

# **Risk Management Policy**

**Policy Statement**

The University of Stirling recognises that there is risk involved in delivering its strategy. This is both in responding to challenges and from inaction in the face of opportunities. The Risk Management Policy sets out the University’s approach to effective risk management. It aims to strengthen our ability to respond to risk in a way that contributes positively to the University achieving its objectives.

**Purpose**

The purpose of the policy is to ensure that:

* Risk is considered in the development and delivery of the University’s activities.
* Effective risk management is integrated into our decision-making processes through the identification, evaluation, monitoring, and review of risks in a systematic and proactive manner.

The Risk Management Policy:

* sets out a definition of risk, roles and responsibilities;
* is supplemented with guidance tools to embed good practice in the identification, assessment, mitigation and monitoring of risk.

The University aims to:

* ensure that the delivery of our Strategy and key objectives is not negatively impacted by significant unanticipated risk.
* ensure reliable contingency plans are in place and developed to deal with unexpected risks.
* embed risk management into our decision-making processes.
* promote an innovative and less risk-averse culture in which taking risks within the University’s risk appetite range in pursuit of opportunities is encouraged and supported.

**Scope**

This Policy extends to all the University’s activities and operations. All staff have responsibility for identifying and reporting risks within their respective areas of expertise and should be aware of and participate in implementation of this policy.

**Definitions**

Risk exists as a consequence of uncertainty and is present in all University activities. The exposure is normally expressed in terms of the failure to reach an objective and the operational, reputational and financial damage that may be incurred as a result.

Risk management is defined as the planned and systematic approach to identifying, evaluating, addressing, and monitoring risk.

Strategic risk is defined as the possibility that an action, event or set of circumstances will have an effect on the University’s ability to achieve its strategic objectives or have an impact on the University as a whole. These are risks that should be collectively monitored or managed by the governing body, University Court and the Senior Management Team.

Operational level risk is the possibility that an action, event or set of circumstances will have an effect on the ability of a faculty or directorate to achieve its objectives. The risk is generally associated operational procedures and systems and may results from inadequate or failed internal processes and systems or human error. A faculty, departmental or project level risk could be classified as a strategic risk where the severity of its impact may effect the University’s ability to achieve its strategic objectives or have an impact on the University as a whole.

**Roles and Responsibilities**

The key roles and responsibilities are outlined below:

**University Court**

* University Court approves the strategic objectives and major policies required to comply with statutory requirements and is accountable for ensuring the University’s control framework and assessment of risk is effective.
* University Court will determine the risk appetite of the University as a whole and will review the risk appetite periodically (at least annually) to ensure alignment with objectives, the operating environment and emerging risks.
* University Court has delegated responsibility for the oversight of strategic risk management arrangements to the Audit Committee.

**Audit Committee**

* Audit Committee will keep under review the University’s approach to, and policies on risk management, regularly considering the effectiveness of the University’s control framework and the assessment of risk.
* Audit Committee will report to Court (at least annually) its opinion on the effectiveness and adequacy of governance arrangements including risk management arrangements and control.

**University Strategy and Policy Group (USPG)**

* USPG has prime responsibility for ensuring a culture of effective risk management is supported and sustained.
* USPG will identify and periodically evaluate (at least three times per academic year) the significant risks faced by the University for review by Audit Committee and Court.

**University Community**

* Ownership of the Risk Management Policy and reporting is delegated to the Deputy Secretary and Executive Director of Student, Academic and Corporate Services to ensure the managing processes are robust and demonstrate assurance to the Audit Committee.
* Accountability and ownership for each strategic risk is assigned to a member of the Senior Management Team.
* The role of risk owner is to take responsibility for ensuring that suitable management strategies are in place for dealing with each identified risk.
* Internal Audit evaluate the internal control systems and provide assurance to Audit Committee and University Court on the effectiveness of risk management processes. The internal audit strategy is developed around the University’s strategic objectives and is informed by the Institutional Register of Strategic Risk.
* The University’s planning and budgeting cycle sets the objectives and targets necessary to achieve the delivery of our strategic ambitions. Operational risk management is embedded within this process, is reviewed periodically, and informs strategic risk review. Where risks identified are either common to all operational areas or where they have been identified as having potentially broader implications, they will be recorded, evaluated and monitored within the Institutional Register of Strategic Risk.
* Deans of Faculties and Service Directors are responsible for identifying, assessing and monitoring risks at faculty and service level.
* Employees of the University must understand the nature of risk and are responsible for managing risk associated with their area of authority.
* Risks associated with projects (including, for example, capital building or other infrastructure projects, collaboration and partnership agreements, business improvement, IT projects, etc.) will be examined as an integral part of the authorisation and project management processes.
* Identification, assessment and mitigation of health and safety risk is managed by the Head of Safety, Environment and Continuity.  These risks will not be managed as part of the University Risk Management Policy.  Please refer to the [University’s Safety Policy and Risk Assessment Procedure](https://www.stir.ac.uk/about/professional-services/estates-and-campus-services/safety-environment-security-and-continuity/safety/) for further details.

**Risk Identification and Assessment**

The University has established a framework for systematically identifying and documenting potential risks across a range of categories such as financial and reputational that could have an effect on the ability of the University to achieve its objectives. The key risk categories and definitions are presented at **Appendix 2**.

Risks must be assessed in relation to the likelihood of their occurrence and their potential impact on the achievement of objectives using the established criteria at **Appendix 2 – Risk Assessment Matrix**. The assessment process will consider qualitative and quantitative factors to inform decision making, enable the prioritisation of risk, and the effective allocation of resources.

