Risk Management Framework

April 2025

CONTENTS

1. Impact Statement and Objectives

Heriot-Watt University has implemented a robust risk management framework to support the sustainable pursuit of strategic aims, and to ensure resilience and continuity, protecting its community and assets from potential threats. The Risk Management Framework enhances the University's ability to identify, assess, and mitigate risks, safeguarding academic excellence, financial health, and reputation, while ensuring transparency and long-term success.

The five objectives of the University's Risk Management Framework are set out below:

1. **Support Strategic Goals:** Align risk management practices with the University's strategic objectives to enable informed decision-making and sustainable growth.

2. **Enhance Resilience:** Ensure the University can effectively respond to and recover from disruptions, safeguarding its academic and operational continuity.

3. **Protect Reputation and Assets:** Safeguard the University's reputation, financial health, and physical and intellectual assets through proactive risk identification and mitigation.

4. **Foster Innovation:** Encourage a balanced approach to risk-taking that supports innovation and the pursuit of new opportunities in teaching, research, and administration.

5. **Promote Compliance and Ethics:** Ensure adherence to legal, regulatory, and ethical standards to maintain trust and integrity in all university activities.

2. Introduction

The University has established a comprehensive Risk Management Framework to pursue its strategic objectives while managing the inherent risks in its activities. The Framework allows the University to effectively identify, assess, and manage risks across all its operations.

The University's Risk Appetite Statement supports the University in making appropriate risk-based decisions to underpin the implementation of its strategy, and it serves as a key tool within the University's strategic decision-making processes, outlining the level of risk the University is willing to accept in pursuit of its goals.

By regularly reviewing and updating risk registers, and through detailed reporting to the University Executive (UE), Audit and Risk Committee (ARC) of Court, and Court itself, the University ensures that risks are managed proactively. This approach not only helps create value in times of uncertainty but also addresses significant threats to academic and business objectives, financial health, and reputation.

Heriot-Watt University uses horizon scanning to identify and assess emerging trends and potential threats. This proactive approach helps the University anticipate future challenges, evaluate impacts, and make informed strategic decisions to stay resilient and adaptable.

3. Scope

This Framework applies to all types of risk affecting the University, including Strategic, Operational, and Project risks, with the exception of Health and Safety risks which are subject to a separate framework. A risk universe for the University has been defined consisting of 11 risk categories which sets out all types of risk that the University may be subject to and are outlined below.
The Framework applies across the University and the Heriot-Watt Group including across all Campuses, Subsidiaries, and Primary Organisational Units including Professional Services Directorates, Schools, and Global Institutes.

3.1 Risk Categories

The University's Risk Appetite Statement outlines 11 distinct risk categories which define the universe of risks applicable to the University, and sets a risk appetite for each category. This allows the University to direct its attention more effectively to those risks which are outside of the defined appetite, while still encouraging that all risks are mitigated as fully as possible. The following 11 risk categories are defined as follows:

Financial: Risks related to income targets, expenditure management, and financial sustainability.

Reputational: Risks affecting the University's reputation and its ability to attract students, staff, and partnerships.

Compliance: Risks related to adherence to laws, regulations, policies, and health and safety practices.

Environmental Sustainability: Risks involving compliance with sustainability legislation, internal targets, and strategic goals.

People: Risks related to recruiting, maintaining, and developing a high-quality workforce and ensuring a positive student experience.

Information: Risks concerning data security and the University's role as a data controller and processor.

Cyber: Risks of cyber-attacks against the University.

Students: Risks affecting the quality of learning, teaching, and overall student satisfaction.

Infrastructure: Risks related to the University's physical and digital infrastructure supporting its strategic ambitions.

Strategic: Risks impacting the University's ability to achieve long-term strategic objectives.

External: Risks from external events or policies affecting the University's strategy implementation.

3.2 Types of Risk

The University faces into several types of risks which are defined as follows:

Strategic risks encompass the uncertainties and vulnerabilities that may affect the University’s ability to achieve its strategic mission, academic excellence, and financial sustainability against its long-term strategy. Strategic risks include factors such as changing demographics of the student body, shifts in educational trends and demands, evolving technologies, funding uncertainties, competitive pressures, and the ability to adapt to external forces like economic, social, and political changes.

