

# UNIVERSITY OF STIRLING

**RISK MANAGEMENT POLICY AND GUIDANCE**

# Contents

## Introduction

1. Purpose
2. What is risk?
3. What is risk management?
4. The University’s approach
5. Responsibilities
6. Defining the risk appetite
7. Management of risk
8. Annual review of effectiveness

### Introduction

The University faces numerous risks that could affect any aspect of its academic, administrative or commercial business activities. Sound risk management is therefore required to ensure the University is able to achieve its operational aims and strategic objectives.

The University considers risk management to be fundamental to good management practice and a significant aspect of corporate governance. Risks include not only threats facing the University, but also a failure to seize opportunities. An assessment of risk must therefore be conducted to identify, analyse and report to the most appropriate management level within the University.

It should be noted that risk management is the responsibility of everyone at the University, not just a small number of named individuals. The University maintains a register of strategic risks, and all academic schools and service areas maintain operational risk registers that are integrated into the planning and budgeting process.

### Purpose

This risk management policy identifies the underlying approach to risk management across the University. It defines the roles and responsibilities of senior managers and governing bodies together with the annual mechanism for reviewing risk management processes.

The purpose of this policy is a formal acknowledgement of the commitment made by the University to risk management. The University considers that taking well-managed risks is essential to the success of higher education, in the management of its core activities of research and teaching, as well as its supporting activities. The aim of the policy is not eliminate risk from the University’s activities, but rather to manage risk appropriately.

This document is supported by the Risk Appetite Statement and guidance for all staff (Appendix 1).

### What is risk?

Risk is commonly defined as the possibility that an action, event or set of circumstances will adversely or beneficially affect an organisation’s ability to achieve its objectives.

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.

### What is risk management?

Risk management is the planned and systematic approach to identifying, evaluating and controlling risks at all levels of the organisation.

### The University’s approach

The University’s approach to risk management is guided by the following principles:

* + the University Court has responsibility for the effectiveness of internal controls based on information provided by Audit Committee
	+ risk management is implemented as an integral part of University activities at all levels and is monitored by the Audit Committee
	+ risks are identified, analysed and recorded as appropriate, normally within a risk register that scores the likelihood and impact of risks
	+ the management of risk will involve user-friendly language and University processes will be kept as simple and effective as possible
	+ the financial and non-financial implications arising from risks and associated controls will be estimated as accurately as possible
	+ the University Strategy and Policy Group (USPG) will support, advise and implement risk management processes and will act as a risk management committee when required
	+ risk will be a standing item at meetings of the Senior Management Team (SMT), and heads of academic schools and service directors will be responsible for embedding good risk management practice within their school or service area.

The University uses five steps to manage risks, and a common template to record and report strategic and operational risks:

***Step 1 – Identifying risks***

The identification and review of risks takes place throughout the year and is a formal part of the planning and budgeting cycle. Each management group is encouraged to carry out ongoing reviews and updates of the linkages between strategic objectives and risks to ensure that focus is maintained on priority activities.

Strategic risks typically affect the whole of an organisation and not just one or more of its parts. Because of this, strategic risks are recorded and monitored at an institutional level and form a key part of strategic management. Operational risks refer to issues arising from the normal business operations. Accordingly, they affect the day-to-day running of the University in contrast to strategic risks that arise from the organisation’s strategic positioning. Operational risks are typically managed at school or service level and can be managed and mitigated by internal control systems.

***Step 2 – Analysing the risk***

The University uses a risk model to measure the likelihood and impact of individual risks identified in operational or strategic registers. Impact is the potential severity or effect of the risk. Likelihood is the frequency or probability of a risk occurring. The risk score is calculated using the impact and likelihood to produce an evaluation of net risk that can be translated into a traffic light system.

***Step 3 – Determining the risk owner***

Strategic and operational risks should be assigned to a risk owner, who is responsible for managing the risk and associated control measures.

***Step 4 – Identifying control measures***

The identification of control measures will depend on the treatment category of the risk at residual level. The University uses the 4Ts to categorise risk:

* + Tolerate – risks are accepted and built into operational or project management
	+ Treat – risks are reduced by management action (e.g. putting in place a business continuity plan)
	+ Transfer – risks are passed on to another organisation or body (e.g. outsourcing, insurance or subcontracting)
	+ Terminate – risks are avoided by doing something else

Actions to mitigate or control a risk will have a direct cost or an opportunity cost that should be recorded in the risk register. The risk should be reassessed to identify the impact of any action on the net risk. The result of any control measure is known as the residual risk.

