MONASH University

ENTERPRISE RISK MANAGEMENT PROCEDURE

SCOPE

This policy applies to all staff at all Monash University locations, including its controlled entities.

PROCEDURE STATEMENT

This procedure outlines how Monash University (the University) manages risk effectively, and sets out the procedures for staff involved in risk management.

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

1. Responsibilities for Risk Management

Risk and Compliance Unit

1.1 The RCU works collaboratively with University staff to manage strategic, operational, regulatory and project risks. The RCU's key responsibilities include:

- delivering and ensuring the review of the University's Risk Appetite Statement;
- developing and implementing risk strategies to deliver the University's Enterprise Risk Management (ERM) framework, in consultation with University staff;
- embedding risk practices and capacity within the University to help foster a culture of risk management;
- working with functional areas, legal compliance officers, committees and risk owners on risk matters;
- supporting the University community in undertaking risk analysis and assessments;
- identifying and consulting on the University's regulatory compliance landscape;
- identifying and reporting on emerging risks and significant events; and,
- promoting awareness of the ERM framework and providing risk management training and education to the University community.

Supervisors and Heads of Departments

1.2 Supervisors and Heads of Departments are responsible for the day-to-day operation of the University. They may be expected to:

- own operational and project risks;
- identify, assess and mitigate operational and project risks;
- contribute to the development of University key risks; and,
- provide expert advice in support of risk assessments.

1.3 For guidance on how to assess and manage risks, see the Risk Assessment Guidance and Definitions, the Risk Management Manual or contact RCU for support.

2. Enterprise Risk Management Framework

2.1 As stated in the Enterprise Risk Management Policy, risk is categorised into four risk pillars, namely; key, operational, regulatory and project risks.

Managing Key Risks

2.2 The RCU manages key risks through the University's Key Risk Profile.

2.3 Risks in this profile are owned by members of the VCG and reviewed by the MIIO committee, the Audit and Risk Committee (ARC) and Council.

2.4 New key risks can be added as part of the annual refresh of the Key Risk Profile.

2.5 The RCU may contact staff nominated by the risk owners to seek their assistance in developing and updating key risk assessments. Assistance can include providing information relating to key risk indicators, commenting on the key risk and assessing the risk ratings.

2.6 Staff are expected to provide timely specialist advice on risk indicators, commentaries and mitigations.

2.7 Any enquiries relating to key risks can be directed to the RCU.

Managing Operational Risks

2.8 The RCU manages:

- the Operational Risk Profile, which captures operational risks the University actively manages or considers to be of notable risk; and,
- the RiskMaps, which catalogue all potential operational risks the University considers adequately managed through existing controls.

2.9 The Operational Risk Profiles and corresponding emerging risks are reviewed through a quarterly process and RiskMaps are reviewed every two years. These are undertaken by RCU in conjunction with the risk owners and/ or managers of functional areas. Updates outside the scheduled reviews can be completed at the risk owner's discretion. For more information, see the Risk Management Manual.

2.10 Risks in this profile are reviewed by members of the VCG, MIIO committee, and the ARC.

2.11 Policy owners are responsible for ensuring policies and procedures in their area address operational risks. The RCU may contact policy owners to understand how policies and procedures address risks.

2.12 Where a local, operational risk register developed outside of the ERM framework exists, owners of such registers are encouraged to contact the RCU to explore potential for these risks to be aligned with equivalent Operational RiskMaps or Risk Profiles.

2.13 Any query relating to operational risks can be directed to the RCU.

Managing Regulatory Risk

2.14 The RCU helps the University capture, understand and meet its obligations to comply with applicable laws and regulations, including the University's own statute and regulations. The RCU does this by engaging with stakeholders throughout the University.

2.15 All staff are encouraged to understand the regulatory environment relevant to their role and/or activities. If uncertain, staff can seek the advice of the relevant Legal Compliance Officer (LCO) and/or RCU to clarify/confirm their regulatory responsibilities.

2.16 All staff can contact the RCU and/or nominated LCO if it is found that appropriate controls have not been put in place to effectively address relevant regulatory obligations.

2.17 All staff must contact RCU about new legislation that needs to be complied with by the University either due to changes to the law and/or commencement of new activities within the University.