**Risk Appetite**

Utilising risk appetite principles enables the University to identify and set appropriate thresholds for risks, whereby University Court establishes the level of risk the University is willing and able to accept or absorb in pursuit of its objectives.

The University recognises that risk appetite will vary according to the activity, and that its acceptance of risk is subject to ensuring the potential benefits and risks are clearly identified, and that measures to mitigate risk are established before activities are approved.

By linking risk residual scores established during the assessment process to agreed risk appetite levels, the University ensures that its risk management efforts are aligned with strategic objectives and tolerance for risk. This ultimately supports informed decision-making and effective risk governance. Each risk appetite level in **Table 1** overleaf correlates with a residual risk score on the University’s risk assessment matrix.

**Table 1 – Risk Appetite, Description and Risk Tolerance**

|  |  |  |
| --- | --- | --- |
| **Risk Appetite**  | **Description**  | **Risk Tolerance** |
| **Averse** | Avoidance of risk and uncertainty in achievement of key deliverables or initiatives is a key objective. Activities undertaken will only be those considered to carry low risk.  | The University will accept risk with a residual score of 1-4 |
| **Cautious**  | Preference for safe options that have a low degree of risk and may only have limited potential for reward (potential for benefit/return is not a key driver). Activities will only be undertaken where they have a moderate degree of risk. | The University will accept risk with a residual score 5 – 9 |
| **Open**  | Willing to consider all potential options and choose one most likely to result in successful delivery while providing an acceptable level of benefit (reward and value for money). Willing to tolerate a degree of risk in selecting which activities to undertake to achieve key deliverables or initiatives, where we have identified scope to achieve significant benefit and/or realise an opportunity. Activities undertaken may carry a high degree of risk that is deemed controllable to a large extent.  | The University will accept risk with a residual score of 10 – 16 |
| **Eager** | Eager to be innovative and to choose options based on maximising opportunities and potential higher benefit even if those activities carry a very high residual risk. | The University will accept risk with a residual score of 20-25 |

**Risk Tolerance and Mitigation**

Risk tolerance is the maximum level of risk the University is able to accept regarding each type of risk. If a risk is ‘out of appetite’, this indicates that close monitoring and action is required. These risks must be monitored and escalated appropriately following risk register hierarchy and management arrangements in accordance with the agreed risk appetite and tolerance for that category of risk.

Once risks are identified and assessed, appropriate mitigation strategies will be developed to reduce their impact and likelihood. These strategies may include risk avoidance, risk transfer, risk reduction or acceptance, depending on the nature and severity of the risk.

Appropriate action to manage the risk will include one of the following four options:

* **Tolerate the risk** – this involves accepting the risk without putting in place any controls to manage the risk, as it is considered to be of a tolerable level for the University, in line with approved risk appetite.
* **Treat the risk** – this involves accepting the risk but applying relevant control/mitigating action to reduce it to a risk appetite approved by University Court, the governing body.
* **Transfer the risk** – this involves handling the risk elsewhere, either totally or in part, such as outsourcing the provision of services or the use of insurance. Please note that the University will retain ultimate and certain levels of responsibility for risk management regardless of whether provision is outsourced elsewhere; and
* **Terminate the risk** – this involves eliminating the risk entirely by ceasing the activity or changing the strategy of the University.

**Monitoring and Review**

The ongoing management and review of risk is a critical part of the process as it enables adjustments to mitigation strategies necessary to address emerging risks or changing operating conditions. It also provides assurance on the overall management of the University’s risk profile.

Required risk review timescales are outlined below:

* Out of Tolerance or Appetite – Monthly
* In Appetite or Tolerance – Quarterly

These are the minimum review timescales, if there are changes in the operating environment which could affect the severity of a risk, a review should be undertaken and reported more frequently.

During a risk review, the risk score must be re-assessed by the risk owner. If it is identified that the risk continues to exist, the list of current controls and action required will be reviewed and amended as required. Based on progress with actions and the assessment of the risk environment (i.e. are there any significant changes to the internal/external context), a re-assessment of the current scores must be undertaken using the risk assessment matrix. This will determine whether the risk is decreasing, increasing or remaining static, and whether the risk requires escalation.

If a current residual risk score is above the agreed risk appetite for that risk category the faculty, directorate or equivalent should closely monitor the risk and undertake corrective action by amending existing controls or applying new controls. If the risk remains ‘out of appetite’ after 6 months, the risk should be escalated to a strategic risk for oversight and direction of mitigating action. If a current residual score significantly exceeds the agreed risk appetite tolerance, it should be escalated to as a strategic risk immediately for enhanced oversight and direction of action.

**Communication and Reporting**

Clear communication and reporting channels have been established to facilitate the sharing of risk-related information and update across all levels of the University. Regular reports on risk management and risk management activity are provided to University Strategy and Policy Group (USPG) and relevant governance committees, and University Court as required.

**Relevant Legislation and Regulation**

The University is required to comply with the provisions of the Scottish Funding Council’s (SFC’s) Financial Memorandum with Higher Education Institutions.  The Memorandum requires the governing body, University Court, to comply with the principles of good governance set out in the Scottish Code of Good Higher Education Governance. The Code is a framework for good governance that sets out principles and standards including the recommendation that the governing body must be attentive to risks which could threaten the sustainability of the institution and ensure that the institution has appropriate procedures to identify and actively manage risk. The governing body needs to understand the external environment in which the institution operates and the strategic risks and opportunities it faces. The University should maintain a risk register and is expected to provide a description of the principal risks and uncertainties being faced, including risk management arrangements, in their annual audited financial statements.

**Approved by University Court**

**December 2024**