Operational risks encompass the potential for internal disruptions and failures in day-to-day operations that can result in financial losses, reputational damage, and disruptions in the University’s ability to carry out its core functions, including teaching, research, and providing support services. This risk type is primarily associated with internal factors, such as human error, technology failures, regulatory compliance issues, and other operational shortcomings, and financial mismanagement.

Project risks The University's project management policy requires that all significant projects maintain a project risk register to ensure that all risks relating to change projects are effectively identified, managed, and reported in order to achieve the successful outcomes of a project.

4. Risk Management Framework overview

The Risk Management Framework is designed to support the University's sustainable delivery of its strategy. The current strategy, Strategy 2025, is ambitious, aiming to drive significant improvements in student experience, research, and enterprise activities. Strategy 2035, which is under development, is set to be transformative, continuing to push boundaries in education and innovation. As a global university, Heriot-Watt faces significant disruptive changes within the Higher Education sector and society, including geopolitical conflicts, climate change impacts, and the use of Artificial Intelligence. These changes present both risks and opportunities across learning, teaching, research, and operations. To succeed, the University must take appropriate risks in a managed, considered, and controlled way. This Framework is designed to support those goals.

Key elements and management tools within this Framework include the Risk Appetite Statement, the Ethical Business Statement, the Risk Identification and Evaluation Guide, and the University's risk management system, 4Risk. These tools support risk evaluation, recording and management, whilst supporting appropriate risk-based decision-making.

The University also has a Risk Management Improvement Plan which seeks to continuously enhance its risk management practices. This includes continuous feedback and improvement on relevant risk and assurance reporting provided to senior management and governance bodies including the UE, ARC, and Court itself. The Plan also seeks to improve awareness, engagement and training on the Risk Management Framework and risk management more generally.

4.1 Risk Appetite Statement

The Risk Appetite Statement is a key tool within the University's strategic decision-making processes and is designed to support the University in making appropriate risk-based decisions to underpin the implementation of its strategy. It is intended to be used when significant proposals and initiatives are being considered. The University has identified 11 risk categories as set out above within the Statement, each with a defined risk appetite set for each category. Management is required to develop controls and mitigating actions for all risks, but there is a particular focus on risks are outside the defined risk appetite, where there is a requirement to bring those risks within appetite by taking mitigating actions and implementing controls within agreed timeframes.

4.2 Ethical Business Statement

The University is committed to conducting business ethically and responsibly. The University's Ethical Business Statement is treated as part of the Risk Management Framework and outlines the principles and standards that guide the University's actions, ensuring integrity, transparency, and accountability in all dealings. This commitment supports the University's mission to create and exchange knowledge that benefits society while maintaining the highest ethical standards.

4.3 TransNational Education (TNE) Evaluation Framework

The TNE Evaluation Framework provides a high-level summary of TNE partner due diligence and development process, presented in an accessible format for HWU's Committees to demonstrate the effectiveness and robustness of the underpinning partner evaluation, and thereby assure and assist each Committee in its decision-making.

The University's Risk Appetite Statement provides the basis for the TNE Evaluation Framework and they are fully aligned with the principle that risk acceptance processes will be used to transparently document and agree any decisions, including any additional monitoring, oversight, and mitigations which might be required to support approval and implementation of TNE partnerships.

4.4 Risk Identification and Evaluation Guide

The Risk Identification and Evaluation Guide supports staff in the identification, evaluation and rating of risks. It contains detailed descriptions of the types of risks, how to identify, define, and evaluate risks, plus definitions for risk impact and likelihood which can be used to evaluate and rate risks. The purpose of this procedure is to provide a clear and systematic approach to risk management. This procedure is designed to be a practical tool that supports consistent strategic and operational risk management processes across the University.

The five-by-five **Risk Matrix** diagram evaluates the impact and likelihood of risks to assist in the consistent rating of risk. Further definitions and criteria for the likelihood and impact calibration can be found within the Risk Identification and Evaluation Guide.