2.18 Policy owners are responsible for ensuring the policies and procedures they develop and review adequately address relevant regulatory obligations, and the RCU and policy owners are expected to have ongoing interactions. For example, the RCU may seek a policy owner's input in understanding policy changes and policy owners may seek RCU's advice in understanding implications to University policies as a result of legislative changes.

Legal Compliance Officers

2.19 LCOs provide a local point of contact and expert knowledge on specialised regulatory matters. They are nominated based on their expertise and appointed by the RCU. LCOs work with RCU to identify regulatory obligations relevant to their functional expertise. They are expected to:

2.19.1 work with policy owners to ensure that compliance obligations are reflected in relevant policy and procedures and/or other controls;

2.19.2 provide advice to the University community on the implications of new or amended legislation;

2.19.3 assist with the maintenance of the University's compliance management system by responding to notifications by the RCU of changes to regulatory obligations;

2.19.4 inform the RCU when they become aware of changes to activities undertaken within their area that may affect the regulatory obligations the University is required to monitor;

2.19.5 educate and promote a culture of regulatory compliance; and,

2.19.6 complete periodical reviews of the regulatory obligations they monitor using a set of ‘Self-Assessment Questions’ (SAQ) as a tool to map compliance with specific obligations.

Managing Project Risks

2.20 Staff required to conduct a risk assessment for a project should use the Project Risk Assessment Template with reference to the Risk Assessment Guidance and Definitions and the University Risk Appetite Statement. The RCU can be contacted for support.

2.21 Project risk profiles can be reviewed and approved by supervisors, heads of departments projects sponsors, project committees, VCG and/or Council.

3. Recording and Reporting

3.1 The following reports are produced through the RCU.

Title	Content	Stakeholders consulted	Oversight and/or approval	Frequency
Key Risk Profile	Profile of Key Risks to the University including associated Key Risk Indicators.	Risk owners and KRI contributors	VCG, MIIO, ARC and Council	Annually (Q1) with an update in Q3.
Operational Risk Profile	Profile of existing and emerging operational risks.	Risk owners and functional leads	VCG, MIIO and ARC	Quarterly
Regulatory Compliance Bulletin	Bulletin of regulatory updates relevant to the University and notable changes to policies with regulation mandating compliance	Policy Team, LCOs, OGC and policy owners	N/A (Distributed to staff)	Quarterly
Annual Regulatory Compliance Report	Report of all regulatory updates relevant to the University and notable changes to policies with regulation mandating compliance throughout the year	Policy Team, LCOs, OGC and policy owners	Vice President (Strategy and Governance) and ARC	Annually (Q4)
University Risk Appetite Statement	Identifies risk appetite and tolerances for the University	VCG, ARC and Council	VCG, ARC and Council (Published to staff)	Annually (Q1)
RCU status report	Update of activities undertaken by RCU across the four risk pillars.	N/A	Vice President (Strategy and Governance) and ARC	Quarterly

DEFINITIONS

Legal Compliance Officers	Nominated University staff members with expertise and knowledge of University activities regulated by particular legislation through their responsibilities in an area of the University's operations. Legal Compliance Officers work with the Risk and Compliance Unit to assess legislation for compliance obligations.
Policy owner	The body or position with the responsibility or delegated responsibility to oversee the development, implementation and review of a policy.
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	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 with the accountability and authority to manage a risk

GOVERNANCE

Parent policy	Enterprise Risk Management Policy
Supporting schedules	N/A
Associated procedures	• OHS Risk Management Procedure • Work Integrated Learning Student Placement and Cocurricular Internship Procedures • Electronic Information Security – Information Classification Procedure
Legislation mandating compliance	• Monash University Act 2009 (Vic) • Tertiary Education Quality and Standards Agency (TEQSA) Act 2011 (Vic) • Higher Education Standards Framework (Threshold Standards) 2015 (Vic)
Category	Governance
Approval	Audit and Risk Committee DATE: 29 November 2019 4/2019 / Agenda item 5
Endorsement	Vice-President, Strategy and Governance DATE: 26 November 2019
Procedure owner	Director, Risk and Compliance
Date effective	16 December 2019
Review date	16 December 2022
Version	4.0
Content enquiries	riskandcompliance@monash.edu