the planning process. Risk cannot always be eliminated, but it can be managed to reduce any adverse impact ('mitigation'). Risk management is therefore a management tool to enable us as far as possible to quantify, prioritise and contain risk at all levels of the University's operation. It is a means to make informed decisions as to the acceptability of a course of action in the light of those risks.

6. The Higher Education Code of Governance issued by the Committee of University Chairs (CUC) requires the governing bodies of universities to ensure that there are effective systems of control and risk management in place. This includes ensuring

that there is an effective and proactive system of risk management by which risks are rigorously assessed, understood and effectively managed across the organisation.

7. The University is required by the Office for Students (OfS) Regulatory Framework to operate comprehensive corporate risk management and control arrangements (including for academic risk), to ensure the sustainability of the University's operations and its ability to continue to comply with all of its conditions of registration with the OfS. This is also a requirement of the Terms and Conditions of UK Research and Innovation Funding administered through Research England.

8. The University's Articles of Association require the Governing Body to "ensure that the University has an active process for the management and control of risk", including regular reporting from the Audit and Risk Committee (ARC).

9. Risk Management serves a number of purposes:

    - It documents to the OfS, the DfE, Research England and other funding bodies that we are carrying out our obligations to operate a risk management programme, as required by the OfS.
    - It helps us ensure that risk management is "an integral part of planning and decision-making" (HM Government, *The Orange Book: Management of Risk – Principles and Concepts*, 2020). For example, the Statement of Risk Appetite specifies the amount of risk the University is willing to seek or accept in the pursuit of its long-term objectives, and is thus a guide to risk-taking activities.
    - It informs our actions and decisions in achieving the University's objectives, set out in the Strategic Plan to 2030, This Is Our Time, which are reflected in the Key Performance Indicators approved by Governing Body.
    - It demonstrates a responsible and professional approach to business planning, and the monitoring of performance against plans.

**Risk levels**

10. **Strategic risks** are risks that might threaten the University's ability to meet its core strategic objectives and responsibilities. This includes risks that may threaten the University's ability to meet the objectives in the Strategic Plan, or to comply with legal and regulatory requirements. Strategic Risks are recorded in the University's Strategic Risk Register. The management of strategic risks and other risks is informed by the University's Statement of Risk Appetite, which specifies the amount of risk the University is willing to seek or accept in the pursuit of its long-term objectives.

11. **Sub- and enabling strategy risks** are risks that relate to the individual sub- and enabling strategies under the Strategic Plan. They are risks that may threaten the ability to achieve the objectives and goals in the sub- and enabling strategies. Sub- and enabling strategy risks are recorded in risk registers which are overseen by the boards responsible for the sub- and enabling strategies and reported to the University's Strategy Programme Board.

12. **Operational risks** are risks that are present in the day-to-day functions and services of the University. All staff of the University have some responsibility for managing operational risks. Faculty and Directorate risks are regularly reviewed by Faculty and Directorate management teams to ensure that new initiatives are properly identified and assessed for risk, and that continuing activities are properly managed so as to mitigate as far as possible the risks inherent in carrying out University operations.

13. Strategic risks inform, and are informed by, operational risks and sub- and enabling strategy risks. The relationship between them is therefore one of symbiosis and integration

**Roles and Responsibilities**

14. Roles and responsibilities under the University's Risk Management Framework are set out in in the Risk Management Policy.

**Risk Appetite**

15. The University's Statement of Risk Appetite specifies the amount of risk the University is willing to accept in the pursuit of its objectives, including those in the Strategic Plan. It indicates the parameters within which the University would want to conduct its activities, and in intended to act as a guide when taking risks.

16. The Statement of Risk Appetite is used to set the maximum **risk tolerance** (the maximum level of residual risk which the University is willing to tolerate after controls and mitigating actions) for Strategic Priorities and Compliance and Cross-cutting Strategic Risks, using the scoring system in this Guide and the risk tolerance bands in the Statement of Risk Appetite. The maximum risk tolerance associated with each priority should be reflected in the Strategic Risk Register and other risk registers. Where a risk relates to more than one priority, the risk tolerance will be that associated with the most 'cautious' priority (i.e. the priority with the lowest tolerance level).

**Recording of Risks**

17. Risk management is a continuous process. Areas should take account of Strategic Risks identified at an institutional level, and the controls required to mitigate Strategic Risks, when determining their local risk analysis. The Strategic Risk Register in turn is informed by the risks identified at lower levels. The process is both cyclical and continuing, and enables the University to take a dynamic and evolving approach to the management of its risks.

18. The key objectives of the framework are to ensure a consistent basis for the measurement, control, monitoring, follow-up and reporting of risk across the whole institution that is based on the University's appetite for risk, not those of individuals.

