ENTERPRISE RISK MANAGEMENT PROCEDURE

SCOPE

This procedure applies to all Monash University staff.

For the purpose of this procedure, 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.

PROCEDURE STATEMENT

This procedure outlines how Monash University (the University) manages risk effectively, and sets out the procedures for staff involved in risk and compliance 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 Vice-Chancellor's Executive Implementation and Oversight (VCEIO) Committee or on request by the management of these entities and/or partnerships.

1. Responsibilities for Risk and Compliance 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 Apetite 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;
- escalating reports of non-compliance to senior management and governance committees, as appropriate;
- following up and recording the resolution of non-compliance reports; 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, regulatory, and project risks;
- identify, assess and mitigate operational, regulatory, and project risks;
- contribute to the assessment of University key risks;
- provide expert advice in support of risk assessments;
- promote and maintain a culture of compliance and accountability by providing training, recording and reporting on regulatory compliance; and
- ensure that regulatory non-compliance is reported to the RCU, senior management and governance committees.

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, the ERM framework is underpinned by four risk pillars, namely; key, operational, regulatory and project risks.

Managing Key Risks

2.2 The RCU assists in the management of key risks through the development, maintenance, and review oof the University's Key Risk Profile.

2.3 Key risks are owned by members of the VCG and reviewed by the Vice-Chancellor's Executive Implementation and Oversight (VCEIO) Committee, the Audit and Risk Committee (AR&C) and Council.

2.4 New key risks can be added a part fo 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 mitigation measures.

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

Managaing Operational Risks

2.8 The RCU develops, maintains, and reviews:

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

2.9 The Operational Risk Profile and corresponding emerging risks are reviewed periodically and RiskMaps are reviewed every two years. These reviews 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, VCEIO committee, and the AR&C.

2.11 Policy owners are responsible for ensuring policies and procedures in their area manage operational risks. The RCU may contact policy owners to understand how policies and procedures manage such 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 the 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 identify, 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 Any staff member can contact the RCU and/or nominated LCO if it is found that appropriate controls have not been put in place to effectively manage relevant regulatory obligations.

2.17 Any staff member who becomes aware of new legislation that applies to the University, either due to changes to the law and/or commencement of new activities within the University, must contact the RCU accordingly.

2.18 Policy owners are responsible for ensuring the policies and procedures they develop and review will ensure compliance with 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 the RCU's advice in understanding the implications for University policies as a result of legislative changes.

Legal Compliance Officers (LCO)

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 the 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 among relevant staff;

2.19.6 report any regulatory non-compliance to senior management and governance committees (as appropriate); and

2.19.7 complete periodic 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 department, project 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, VCEIO, A&RC and Council	Annually (Q1) with an update in Q3.
Operational Risk Profile	Profile of existing and emerging operational risks.	Risk owners and functional leads	RCU	Quarterly
Regulatory Compliance Update	Regulatory updates relevant to the University and notable changes to policies relevant to regulatory compliance	Policy Team, LCOs, OGC and policy owners	N/A (Distributed to staff)	As required
Annual Regulatory Compliance Report	Report of all regulatory updates relevant to the University and notable changes to policies with relevance to regulatory compliance throughout the year	Policy Team, LCOs, OGC and policy owners	President and Vice-Chancellor and A&RC	Annually (Q4)
University Risk Appetite Statement	Identifies risk appetite and tolerances for the University	VCG, AR&C and Council	VCG, A&RC and Council (Published to staff)	Annually (Q1)
RCU Key risk briefing	Events and issues arising that could affect the University's key risks, and the identification of new and emerging risks	University community as required	President and Vice-Chancellor and A&RC	Every two months
Non-Compliance	Report of contractual and regulatory non-compliance(s), mitigative actions and resolutions	Risk owners, LCOs and/or functional leads	President and Vice-Chancellor and A&RC	NA

DEFINITIONS

Legal Compliance Officer	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
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	Audit and Risk Committee 29 November 2019 4/2019/Agenda item 5
Endorsement	Vice-President, Strategy and Governance 26 November 2019
Procedure owner	Director, Risk and Compliance
Date effective	16 December 2019
Review date	16 December 2022
Version	4.2 (*minor amendment effective 23 August 2022)*
Content enquiries	riskandcompliance@monash.edu