

# Risk Management Policy

## Section 1 - Purpose

(1) The purpose of this policy is to set out the key principles and expectations to support the effective management of risks to RMIT's activities, objectives and strategy, and promote transparency and integrity in the University's decision making.

## Section 2 - Overview

(2) RMIT University is a public institution under Victorian law and stands on Aboriginal Country of the Kulin Nation. RMIT recognises and acknowledges the [Bundjil Statement](#) that helps all RMIT staff to respectfully work, live and study on Aboriginal Country.

(3) This policy outlines the University's approach to risk management which is based on the international standard ISO 31000 and describes the key principles and responsibilities to facilitate the effective management of risks across the University.

## Section 3 - Scope

(4) This policy applies to all employees, researchers and contractors of RMIT, its controlled entities and to any other person notified that this policy applies to them.

## Section 4 - Policy

### Principles

(5) Risk management activities operate under RMIT's risk management framework. Adherence to this framework enables the University to have a consistent approach for managing risks across the University.

(6) Everybody in RMIT plays a role in the management of risks. The Three Lines of Defence Model supports effective enterprise risk management by distinguishing roles and responsibilities within RMIT's risk management framework.

(7) Risks are inherent in the activities, markets and countries in which RMIT operates. They are considered as part of all key conversations, analysis, recommendations, and decision making.

(8) Risk management takes account of any RMIT thresholds and limits that are set out in policies and procedures, delegations of authority, and other measures.

(9) Risks change over time. Risk are monitored and reviewed to ensure decisions regarding risks remain relevant and appropriate.

### Responsibilities

(10) All employees, researchers and contractors are responsible for:

- a. understanding their role and responsibilities, and appropriately managing the risk requirements associated with their day-to-day activities.
- b. identifying, understanding and managing any relevant or emerging risk matters related to their activities, role or area of responsibility.
- c. developing appropriate action plans when they decide to manage a risk by reducing the risk exposure.
- d. ensuring that relevant stakeholders who may be impacted by their decision to accept a risk without putting in place actions to further mitigate it, are aware and understand the potential consequences.
- e. appropriately documenting risks, controls, action plans and risk decisions within their area of responsibility or influence. This will help them to better understand their risks and communicate them to others.
- f. continuing to monitor and review risks within their area of responsibility or influence.
- g. reporting and escalating any actual or perceived risks that may impact the University as they become known. If there is uncertainty regarding who to raise risks with, speak to the Central Risk Management team, Chief Audit and Risk Officer or the Legal Services Group.

(11) RMIT University Council (Council) is responsible for:

- a. overseeing and monitoring the assessment and management of risk across the University, including University commercial activities, in accordance with the [Royal Melbourne Institute of Technology Act 2010](#) (Vic).
- b. ensuring a sound system of risk oversight, with appropriate policies and processes for management, internal control and external oversight, in accordance with the RMIT Council Governance Charter.

(12) Audit and Risk Management Committee is responsible for:

- a. acting on behalf of Council to monitor the audit controls and risk management of the University and associated processes.
- b. reviewing the University's risk profile, risk framework, risk identification and risk management on a regular basis to ensure they are regularly updated, and material business risks of the University are dealt with appropriately and on a timely basis.

(13) Senior Management is responsible for:

- a. exhibiting risk leadership by taking accountability for risk management, dedicating appropriate resources to the management of risks, and implementing risk management processes within their area of responsibility.
- b. promoting a strong risk culture by adhering to limits and thresholds, managing risk exposures, and enabling considered, transparent and risk-aware decisions to be made.

(14) The Central Risk Management team is responsible for:

- a. developing and maintaining RMIT's risk management strategy and framework; this includes the associated risk management policy, processes, guidance and tools.
- b. facilitating and coordinating the regular reporting of risks to Council, the Audit and Risk Management Committee, the Academic Board and Vice-Chancellor's Executive.
- c. advising and supporting teams across RMIT in the effective identification of risks, assessment of risk exposure, and in the development of risk mitigation and monitoring strategies.

## **Breach of this Policy**

(15) Compliance with this policy will be monitored. Non-compliance with this policy may result in disciplinary action.

This may include termination of employment or engagements. If the law is broken, the person or people responsible for the breach may also be personally liable.

## Review

(16) This policy will be reviewed every three years in accordance with the [Policy Governance Framework](#).

## Section 5 - Schedules

(17) This policy includes the following schedules:

- a. [Schedule 1 - Three Lines of Defence Risk Governance Model](#)

## Section 6 - Definitions

(Note: Commonly defined terms are in the RMIT Policy Glossary. Any defined terms below are specific to this policy).

Risk	The effect of uncertainty on the University objectives.
Risk management	Coordinated activities to direct and control the University's activities with regards to risk.
Risk management framework	A set of documents that provide the foundations and arrangements for designing, implementing, monitoring, reviewing and continually improving risk management at the University.
Control	A measure that currently exists which will change the likelihood and/or consequence of a risk. This can include any process, policy, device, practice, action that modifies the risk.
Risk exposure	The extent or severity of the risk expressed in terms of consequence and likelihood.
Risk acceptance	Not undertaking any additional risk mitigations and accepting the current consequences of a risk.
ISO 31000	The International Standard for Risk Management provided by the International Standards Organisation.
Three Lines of Defence Model	A model that delineates the risk management roles across the university in terms of day-to-day management of risks, risk facilitation and assurance.

## Status and Details

<b>Status</b>	Current
<b>Effective Date</b>	19th October 2020
<b>Review Date</b>	19th November 2021
<b>Approval Authority</b>	Audit and Risk Management Committee
<b>Approval Date</b>	3rd September 2020
<b>Expiry Date</b>	Not Applicable
<b>Policy Owner</b>	Clare Lezaja Chief Financial Officer
<b>Policy Author</b>	Tom McLeod Chief Audit and Risk Officer
<b>Enquiries Contact</b>	Central Risk Management team