Severe	**Major**	**Major**	**Severe**	**Severe**	**Severe**
Major	**Moderate**	**Major**	**Major**	**Severe**	**Severe**
Moderate	**Moderate**	**Moderate**	**Major**	**Major**	**Severe**
Minor	**Low**	**Low**	**Low**	**Moderate**	**Moderate**
Insignificant	**Low**	**Low**	**Low**	**Low**	**Low**
Impact/Likelihood	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost Certain**

4.5 Risk Management System – 4Risk

The risk management system used to manage risk at Heriot-Watt University is Insight4GRC ('4Risk'). This system is the repository for the University's institutional Strategic Risk Register, all Operational Primary Organisational Unit (POU), Campuses, and Subsidiary risk registers, plus relevant Strategic Project risk registers.

The system also provides real-time risk monitoring, interactive risk dashboards, action tracking, and an audit trail of changes and updates to registers. System access to view or edit is granted by the Assurance and Legal Services team as required.

The system underpins risk reporting to the UE, ARC, and Court on risk management activities, providing comprehensive insights and facilitating informed decision-making. Those who have been granted permission can access the 4Risk system through the following link https://hw.insight4grc.com/.

5. Continuous Improvement of the Risk Management Framework

The University is dedicated to maintaining and enhancing its risk management practices through various the Risk Management Improvement Plan plus continuous improvement strategies. To achieve this, the University continuously reviews and updates its risk management processes and reporting, integrating feedback and lessons learned from ongoing risk management activities. This proactive approach allows the University to adapt to emerging challenges and opportunities, ensuring that its risk management practices remain robust and effective. Key initiatives include the implementation of the Risk Management Improvement Plan, the Risk Champions Network, Controls Risk Self Assessments (CRSAs), and processes for risk crystallisation, all of which are further outlined below.

5.1 Risk Management Improvement Plan

The Risk Management Improvement Plan is a continuous initiative, reset on an annual basis, which aims to develop and enhance the operation of the University's Risk Management Framework. The plan ensures ongoing improvements are made in risk management practices across the University.

5.2 Risk Champions Network

The Risk Champions Network consists of designated individuals from each POU across the University who have been identified to lead and promote risk management practices within their area. They are responsible for identifying, assessing, and mitigating various risks related to their operational, financial, and administrative functions. This includes analysing both internal and

external factors, gauging the impact and likelihood of risks, and developing strategies to reduce their adverse effects. They also support the awareness and actions required on other risk matters within local Management Teams including Financial Delegations, Business Continuity Planning and supporting audits and reviews undertaken.

Their work also includes supporting local Management to monitor and maintain operational risk registers including assessment of the effectiveness of risk controls and actions, plus escalating significant risks to senior management or relevant governance committees. This network meets quarterly to obtain updates on trending risk and audit matters, discuss feedback from UE Audit and Risk and ARC meetings, and address potential internal and external training needs and requirements.

5.3 Controls Risk Self Assessments (CRSAs)

CRSAs are carried out regularly by Assurance Services with POUs. These guided assessments involve Risk Champions and local management to evaluate and update operational risk registers and review the effectiveness of the listed controls. This process ensures that risk controls remain robust and relevant, supporting the University's Risk Management Framework goals.

5.4 Risk crystallisation

Risk crystallisation refers to risks that have materialised and caused actual impacts. If a risk crystallises then it is important to identify the root causes of these risks and inform necessary changes to systems, processes, and controls. The objectives of conducting lessons learned are to identify the impacts of crystallised risks and manage those impacts through an action plan, review controls and actions that may have been absent or ineffective in addressing the risks and assess whether there were gaps in assurance processes. This proactive approach ensures continuous improvement in the University's Risk Management Framework, enhancing preparedness and response to potential future risks. It is important to note that this practice is new and emerging and is not yet fully in place.

6. Assurance

Assurance in risk management refers to the confidence provided by various processes and controls that risks are being managed effectively. The University uses the 'Four Lines of Defence' model for organising assurance activities. It includes:

First Line of Defence - Management

Includes day-to-day operational management processes and control frameworks.

Second Line of Defence – Independent Internal Review

Involves independent reviews by teams or specialists separate from daily operations. It includes risk and compliance reviews, operational controls reviews, and oversight by Court Committees, ensuring independence and objectivity.

Third Line of Defence – Internal Audit

Provided by Internal Audit, this line is completely independent of management, ensuring objectivity.

Fourth Line of Defence – External Reviews (including External Audit)

Includes external reviews such as those conducted by External Audit and other specifically commissioned external reviews. By nature, these reviews are completely independent of management and objective.