19. Risk registers will be used to record the University's risks, controls and actions across all areas of the institution.

20. The University's risk registers will be held at three levels:

a) **Strategic Risk Register** – key risks linked directly to the priorities in the University's Strategic Plan, plus cross-cutting Strategic Risks and Compliance risks.

b) **Sub- and Enabling Strategy Risk Registers** – risks to the achievement of the priorities and goals relating to the sub- and enabling strategies underneath the Strategic Plan.

c) **Operating Risk Registers** – risks identified at Faculty and Directorate level, arising both from the Faculty / Directorate operating experience and from assessment of the impact of institutional risks in a local context.

21. At each level, Risk Registers should include at least the following elements. Standard templates are available on the University's Risk Management webpage:

- Risk description
- Risk owner
- Associated strategic priority
- Risk tolerance
- Raw risk score (inherent impact and likelihood assessment, before the operation of controls and actions)
- Existing controls
- Evidence of the effectiveness of controls and actions, e.g. Strategic Plan KPIs
- Residual risk score (residual impact and likelihood assessment, after controls and actions)
- Risk status since last review, based on residual risk score (increasing, decreasing, static, new risk)
- Current actions to mitigate the risk, with action owner and due date
- Progress on actions

*Faculties and Directorates*

22. Faculties and Directorates will have access to the Strategic Risk Register via the University Secretary, who will circulate it quarterly to the Professional Services Group (PSG). Regular updates to local Operating Risk Registers will be generated after consideration by the relevant Faculty and Directorate management teams.

23. Operating Risk Registers should reflect Faculty and Directorate plans and should be updated on a quarterly basis through the year. Updated Operating Risk Registers should be provided for quarterly review to the University Secretary and the PSG, by deadlines specified by the University Secretary.

*Sub- and enabling strategies*

24. The member of Vice-Chancellor's Executive (VCE) who is the lead responsible for the sub- or enabling strategy should ensure that a risk register is kept of risks to the achievement of the strategy's priorities and goals. This should take account of the

Strategic Risk Register which the University Secretary will circulate quarterly to strategy leads.

25. Sub- and enabling strategy risk registers should be reviewed quarterly by the board responsible for the strategy. Following review, risks should be reported quarterly to the Strategy Programme Board and this will inform updating of the Strategic Risk Register by the University Secretary.

*Strategic Risk Register*

26. The Strategic Risk Register will be updated quarterly by the University Secretary, informed by Operating Risk Registers and sub- and enabling strategy risks. As part of the updating process, every other quarter the University Secretary and the Vice-Chancellor shall review risks in the SRR in conjunction with the risks sponsors and operational leads responsible for each risk. The Strategic Risk Register is approved by the VCE before it is submitted to the ARC. Following review by the ARC, a report on strategic risks will be prepared by the University Secretary for the Governing Body.

**Measurement of Risk**

27. The process for risk assessment will be the same at each level: the impact and likelihood for each risk, before and after controls, will be considered and a 1 to 5 scoring mechanism used to give a position on a 5 X 5 matrix. This will result in scores ranging from 1 to 25, with 25 being the highest score. In order to ensure consistent application across the University, criteria for the impact and likelihood scores should be in accordance with the following guidelines:

28. **Size of Risk – Impact**

| Descriptor | Impact Guide (impact is determined by one or more of the criteria below) | University-level financial impact |
|---|---|---|
| 1 Insignificant | No significant impact<br>Financial net impact of less than 0.5% of turnover (Faculties/Directorates: less than 0.5% of budget) | <£1.5m |
| 2 Minor | Financial net impact of less than 1.5% of turnover (Faculties/Directorates: less than 2% of budget)<br>No regulatory consequence<br>No impact outside a local process or product<br>Minor reversible injury<br>Internal adverse publicity | <£4.5m |
| 3 Moderate | Financial net impact of less than 3% of turnover (Faculties/Directorates: less than 5% of budget)<br>Limited regulatory consequence<br>Impact on other processes or products<br>Major reversible injury<br>Local adverse publicity | <£9.0m |

| Descriptor | Impact Guide (impact is determined by one or more of the criteria below) | University-level financial impact |
|---|---|---|
| 4 Major | Financial net impact of less than 10% of turnover (Faculties/Directorates: less than 20% of budget)<br>Significant regulatory consequence<br>Impact on many other processes or products<br>Irreversible injury<br>Death<br>National adverse publicity | <£30m |
| 5 Catastrophic | Financial net impact over 10% of turnover (Faculties/Directorates: more than 20% of budget)<br>Substantial regulatory consequence / regulatory intervention<br>Impact at strategic operational level<br>Irreversible multiple injury<br>Multiple deaths<br>International adverse publicity<br>Closure of University | >£30m |

