

ENTERPRISE RISK MANAGEMENT POLICY

SCOPE

This policy applies to all Monash University staff.

For the purpose of this policy, references to 'the University' includes activity at Monash University Australia, Monash University Indonesia, Monash University Malaysia, Monash Suzhou, the Monash University Prato Centre, Monash College, and World Mosquito Program Ltd (and its subsidiaries), unless indicated otherwise.

POLICY STATEMENT

Monash University (the University) characterises risk as the effect of uncertainty on the University's objectives. Effective risk and compliance management supports the University to achieve its goals and protect its reputation. This policy outlines the University's approach to manage risk and compliance effectively and foster a culture where risk management is an enabler of informed decision making.

The Risk and Compliance Unit (RCU) may provide risk and compliance management services to associated entities or strategic partnerships, under the direction of the Vice-Chancellor's Group (VCG), the Vice-Chancellor's Executive Implementation and Oversight (VCEIO) Committee or on request by the management of these entities and/or partnerships.

1. General Principles

- 1.1 Risk is inherent in all academic, administrative and operational activities at the University.
- 1.2 Risk and compliance management is essential to good governance.
- 1.3 Risk management seeks to minimise threats and maximise opportunities through considered decision making. Such decision-making is guided by the University's [Risk Appetite Statement](#).
- 1.4 The risk management process includes risk assessment, treatment and review. Further details on each of these activities can be found in the University's [Risk Management Manual](#) and instructions for assessing and treating risks can be found in the [Risk Assessment Guidance and Definitions](#).
- 1.5 All staff share responsibility for the management of risk and compliance across the University's operations. The degree and nature of this responsibility is guided by the staff member's role, as set out in the [Enterprise Risk Management Procedure](#). Staff should familiarise themselves with risks associated with their roles and responsibilities.
- 1.6 Risk and compliance management applies to all University activities and should be integrated into existing processes such as planning, project management, decision making and reporting; this ensures accountability for risk and compliance management across the University.
- 1.7 Regulatory compliance is consistent and must be to the highest standard. The compliance mechanism(s) should also be efficient.
- 1.8 Risk management is proactive and helps reduce uncertainty in obtaining the University's objectives.

2. Managing Risk at Monash University

- 2.1 The Enterprise Risk Management (ERM) framework is underpinned by four [risk pillars](#).
 - **Key Risk:** risks to strategic objectives. These risks can relate to any aspect of University business and are guided by sources such as the Operational Risks, [University plans](#), major projects and other specialist advice within the University.
 - **Operational Risk:** risks associated with transactional activities undertaken as part of day-to-day operations, such as the payment of invoices, enrolling students and scheduling of classes, including contractual compliance.
 - **Regulatory Risk:** risks associated with regulatory compliance. These risks are driven by the University's regulatory obligations arising from legislation (e.g. Foreign Influence Transparency Scheme, Autonomous Sanctions, Defence Trade Control) and mandated codes such as the [Australian Code for the Responsible Conduct of Research](#).
 - **Project Risk:** risks associated with individual projects. All projects carry a certain degree of risk, which must be considered according to each project's unique circumstances and project management arrangements.

2.2 Risks relating to health and safety are covered in the [Occupational Health, Safety and Wellbeing Policy](#).

Risk Appetite Statement

2.3 The University's [Risk Appetite Statement](#) (RAS) sets out the degree of risk the University is prepared to accept in its activities. It is reviewed annually by VCG and Audit and Risk Committee and approved by Council.

2.4 The RAS needs to be considered as part of University planning and in making decisions to ensure risk-taking activity is acceptable.

2.5 Local areas may develop their own risk appetite statements. These statements must be subordinate to the University's RAS.

Assessing Risk

2.6 Risk assessments are used to generate a risk rating. This risk rating forms the basis for prioritising and consistently managing the risk in accordance with the University's RAS. Risk assessments are part of each staff member's risk management responsibilities.

2.7 Circumstances that require staff to undertake risk assessments include, but are not limited to:

- identification of an emerging key or operational risk that could have a significant impact on the University;
- a request from an internal stakeholder (such as senior management, Office of General Counsel, Insurance Services, or Monash Innovation);
- a requirement of a Monash Policy and/or Procedure;
- a major initiative; or
- commencement of a new project (see [Project Management Central](#)).

2.8 All risk assessments and the treatment of risks must adhere to the [Risk Assessment Guidance and Definitions](#). Exceptions to this must be approved by the RCU.

Three Lines of Defence

2.9 The University adopts a 'three lines of defence' model to support accountability in risk management through a layered defence approach. These lines of defence are:

- 1st – risk owners
- 2nd – standard setters; and,
- 3rd – independent assurance providers.

2.10 Further information can be found in the [Risk Management Manual](#).

Authority for Risk Management

2.11 Monash University Council has responsibility for overseeing and monitoring the management of risk across the University's operations, including its commercial activities.

2.12 The Audit and Risk Committee of Council is responsible for advising the University in meeting these obligations.

2.13 The RCU is the operational unit that assists in the management of strategic, operational, regulatory and project risks under the [Risk and Compliance Charter](#) approved by the Audit and Risk Committee. It is responsible for the co-ordination and implementation of the ERM Framework. The RCU is also a source of advice to the staff of the University. The RCU sits within the Deputy Vice-Chancellor & Senior Vice-President (Enterprise and Governance) and works closely with other staff to embed risk ownership at all levels of the University.

DEFINITIONS

Risk	The effect of uncertainty on objectives.
Risk appetite	The type and level of risk that an organisation is prepared to pursue, retain or take.
Risk assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk management	Coordinated activities to direct and control an organisation with regard to risk.
Risk management framework	The set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout the organisation.
Risk owner	University staff member with the accountability and authority to manage a risk.
Risk treatment	Process to modify risk, may include deciding to accept, reduce, share or avoid the risk.

Standard setters	University staff/functions responsible for providing specialist advice to risk owners and setting the approach, processes and frameworks for risk management. (e.g. RCU and Office of General Counsel)
Independent assurance providers	University functions responsible for providing independent assurance and oversight on how effectively the University manages risk (e.g. Internal Audit).
Supervisor	Someone who supervises a staff member's work (e.g. Head of Department, Dean, Director or Project Director).

GOVERNANCE

Supporting procedures	Enterprise Risk Management Procedure
Supporting schedules	N/A
Associated policies	Electronic Information Security Policy Industry-Based Experiences for Students Policy Occupational Health, Safety and Wellbeing Policy
Related legislation	Monash University Act 2009 (Vic) Tertiary Education Quality and Standards Agency (TEQSA) Act 2011 Higher Education Standards Framework (Threshold Standards) 2021
Category	Governance
Approval	Monash University Council DATE: 11 December 2019 Meeting 8/2019/Agenda Item 10.2.2
Endorsement	Audit and Risk Committee DATE: 29 November 2019 Meeting 4/2019/Agenda Item 5
Policy owner	Director, Risk and Compliance
Date effective	16 December 2019
Review date	16 December 2022
Version	4.2 (<i>minor amendment effective 6 August 2022</i>)
Content enquiries	riskandcompliance@monash.edu