Assurance is gathered on all strategic risks through the lens of these four lines of assurance which provides updates on individual and ongoing assurance work including the outputs of that work and any remedial actions required. An Assurance report is presented quarterly to UE and ARC, providing a detailed overview of the assurance landscape, evaluating strategic risks within each risk category, and the extent of assurance provided by each line. By collating and presenting assurance in this structured manner, the University can identify gaps, strengthen controls, and enhance overall risk management practices.

6.1 Internal Audit and Assurance

As noted above, the third line of defence is Internal Audit. Internal Audit at Heriot-Watt University is carried out by an outsourced auditing firm (RSM) to ensure independent oversight of internal control systems. The auditor provides recommendations to improve internal processes, mitigate risks, and enhance overall efficiency and value-for-money, and to offer assurance to the University's

management and governing body that operations are running effectively within a robust financial control framework.

The auditor independently evaluates and assesses various aspects of the University's operations, ensuring compliance with regulations and proper controls, and their insights contribute to the University's overall governance and risk management efforts.

The auditor reports directly to the University Secretary and the ARC, providing updates on the internal control system.

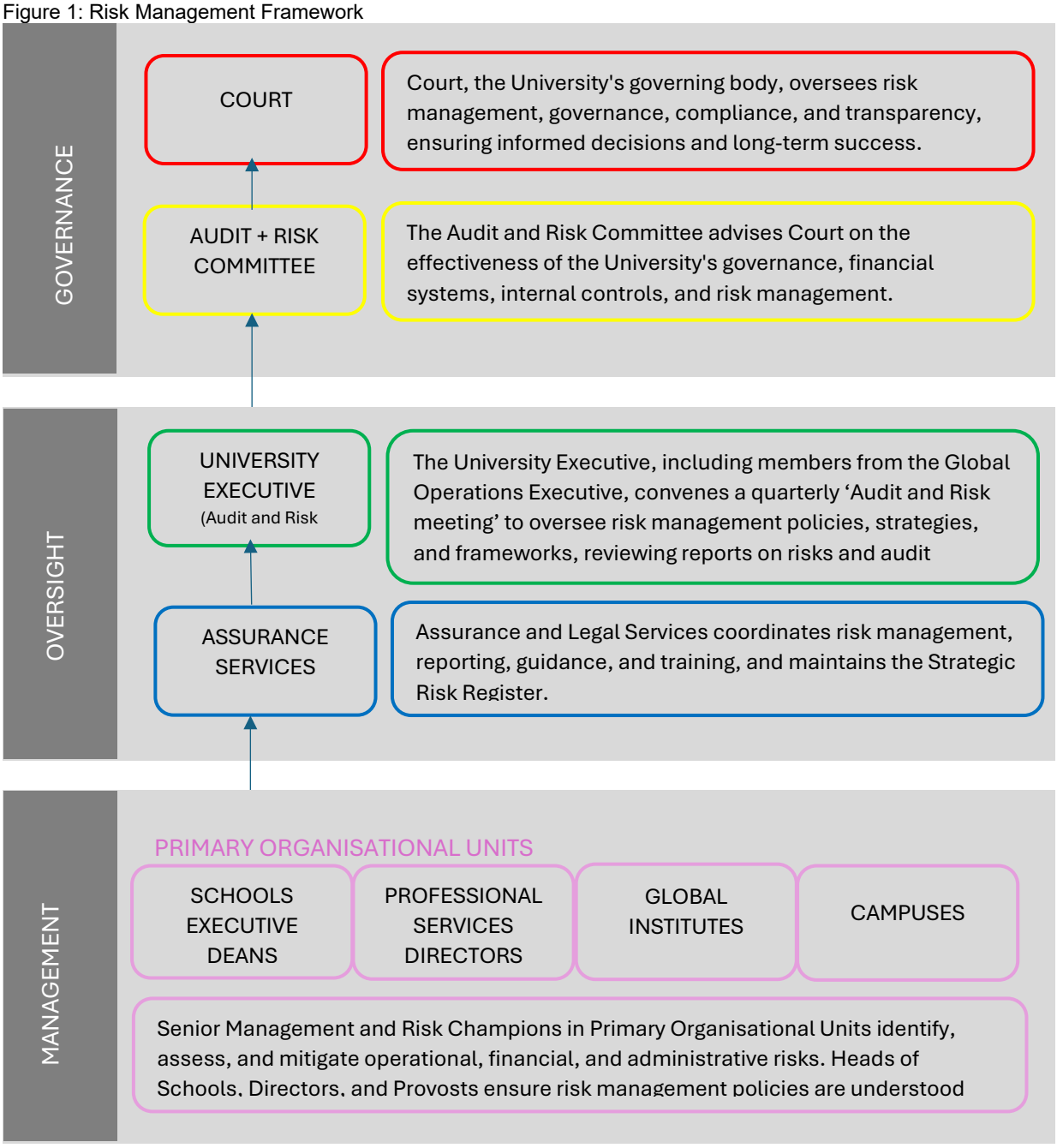
The auditor develops an audit strategy and plan, considering the entire governance framework and other assurance mechanisms, reviewed and approved annually by the ARC.

