Category: Governance and Management
Version: 10
Document Type: Policy
Document Status: Published
Approved On: 07 December, 2022
Audience: Staff, Research, Academic
Effective Date: 07 December, 2022
Review due by: 03 December, 2025
Policy Approver: Council
Policy Steward: General Counsel And Executive Director, Legal And Risk
Supporting Process:

Governance and Management Processes

Risk Management Policy (MPF1194)

1. Objective

1.1. The objectives of this policy are to:

a) outline the University's approach to risk management;

b) align the University with best practice AS/NZS ISO 31000:2018 Risk management – Guidelines;

c) establish priorities that enable the University to continue to create value and maintain core operations;

d) establish the roles and responsibilities of staff in risk management; and

e) affirm the University's commitment to developing a compliance management framework in line with AS ISO 19600:2015 Compliance management systems – Guidelines, incorporating a risk-based approach to compliance that supports compliance with legislation and regulation (University's Regulatory Framework).

2. Scope

2.1. This policy applies to staff and honorary appointees of the University, and to people authorised to undertake University business.

3. Authority

3.1. This policy is made under the *University of Melbourne Act 2009* (Vic) and Council Regulation , and supports management of risk according to applicable legislative and regulatory standards and codes to which the University is subject.

4. Policy

4.1. Council, through Council's Audit and Risk Committee (ARC), is responsible for overseeing and monitoring the assessment and management of risk and compliance.

4.2. Risk is managed in accordance with the University's Risk Management Framework developed by Legal and Risk. The Risk Management Framework is approved by the ARC on behalf of Council and informed by the advice from the Risk Management and Compliance Committee (RMCC).

4.3. The management of risk aligns with the University's risk appetite, as approved by Council.

4.4. The Vice-President (Strategy & Culture) oversees the development of the risk appetite statement and advises the University Executive Committee on risk as it relates to strategy and objective setting.

4.5. The Vice-President (Administration & Finance) and Chief Operating Officer advises on and oversees University wide implementation of the:

a) Risk Management Framework that is consistent with AS/NZS ISO 31000:2018 Risk management – Guidelines;

b) Compliance Management Framework that is consistent with AS ISO 19600:2015 Compliance management systems – Guidelines and supports the University's Regulatory Framework;

c) Critical Incident Management that is consistent with Australasian Inter-Service Incident Management System;

d) Business Continuity Program. Business Continuity is managed in accordance with the standards set out in ISO 22301:2019 Security And Resilience - Business Continuity Management Systems - Requirements and is overseen by the Resources and Operations Sub-Committee (ROS) .

4.6. Risk management and compliance obligations are formally integrated into planning processes and management activities and incorporated into ongoing 'business as usual' practices by those with management responsibilities.

4.7. The head of division is responsible for the monitoring and reporting of compliance breaches.

4.8. In the event of a critical incident, the University's response will prioritise:

a) human life, safety and wellbeing;
b) animal life, safety and wellbeing;
c) environmental protection;
d) maintenance of core operations; and
e) the protection of property interests,
taking into account the nature of the incident and relevant circumstances.

5. Procedural principles

5.1. Legal and Risk maintains the:

a) University Risk Register; and
b) University Compliance Obligations Register.

5.2. Legal and Risk:

a) provides risk management advice and training;
b) provides compliance training; and
c) documents process in support of risk management.

5.3. Legal and Risk is responsible for internal audits, taking into account any recommendations made by Risk Management and Compliance Committee in relation to the conduct of risk-related audits.

5.4. The Vice-President (Administration & Finance) and Chief Operating Officer is responsible for:

a) developing and implementing a University-wide business continuity planning and management program;

b) developing and implementing a University-wide critical incident management program;

c) developing processes to align with the Australian Inter-service Incident Management System; and

d) coordinating the University's response to any critical incident or major business disruption that may occur, in accordance with the critical incident management and business continuity program described in section 5.4(a and b) and the relevant University policies and processes.

5.5. Risks are identified and managed so that:

a) activities on behalf of the University are performed in an informed manner; and

b) areas of risk or potential risk undertaken in day-to-day activities are the responsibility of staff, including persons authorised to undertake University business and/or activities (eg service providers and contractors).

5.6. Staff, including people authorised to undertake University business and/or activities (eg service providers and contractors) have a responsibility to comply with legislative and regulatory compliance obligations so that:

a) activities on behalf of the University comply with applicable laws and related University policies, and are performed in an ethical, lawful and safe manner; and
b) they are aware of areas of legislation/regulation that affect their day-to-day work.