***Step 5 – Reviewing the risk***

Risks should be reviewed on a regular basis to ensure that strategic and operational registers are kept up-to-date. At a University level, the register of strategic risk is reviewed and discussed at each meeting of Audit Committee.

### Risk responsibilities

It is essential that all participants in risk management are aware of their roles in the overall process and their own responsibilities. The key responsibilities are outlined below:

*University Court*

The Court has a fundamental role to play in the management of risk and in setting an overall culture of risk management within the University. This includes:

* + determining and reviewing the risk appetite of the University as a whole, and agreeing a risk appetite statement that is reviewed annually
	+ approving major decisions affecting the University’s risk profile or exposure
	+ determining what types of risk are acceptable or not acceptable

***Audit Committee***

Acting on behalf of Court, Audit Committee will:

* + monitor the management of key strategic risks
	+ satisfy itself that less significant risks are being actively managed, with the appropriate controls in place and working effectively
	+ annually review the University’s approach to risk management, and approve changes or improvements to key elements of its processes and procedures
	+ approve the internal audit plan which is linked to the Strategic Risk Register
	+ report to Court on the effectiveness of risk management processes as appropriate

***Executive Group***

The University Strategy and Policy Group (USPG) is responsible for strategic risks by:

* + identifying and evaluating significant risks faced by the University for consideration by Court, via Audit Committee
	+ implementing policies on risk management and internal control
	+ providing adequate information in a timely manner to Court, via Audit Committee, on the status of risks and control measures
	+ regularly reviewing the effectiveness of internal controls
	+ identifying and acting as risk owner for appropriate strategic risks

***Senior Management Team (SMT)***

Deans of Faculties and service directors are responsible for identifying, assessing and monitoring risks at faculty and service level. They will:

* + disseminate good and appropriate risk practice within their faculty/service
	+ identify, monitor and assess risk issues within their faculty/service
	+ monitor and discuss risk as a standing item on the agenda of SMT
	+ report on risk and control issues in their annual Planning Statement, and review regularly as appropriate
	+ alert the risk management committee (USPG) to risks which may have strategic importance

***Staff and students***

Effective risk management depends on the commitment and co-operation of all staff and students. All staff have a significant role in the management of risk, particularly within their own areas of control. Students have the opportunity to participate in and contribute to the effective management of risk through faculty governance arrangements, such as student and staff consultative groups. Project managers and project teams are responsible for managing project-specific risk and will complete a project risk register to demonstrate that this is being done.

### Defining the risk appetite

The University Court determines the extent to which the University is “risk-taking” or “risk- averse”. The evaluation of the University’s strategic risks via Audit Committee provides a regular review of the University’s risk tolerance line.

### Management of risk

The management of risk is supported by a system of internal control, and is closely related to the planning and budgeting process and institutional performance management. This enables the University to respond to a variety of operational, financial, reputational and commercial risks. The elements of this system include:

*Policies and procedures*

Attached to significant risks are a series of policies that underpin the internal control process. These policies are approved by Court and are supported by written procedures where appropriate.

*Reporting*

Strategic risks are reported regularly to Audit Committee via the risk register or on an ‘exception’ basis as required, for example, on risks associated with new projects, or on emergent external risks.

*Planning and Budgeting*

The annual planning and budgeting process is used to set objectives, agree action plans and allocate resources. Schools and service areas are responsible for updating their planning statements and associated risk registers and performance measures as part of this process. Progress towards meeting planned objectives is monitored regularly by the senior management team.

*Risk Framework*

The register of strategic risks is reviewed by the risk management committee (USPG) and is used to identify, assess and monitor risks significant to the University. Improvement actions and risk indicators are monitored regularly.

*Audit Committee*

Audit Committee is required to report to Court on internal controls and inform Court about any emerging issues. In addition, Audit Committee oversees internal audit, external audit and management as required in its review of internal controls. Audit Committee will advise Court on the effectiveness of the risk management and internal control systems.