29. **Size of Risk – Likelihood**

| Descriptor | Likelihood Guide |
|---|---|
| 1 Rare | 1-5% likely to happen, for example once in the next 100 years |
| 2 Unlikely | 6-20% likely to happen, for example once in the next 20 years |
| 3 Possible | 21-50% likely to happen, for example once in the next 2 to 5 years |
| 4 Likely | 51-90% likely to happen, for example at least twice in the next two years |
| 5 Almost certain | >90% likely to happen, for example regularly in the next 12 months |

**Risk Before and After Controls**

30. In order to assess the effectiveness of controls, risk will first be scored before considering the operation of the University's controls – this is termed the 'Raw Risk Score'. For each risk, the controls and actions in place will then be identified and assessed and the risk score generally reduced to arrive at the 'Residual Risk Score'.

31. The control and actions should either reduce the likelihood that a risk will occur or the impact of that risk were it to occur (examples of the latter would be purchasing insurance to insure against a risk and running backups in the event of an IT failure). The difference between controls and actions is that while controls will normally run continuously until changed, actions to reduce risks will by time-limited and should be SMART (specific, measurable, achievable, realistic and time-bound). An action may evolve into a control. Residual risk is what is left after considering controls and actions. Where the score after controls is still at an unacceptably high level,

additional controls and actions may be required in order to reduce the risk level further.

32. The University's objective is to optimise its controls and actions, i.e. to ensure the most cost-effective controls and actions are in place for each risk and the cost versus the benefit of the control is considered. This may mean that certain risks have a higher residual score because the cost of reducing the risk still further may be higher than the potential cost if the risk actually happens.

**Monitoring and Review of Risks**

33. As indicated above, risk registers will be kept up to date via a review by management to indicate they have considered changes in the risk profile within their area of responsibility. Operating Risk Registers, sub- and enabling strategy risk registers and the Strategic Risk Register will be reviewed on a quarterly basis to enable the Strategic Risk Register to be updated for the VCE and the ARC and a report on strategic risks to be provided to the Governing Body.

34. The update to risk registers may take the form of new risks, changes to controls and actions or additional controls and actions, and changes to risk scores. Examples of key triggers for significant changes to risk registers include new regulations or legislation, implementation of new projects, changes in the external environment, risk events, and Internal Audit reviews.

35. In the event of an exceptional and significant change in the risk environment arising between quarterly reviews, the relevant risks will be reviewed immediately by management. A review should always take place where a residual risk score is believed to have moved into the 'red' zone of the risk map (see below). An update to Operating Risk Registers or sub- and enabling strategy risk registers will be made using this guidance and escalated immediately to the University Secretary. This will inform the updating of the Strategic Risk Register for consideration by VCE prior to its reporting to the ARC and the Governing Body. Where the change in the risk environment in between quarterly reviews relates to the Strategic Risk Register, the University Secretary will discuss the proposed review with the Vice-Chancellor before escalating the proposed change to the Strategic Risk Register to VCE for approval. The chair of the ARC will then be informed about the change.

36. Using the guidance above, a consistent methodology for measuring and scoring risks will be applied throughout the University. The residual risk score for a risk will lead it to being compared to the associated risk tolerance, which is the maximum level of residual risk which the University is willing to tolerate after risk treatment (controls and mitigating actions). Whether additional controls and actions will be required to further reduce the residual risk score to an acceptable level will be determined by the associated risk tolerance threshold for the relevant Strategic Priority or Compliance and Cross-cutting Strategic Risk in the Statement of Risk Appetite.

37. The comparison of the residual risk score to the associated risk tolerance will result in a risk being classified as either 'above the associated risk tolerance threshold' or 'at or below the associated risk tolerance threshold'. This means that in some cases risks in the 'amber' or even the 'red' zones may be acceptable:

*Strategic Risk Register*

- A residual risk score of **4 or less** is considered acceptable to the institution and will require no further action other than to ensure the relevant controls are operating effectively. Managers should, however, review the controls for low risk areas carefully to ensure there is not 'over control' (i.e. excessive controls being applied). These risks appear **green** in the traffic light system used in the Strategic Risk Register.

- Risks with a residual risk score of **5 to 14** appear as **amber** in the traffic light system used in the Strategic Risk Register. These risks will require the implementation of additional controls where the risk score is above the associated risk tolerance threshold.

- Risks with a residual risk score of **15 or more** appear **red** in the traffic light system used in the Strategic Risk Register. These risks will require the implementation of additional controls where the risk score is above the associated risk tolerance threshold.