5.7. A breach of the University's compliance obligations may result in disciplinary and/or legal action.

6. Roles and responsibilities

Role/Decision/Action	Responsibility	Conditions and limitations
Oversee and monitor the assessment and management of risk and compliance	Council	Through Council's Audit and Risk Committee (ARC)
Oversee development of the University's Risk Register	Vice-President (Administration & Finance) and Chief Operating Officer	In collaboration with Strategy, Planning and Performance. Taking into account any recommendations by RMCC. To be approved by Council through the Council's Audit and Risk Committee.
Oversee development of the risk appetite statement	Vice-President (Strategy & Culture)	In collaboration with Legal and Risk Taking into account any recommendations by RMCC To be approved by Council through the Council's Audit and Risk Committee
Develop the University's Risk Management Framework	Legal and Risk	In collaboration with Strategy, Planning and Performance Taking into account any recommendations by RMCC To be approved by Council through the Council's Audit and Risk Committee
Develop the University's risk management process for assessing, evaluating and treating risk	Legal and Risk	To be approved by the Vice-President (Administration & Finance) and Chief Operating Officer
Incorporate risk management, including compliance obligations and business continuity management, into business practices	Management	

Provide risk advice to the University Executive Committee	Vice-President (Strategy & Culture) Vice-President (Administration & Finance) and Chief Operating Officer	Taking into account any recommendations by RMCC
Maintain University Risk Register	Legal and Risk	
Support the development of any divisional, project / operational risk registers	Legal and Risk	
Maintain and administer Enterprise Risk Management System (ERMS)	Legal and Risk	
Provide advice, training and documentation of process to support management of risk	Legal and Risk	
Conduct internal audits to support the management of risk and compliance obligations	Legal and Risk	Taking into account recommendations from RMCC and ARC in relation to risk-related audits
Develop and implement a University-wide critical incident management program	Health and Safety	Program to be reviewed and approved annually by the Vice-President (Administration & Finance) and Chief Operating Officer, informed by advice from RMCC
Coordinate the University's response to any critical incident that may occur	Incident Coordinator	Supported by the University's Incident Management Team
Develop and implement a University-wide business continuity program	Vice-President (Administration & Finance) and Chief Operating Officer	Program to be approved by the Vice-President (Administration & Finance) and Chief Operating Officer, informed by advice from ROS
Maintain business continuity plans	Deans and Portfolio Heads	Supported by the University's Business Continuity and Resilience team
Identify and manage risk - perform day to day activities in an informed manner adhering to relevant compliance obligations	Staff including persons authorised to undertake University business and/or activities (e.g. service providers and contractors)	Identification of risk and non-compliance to be raised/reported to the next most senior person for assessment
Administer this policy, including informing and assisting staff on compliance issues and consider complaints of compliance breaches	Legal and Risk	

Maintain University-wide Compliance Obligations Register	Legal and Risk	
Develop and implement Compliance Management Framework	Legal and Risk	
Compliance with relevant compliance obligations	Staff, students, contractors and service providers	
Identify and mitigate compliance risks	Obligation owner	
Deliver specific compliance training	Legal and Risk	As identified by the compliance owner in conjunction with Legal and Risk
Manage and report non-compliance	Obligation owner	Reporting of non-compliance to Legal and Risk and / or Regulators as required

7. Definitions

Business continuity planning and management means a process that supports alignment of business planning with potential threats to an organisation and the impacts to business operations; and provides a systematic approach for building organisational resilience and response.

Compliance means meeting the University's compliance obligations.

Compliance obligations has the same meaning as in the Compliance Management Framework.

Compliance obligations register means a comprehensive list of the compliance obligations of the University's functions and activities.

Critical incident means an event that may adversely affect the university and requires an immediate response. It is likely to cause significant personal illness or injury, substantial impact to operations and commercial prospects, a degradation of reputation, or lead to an impact on the wider community.

Risk means the effect of uncertainty on objectives.

Risk management means the coordinated activities of identifying, assessing and controlling threats or risks to the University and its activities.

Risk register means the comprehensive list that describes the type of risk and related characteristics, including risk owners; inherent, residual and target risk ratings; controls in place and control effectiveness; and treatment plans.

University Risk Register means a detailed record of risks that could impact the ability of the University to achieve its strategy/long term ambitions. These risks in the register require oversight at the institutional level.

POLICY APPROVER

Council

POLICY STEWARD

General Counsel and Executive Director, Legal & Risk

REVIEW

This policy will be reviewed by 3 December 2025.

VERSION HISTORY

Version	Approved By	Approval Date	Effective Date	Sections Modified
1	Council	8 July 2013	8 July 2013	N/A
2	Governance and Nominations Committee authorised by Council	23 June 2016	21 July 2016	New version arising from the Policy Consolidation Project, incorporating the Risk Management Policy (MPF1194), Risk Management Procedure (MPF1097) and Compliance Policy (MPF1100).
3	Council	24 August 2017	28 August 2017	Roles and responsibilities updated to improve clarity.
4	University Secretary	24 May 2019	31 May 2019	Amended titles in Sections 4 and 6.
5	Vice-Chancellor on behalf of Council under Section 5(5) Vice-Chancellor Regulation	31 July 2019	1 August 2019	Amended titles in Section 5 and 6.
6	Council	3 December 2019	12 December 2019	Roles and responsibilities updated. Clarification of approach to compliance, critical incident and business continuity management.

7	Policy Officer	5 October 2020	5 October 2020	Corrected references to 'University Executive' to 'University Executive Committee'.
8	Executive Director, Legal & Risk and General Counsel	5 July 2022	8 July 2022	5.6. changed from 'including people' to 'and people'.
9	Council	7 December 2022	7 December 2022	Revised wording and responsibilities for Business Continuity Program. Corrected references from ‘RMAG’ to ‘RMCC’.
10	Policy Officer	7 December 2022	7 December 2022	Amended formatting to fix metadata error.