*Internal audit*

Internal audit is responsible for aspects of the annual review of the effectiveness of the internal control system within the University. The internal audit strategy will be developed around the University’s strategic objectives and is informed by the register of strategic risk.

*External audit*

External audit informs the Audit Committee on the operation of internal financial controls reviewed as part of the annual audit. *However, external audit is not part of the risk management process.*

*Third Party Reports*

From time to time, the use of external consultants may be appropriate in areas such as health and safety (e.g. radiation protection adviser), and human resources. The use of specialist third parties for consulting and reporting can, in some cases, increase the reliability of the internal control system.

*Operational Risk and Environmental Sustainability (OR & ES)*

The University has access to competent safety advice through the Head of OR & ES, who advises the University on aspects of health and safety management and business continuity. The Head of OR & ES reports operationally to the Director of Estates and Campus Services, but also has a reporting line to the University Secretary. Overall responsibility for ensuring that the University complies with health and safety legislation lies with the University Court.

*Policy and Planning*

The Policy and Planning team compiles risk issues, supports University staff in the assessment and management of risk, and reports emergent strategic risks as appropriate. The team also reviews operational risk registers from schools and service areas, identifies training needs and identifies emergent risks to be included within the register of strategic risk.

### Annual Review of Effectiveness

The University Court is responsible for reviewing the effectiveness of internal control of the University, based on information provided by Audit Committee. In doing this, Court will consider the following:

* + The University’s objectives and its financial and non-financial targets
	+ The University’s performance in identifying, assessing and reporting risks
	+ Prioritisation of risks and the allocation of resources to areas of high exposure
	+ Effectiveness of control measures

Audit Committee, on behalf of University Court, will review the risk register and this policy document to ensure on-going effectiveness in the management of risk.

### Policy and Planning

### June 2021

**Risk Management Guidance**

**1. Purpose**

The University of Stirling recognises the importance of effective identification, evaluation and management of all key strategic and operational risks.

Risk is ever present and some amount of risk taking is inevitable if the University is to achieve its objectives. By being ‘risk aware’ and understanding its risk appetite the University is in a better position to avoid threats and take advantage of opportunities.

Risk Management is a key element of the University’s overarching governance arrangements as it demonstrates that we have considered our plans, we have analysed the consequences of things going wrong, and that we have thought through the actions and controls we need to prevent or limit these consequences.

This document, and the related Risk Appetite Statement and Risk Management Policy, should be used as a basis to establish and embed risk management within everyday activities across the University.

**2. Definition of Risk Management**

What is a Risk?

A risk is the uncertainty of an event occurring that could have an impact on the achievement of the organisation’s objectives. Risk is measured in terms of likelihood and impact. The effect may be positive, negative or a deviation from the expected. A risk is often described by an event, change in circumstance or a consequence.

**Strategic risk** is concerned with where the organisation wants to go, how it plans to get there and how it can ensure survival. This is the risk associated with the achievement of future business plan objectives including strategic objectives. This will include new initiatives and funding streams as well as the development of current services and funding streams.

**Operational risk** is the risk of loss or gain, resulting from inadequate or failed internal processes, people and systems or from external events. this is the risk associated with ongoing operational procedures and systems. This will include systems such as payroll, management information and human resources.

**Project risk** – this is the risk associated with the successful completion of a project in order to deliver its strategic and operational objectives effectively, efficiently, in line with agreed resources and to deliver identified benefits. Project risk may occur in relation to the development of a new service, product or provision, the introduction of new systems or significant changes to existing systems.

Project risk will be a short-term consideration in comparison to strategic and operational risk with the relevant strategic and operational elements of the risk moving into the above risk areas upon completion of the project.

What is Risk Management?

In its simplest definition, Risk Management is a process that aims to help organisations understand, evaluate and take action on all of their risks to increase the probability of success and reduce the probability of failure. This requires co-ordination of activities to direct and control an organisation with regard to Risk Management.