The UE is responsible for evaluating risks and establishing effective risk management processes, as well as acting on audit reports and recommendations. Regular reports are provided to the ARC on the status of audits and reviews, key findings and emerging themes, management's implementation of recommendations, and significant changes to the Internal Audit Plan based on new or emerging risks.

7. Roles and Responsibilities

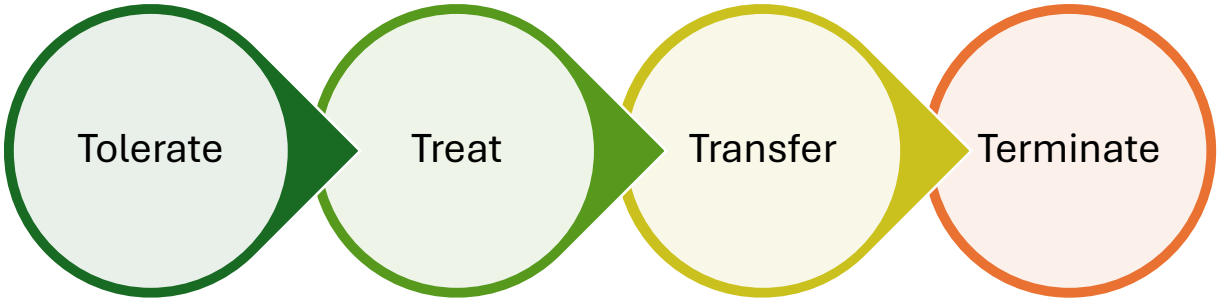
The organisational structure for the identification, management, reporting and oversight of risks within the University is established, with well-defined stakeholders and lines of reporting in place. The specific groups which are outlined in the diagram below have defined roles within the Risk Management Framework, ensuring that risks are identified, assessed, and managed and reported appropriately. This structured approach promotes accountability and ensures that significant risks are escalated to senior management or relevant governance committees for further action.

Figure 1: Risk Management Framework



8. Risk Management

The University follows 'the 4 Ts' of risk management: Treat, Transfer, Tolerate, and Terminate.



Treat: This involves taking actions to reduce the impact or likelihood of a risk. This could include implementing new processes, controls, or safety measures to mitigate the risk.

Transfer: This means moving the risk to another party. Common methods include purchasing insurance (see 8.1 below) or outsourcing certain activities to third parties who may be able to manage the risk more effectively.

Tolerate: Sometimes, it may be appropriate to accept the risk, if it is within risk appetite and especially if its impact is minimal or the cost of mitigation is higher than the potential loss. This involves monitoring the risk and being prepared to manage a suitable response if it crystalises.

Terminate: This involves eliminating the risk entirely by discontinuing the activity that generates the risk. If a particular process or project poses significant risks, it might be best to stop it altogether.

These strategies provide a comprehensive framework for managing risks. By understanding and applying these principles, the University ensures that risks are identified, assessed, and managed effectively.

8.1 Insurance

In order to effectively transfer risk (the third 'T'), the University holds comprehensive insurance policies across all lines of business, including Liability, Property, Business Interruption, and a number of supplementary policies.

9. Related Policies, Procedures and Further Reference

- Risk Appetite Statement
- Risk Identification and Evaluation Guide
- TransNational Education (TNE) Framework
- Ethical Business Statement
- Health and Safety Risk Guidance: Risk Assessment and Guidance Risk Assessments