Risk Management Procedure

Section 1 - Context

(1) The purpose of this document is to provide clear instructions on the specific and prescriptive actions to manage risk in accordance with requirements of the Risk Management Policy.

Section 2 - Authority

(2) Authority for this document is established by the Risk Management Policy.

Section 3 - Scope

(3) This procedure applies to all RMIT Group entities, employees, contractors and third parties undertaking RMIT Group activities in any location.

Section 4 - Procedure

Risk Domains – Minimum Requirements

(4) Risk domains are enterprise-wide categories that help manage risks impacting RMIT's objectives. Risk domains are used to scope or frame risk causes that are validated and controlled in an everchanging risk environment.

(5) Ownership of risk domains reside with members of the University Executive or direct report of the Chief Operating Officer.

(6) The addition or retirement of risk domains is informed by changes to the RMIT Group risk profile. The addition or retirement of risk domains will be approved by the University Executive Committee. The Audit and Risk Management Committee will be informed via the Director of Risk Report.

(7) Amendments to risk domain titles or descriptions are approved by the risk domain owner and updated in the enterprise risk system, Riskware. The University Executive Committee and Audit and Risk Management Committee are informed of amendments to risk domain titles or descriptions via the Director of Risk Report.

(8) Risk domains are assessed using the Risk Exposure Tool, which is based on the Risk Consequence Rating Tool and the Risk Likelihood Rating Tool. The current risk rating for a specific risk domain is informed by the aggregate of the current risk ratings for the tier 1 risks within that risk domain.

(9) All risk domains have a documented Risk Appetite Statement which includes risk posture, risk appetite (limited, balanced or high) risk tolerance statements and metrics for measuring if the risk domain is inside or outside risk appetite. It is the responsibility of the risk domain owner to document the Risk Appetite Statement which is then approved by Council. Enterprise Risk Management will coordinate an annual review of each risk domain's Risk Appetite Statement.

Tier 1 Risks – Minimum Requirements

(10) Tier 1 risks are enterprise-wide subcategories of risk domains for which causes, effect and level of control are identified.

(11) Key characteristics of each tier 1 risk are that they:

a. have a description
b. have an owner who is employed at the Director level or above (including Assistant Directors and Associated Directors)
c. have causes identified which, if not controlled, could lead to the risk materialising
d. are assessed using the Risk Exposure Tool, which is based on the Risk Consequence Rating Tool and the Risk Likelihood Rating Tool. The current risk rating for a tier 1 risk will also be informed by the aggregate of the current risk ratings for tier 2 risks that are linked respective tier 1 risks.

(12) Key characteristics of each cause of tier 1 risks are that:

a. an effect is identified
b. levels of control, including current and target state (across a 1-5 scale) are defined which provide insight into how the cause is being managed
c. treatment plans are documented where current state level of control is below target state
d. controls are identified and documented.

(13) Level of control is an indication of control maturity regarding the management of a specific cause. Current state indicates current control maturity in terms of managing a cause, based on assessment by the tier 1 risk owner and risk domain owner. Target state indicates target control maturity (at the time of assessment) in terms of managing a cause, based on assessment by the tier 1 risk owner and risk domain owner.

(14) It is the responsibility of tier 1 risk owners (or delegate) to embed level of control monitoring into Business as Usual activities and adjust current and target level of controls, and tier 1 risk ratings, as required in Riskware. Rationale will be documented and attached in Riskware explaining the reason for the movement.

(15) A formal review of tier 1 risk ratings, including level of control for each cause, is coordinated by Enterprise Risk Management every 12 months. Any amendments following the review are processed in Riskware by the tier 1 risk owner (or delegate).

(16) At the request of the relevant risk domain owner, Enterprise Risk Management can activate automated notifications from Riskware to inform the risk domain owner (and others as required) when a rating for a tier 1 risk in their risk domain has changed.

(17) Enterprise Risk Management performs sample checking on a periodic basis to confirm tier 1 risks have been rated accurately and adequate rationale is documented in Riskware to support the rating.

(18) The addition or retirement of tier 1 risks is informed by changes to RMIT's risk profile and is approved by the relevant risk domain owner. Audit and Risk Management Committee, University Executive Committee and relevant Council sub-committees are informed via the Director Risk Report.

Tier 2 Risks - Minimum Requirements

(19) Tier 2 risks are specific instances of risk isolated to a portfolio, controlled entity or college.

(20) Tier 2 risks are linked to the most relevant tier 1 risk in Riskware to provide the tier 1 risk owner and risk domain

owner visibility over areas of specific exposure within operational portfolios, colleges or controlled entities. It is the responsibility of the tier 2 risk owner to confirm with the relevant tier 1 risk owner that the linkage is appropriate.

(21) Ownership of tier 2 risks resides at the director level (including Assistant Directors or Associate Directors) or above within the specific college, portfolio or controlled entity that owns the tier 2 risk.