Areas to consider are as follows:

* What internal and external factors could prevent the achievement of our objectives?
* What could go wrong with our operations?
* How likely is it that they will go wrong?
* How bad (i.e. what impact) would it be if they did go wrong?
* What can we do to prevent them (i.e. likelihood) from going wrong?
* Are we doing enough (i.e. mitigating controls) regarding what could go wrong?
* Who is responsible for ensuring that we have good answers to these questions?
1. **Objectives of Risk Management**

Our aims and objectives with respect to Risk Management are as follows:

* To further embed Risk Management into the culture of the University;
* To understand, proactively identify and manage opportunities and risks of both the University and those partnerships with which it is involved, in accordance with good practice;
* To respond to risk in a balanced way, mindful of the risk level, risk reduction potential, cost/benefit, and relationship to resource constraints;
* To take actions to maximise opportunities and to minimise the likelihood of risks occurring and/or reducing the impact of consequences should risks occur; and
* To provide information as to the effectiveness of the arrangements for risk management as a contribution towards the annual disclosure about risk management in audited financial statements.
1. **Risk Management Documentation**

The University’s risk management documentation supports our risk management approach and reporting requirements. In addition to this guidance, key documents include:

* Risk Appetite Statement;
* Risk Management Policy;
* Register of Strategic Risks; and
* Registers of Operational Risk.

**Risk Appetite**

Risk appetite can be defined as the level of risk that an organisation is prepared to tolerate in pursuit of its objectives. Factors such as the external environment, people, business systems and policies and how key stakeholders perceive the University will all influence risk appetite.

Risk Management is not about being ‘risk averse’ – it is about being ‘risk aware’. Risk is ever present and some amount of risk taking is inevitable if the University is to achieve its objectives. Risk Management is about making the most of opportunities and achieving objectives. By being risk aware, employees can be confident in their abilities to make informed decisions.

There are four different stages to Risk Management: Identify, Evaluate, Manage and Review.

Stage 1 – Identify:

The recognition of risks is necessary through identification of the nature of the risk and the circumstances in which it could materialise. Examples of the potential risks facing the University could include the following:

* Inability to operate on campus (flood, power failure, fire etc);
* Student dissatisfaction with our learning and teaching leads to a dramatic loss of income; and
* Damage to reputation through negative media coverage.

Such risks are known as the “original risk” and all those responsible for risk must identify original risks faced by their department.

Stage 2 – Evaluate:

All risks identified at stage 1 should be ranked or evaluated in terms of impact and likelihood to produce the original risk profile. Guidance on how to evaluate risks can be found below. When responding to risks identified, a decision must be taken as to the appropriate action to manage the risk, to do this we can use the following four options:

Risk Mitigation Strategies:

* **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 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.

Once a decision on the treatment of the risk has been reached, this must be recorded in a risk register. The profile scoring of the risk identified must also be assessed. The University uses a 5x5 risk matrix which displays graphically the likelihood and consequence of any risk and score that is recorded in the risk register. Risk scoring matrices can be used in order to illustrate and make judgements upon the evaluated risk scores.

The example matrix provides a traffic light system representing where critical (red), high (amber), moderate (yellow) and low (green) level risks may fall.

**Example of a 5x5 risk matrix:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | **Likelihood** |  |  |
|  | **1** | **2** | **3** | **4** | **5** |
| **Consequence and time to recover** | **Rare (<10%)** | **Unlikely (10-30%)** | **Moderate (31-50%)** | **Likely (51-80%)** | **Almost Certain (>80%)** |
| **1 Insignificant** | 1 – low | 2 – low | 3 – low | 4 – low | 5 – moderate |
| **2 Minor** | 2 – low | 4 – low | 6 – moderate | 8 – moderate | 10 – high |
| **3 Moderate** | 3 – low | 6 – moderate | 9 – moderate | 12 – high | 15 – high |
| **4 Major** | 4 – low | 8 – moderate | 12 – high | 16 – critical | 20 – critical |
| **5 Extreme**  | 5 – moderate | 10 – high  | 15 – critical | 20 – critical | 25 – critical  |

**Key:**

* **Low Risk:** Acceptable risk and no further action required as long as risk has been minimised as possible. Risk needs to be reviewed periodically
* **Moderate Risk:** Tolerable with further action required to minimise risk. Risk needs to be reviewed periodically
* **High Risk:** Tolerable with further action required to minimise risk. Risk needs to be reviewed continuously
* **Critical Risk:** Unacceptable risk and action required immediately to minimise risk where this is possible

It is usual risk management practice for probability to be multiplied by impact in order to quantify risk and enable the comparative mapping of key risks. Evaluated risks are mapped into a scoring matrix in order to enable comparison between risks and to facilitate focused monitoring
and review.