- If the residual risk score of a strategic risk remains above its associated risk tolerance threshold in two or more consecutive quarterly reports to the Governing Body, the Governing Body may decide, on the advice of the ARC and VCE, to accept the residual risk level. In this case, the relevant controls should continue to be operated effectively, but additional controls will not be sought to be implemented.

*Sub- and enabling strategies*

- For sub- and enabling strategy risk registers, risks with a residual risk score appearing 'amber' or 'red' which are above the associated risk tolerance threshold should be actively considered by the board responsible for the strategy. These risks (and all risks that are 'red' after mitigations) should be reported quarterly to the Strategy Programme Board.

- If a residual risk score remains above its associated risk tolerance threshold in two or more consecutive quarterly reports to the Strategy Programme Board, the Strategy Programme Board may decide to accept the residual risk level. In this case, the relevant controls should continue to be operated effectively, but additional controls will not be sought.

- For residual risk scores appearing 'red' and those risks which are above their associated risk tolerance threshold, the Strategy Programme Board should refer the risk to the University Secretary for consideration when updating the Strategic Risk Register.

*Faculty and Directorates*

- For Operating Risk Registers, risks with a residual risk score appearing 'amber' or 'red' which are above the associated risk tolerance threshold should be actively considered at regular Faculty/Directorate management

meetings. These risks should be flagged when the risk register is reported quarterly to the Professional Services Group.

- If a residual risk score remains above its associated risk tolerance threshold in two or more consecutive quarterly reports to the Professional Services Group, the PSG may decide to accept the residual risk level. In this case, the relevant controls should continue to be operated effectively, but additional controls will not be sought.

- For residual risk scores appearing 'red' and those risks which are above their associated risk tolerance threshold, the PSG should refer the risk to the University Secretary for consideration when updating the Strategic Risk Register.

38. The table below shows the range of risk scores:

| Impact | | | | | | |
|---|---|---|---|---|---|---|
| | 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 |
| | | Likelihood | | | | |

Red
Amber
Green

**Reporting of Risks**

39. The University's approach to reporting of risks is described above. The Governing Body will receive quarterly reports on Strategic Risks (including changes to risks) during the year, following consideration of the Strategic Risk Register by the ARC preceded by the VCE. The Risk Management Policy, Risk Management Guide and the Statement of Risk Appetite will be reviewed annually by the VCE and the ARC, with any changes being approved by the Governing Body.

40. The VCE will review residual risk scores in the Strategic Risk Register which are above the associated risk tolerance threshold. Where a score remains above its associated risk tolerance threshold in two or more consecutive quarterly reports, VCE will recommend to the ARC and Governing Body whether the risk should be accepted or additional controls and actions put in place.

41. Faculties and Directorates will review Operating Risk Registers on a quarterly basis prior to their being reported to the PSG. This will inform the updating of the Strategic Risk Register by the University Secretary prior to its consideration by the VCE and the ARC.

42. The boards responsible for sub- and enabling strategies will review their strategy risk registers quarterly and report risks to the Strategy Programme Board, to inform the updating of the Strategic Risk Register by the University Secretary.

43. Internal Audit, via the ARC, will provide the Governing Body with independent assurance on the adequacy and effectiveness of the risk management process.

**Major Project Management**

44. An integral part of the University's project methodology is that all major projects require a risk register to be prepared at the outset of the project.

45. At the beginning of the project, the focus is on identifying the key risks and what controls should be put in place to mitigate these risks. As the controls have not yet been implemented, it is the 'Raw Risk Score' that is the primary focus as this is effectively the residual risk to the University. As the project progresses and controls are implemented, the residual risk score should fall. Sources of assurance that mitigating actions are being implemented should be documented. Senior managers responsible for major projects, in conjunction with the Project Manager, are responsible for reporting on the start and progress of major projects which may have an impact on the Strategic Risk Register.

46. Industry guidelines will determine the assessment of risk in estates-based projects. Academic projects are also subject to quality assurance review procedures. Project managers are expected to make an assessment of risk throughout the lifetime of a project in the light of generally accepted good practice, and to report to and advise senior management appropriately.

47. Major new projects may change the University's risk profile and it is important that the Vice-Chancellor's Executive is able to approve and accept these projects before implementation or any significant commitment has been made. A raw risk score of 20 or more for a major new project will require VCE's approval. The use of a raw risk score of 20 for major new projects reflects the fact that risks are being looked at before controls.

48. During the implementation of a major project, any residual risk scores that are 'red' should be reported to VCE. This will inform the updating of the Strategic Risk Register by the University Secretary prior to its consideration by the VCE and the ARC.

**Approved by the Governing Body: 11 October 2023**
**Date of next review: June 2024**
**Owner: University Secretary**