Very low scoring risks will usually be discarded for risk register purposes unless there is a clear indication that these may increase over time.

The University may determine that a risk with a high impact is more significant than a risk with a high probability, for example the risk of a natural disaster occurring which directly affects the University. Or that a risk with a high probability but low impact is more significant, for example the risk of errors in payments to suppliers, or that both impact and probability are equally significant.

Stage 3 – Manage:

The original risk profile score shows the likelihood and impact of the risk before any controls are in place to manage the effects of a risk. When we are considering how to treat risks, we must identify the resources available for us to implement internal controls. These resources may include people, systems, equipment or time. These are known as mitigating controls and once identified; these should also be recorded within a risk register.

Once mitigating controls have been agreed all original risks should be re-scored in terms of impact and likelihood to produce a current risk profile. The revised score is displayed graphically alongside the original risk score to show the effectiveness of the controls in place. Completion of a matrix for inherent and residual risk and comparison of these will provide insight into the effectiveness of the University’s risk management practice and our reliance upon internal control.

Risks are recorded in a risk register by department and ownership of the risk is assigned to the most appropriate employee in the department. The owner of the risk is responsible for ensuring that reporting and monitoring of risk performance, actions and events takes place regularly, at least quarterly. The risks need to be formally reviewed with any changes agreed updated within the risk register.

Some risks cannot be mitigated as they are out with the University’s direct control (e.g. flood or regional power failure) therefore a Business Continuity and Disaster Recovery plan will be required.

Stage 4 – Review:

There will be a regular review of the Risk Management procedures and arrangements for the review and updating of the Risk Policy and Guidance Document. Part of this process will be to ensure that Departmental Risk Registers are in alignment with University’s strategic objectives.

The risk matrix may also be used to identify where risk has increased, decreased, remained static or been added as a new risk over time in order to focus Audit Committee and management review.

**Types of Risk Register**

The risk register is the output from the evaluation of risk and drives achievement of the risk appetite and any action to reduce the likelihood that risk will be realised. We use Risk Registers to document and record risks we have identified and what we intend to do about them. This demonstrates the management of risk within the University and also, by setting out everything we do and reviewing this regularly (at least quarterly), allows us to consider if we are doing enough to control each risk or whether our resources would be better used elsewhere.

**Strategic risk register** – this will identify key strategic risks to the University. This level should be set to ensure that review and monitoring of the register is not overly bureaucratic and cumbersome but is comprehensive enough to ensure that all risks which require monitoring are reviewed effectively so as not to expose the University to strategic risks being realised.

For example, the University may monitor risks rated as red/high in the strategic risk register at governing body level and lower level risks as part of ongoing management review.

**Operational risk registers** – these will identify key operational risks to the University within the specific academic and support divisions or departments. Management should take care to ensure that all cross divisional/ departmental risks are identified and included either in a specific register, within the register of a relevant division/department or if relevant then within the strategic risk register.

**Risk Register template**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Description of Risk and Impact** | **Accountable person**  | **Likelihood** | **Impact**  | **Inherent Risk Score** | **Controls / Mitigating Actions** | **Control Owner** | **Likelihood** | **Impact** | **Residual Risk Score** | **Magnitude of Financial Risk**  |
| Each risk should be worded to clearly identify what the cause and effect of the risk is  | Insert name of person accountable for each risk | Rare (1)Unlikely (2)Moderate (3)Likely (4)Almost Certain (5) | Insignificant (1)Minor (2)Moderate (3)Major (4)Extreme (5) | The level of risk occurring in the absence of any actions management has taken to alter either the risk’s impact or probability: Low Moderate High Critical | The proportionate responses (mitigating actions) selected to manage the risk in the most efficient way of reducing the residual risk  | Insert name of the control owner for each risk  | Rare (1)Unlikely (2)Moderate (3)Likely (4)Almost Certain (5) | Insignificant (1)Minor (2)Moderate (3)Major (4)Extreme (5) | The rating given to the risk after action has been taken to alter the risk’s impact and probability: Low Moderate High Critical | Low: Up to £100kModerate: £100k to 500kHigh: Over £500k |