(22) The addition or retirement of tier 2 risks will be informed by changes to RMIT's risk profile. The addition or retirement of tier 2 risks will be approved by the owner of the tier 2 risk profile.

(23) Tier 2 risks will be assessed using the Risk Exposure Tool, which is based on the Risk Consequence Rating Tool and the Risk Likelihood Rating Tool.

(24) A formal review of tier 2 risk ratings will be coordinated by Enterprise Risk Management every 12 months. Amendments to tier 2 risks will be processed in Riskware by the tier 2 risk owner (or delegate). Rationale for the risk rating will be documented in Riskware.

(25) At the request of the relevant risk domain owner or tier 1 risk owner, Enterprise Risk Management can activate automated notifications from Riskware to inform the relevant owner when a current rating for a tier 2 risk linked to their tier 1 risk has changed.

(26) Enterprise Risk Management will perform sample checking on a periodic basis to confirm that tier 2 risks have been assessed accurately and adequate rationale is documented in Riskware to support the rating.

Control Design and Operation – Minimum Requirements

(27) A control is defined as 'any action taken by management to manage risk and increase the likelihood that established objectives and goals will be achieved'. A control is not a meeting, a policy or a procedure. There may be certain requirements documented in a policy or a procedure which are a control.

(28) Controls should be designed and operated to:

a. Support compliance with obligations
b. Prevent causal factors so the risk does not materialise (preventive controls) or detect and minimise the consequences (detective controls) if a risk does materialise.

(29) Control descriptions within Riskware should include the following characteristics:

a. Who: Who operates the control
b. Why: What is the objective of the control
c. When: Frequency of the control
d. What: What is the control operator performing
e. How: How is the performance of the control evidenced.

(30) Detailed below is an example of a control description which includes the above characteristics:

a. On a monthly basis (when), the Financial Controller (who) reviews key balance reconciliations (what) to ensure that financial records are accurate and any reconciling items can be resolved in a timely and accurate manner (why). Evidence of reconciliation review is maintained within Workday (how).

(31) Controls can either be preventive or detective:

a. Preventive: A control occurring early in the process to prevent the risk from occurring. Preventive controls are

preferred to detective controls.

b. Detective: A control which exists to detect and notify when a risk has materialised and can mitigate damage once a risk has materialised.

(32) Controls can either be manual or automated:

a. Manual: Controls performed manually by individuals outside of any system
b. Automated: Controls performed automatically by systems / technology with limited human assistance. Automated controls are preferred to manual controls due to the lack of human interface and chance for errors.

(33) The benefits of identifying whether a control is either preventive or detective; and manual or automated; is that it allows a holistic view of the internal control environment and will guide the level of assurance that may be required over specific controls.

(34) Ownership of internal controls should sit at the senior manager level or above. A control owner is a person who is accountable for ensuring a control activity exists, is in place and is operating effectively. The control owner may not necessarily perform the control activity; however if not operating the control they are usually accountable for maintaining a level of oversight over its performance or effectiveness.

(35) Ownership of internal controls cannot be delegated to a third party and must be assigned to a single individual.

(36) Controls can be assessed as either effective or not effective defined as:

a. Effective: Control is designed and operating effectively to fully mitigate the risk and achieve the control objective. Control is performed in line with agreed frequency
b. Not Effective: Control is not designed and operating effectively to fully mitigate the risk and achieve the control objective and/or control is not performed in line with agreed frequency.

(37) Controls can also be ‘not rated’ within Riskware. This may be appropriate when a control has recently been operationalised but it’s effectiveness is not yet known.

(38) It is the responsibility of the control owner (or delegate) to assign a control effectiveness rating in Riskware. If there are circumstances which warrant the control to be reassessed this should occur as part of business as usual. These circumstances may include internal or external audit findings, regulatory findings, assurance results, complaints, incidents, losses etc.

(39) Risk Owners should review and approve controls that are linked to their risk(s) to ensure they are comfortable that the control is relevant in mitigating the risk.

(40) It is the responsibility of risk domain owners to ensure there are appropriate levels of assurance across risk domains they own utilising the assurance plan template provided by Enterprise Risk Management, which details:

a. Key controls to mitigate risks (replicated from Riskware)
b. Control owner (replicated from Riskware)
c. Assurance provider for each control and level of assurance being provided.

Treatment Plan – Minimum Requirements

(41) A treatment plan is defined as formal documentation detailing actions to be taken and responsibilities for implementing controls or processes to reduce the likelihood or impact of risks. Treatment plans may involve enhancements to existing controls which are assessed as ‘not effective’ or the design and implementation of new controls to further mitigate the risk.

(42) It is the responsibility of the treatment plan owner (or delegate) to design the treatment plan and document these in Riskware. The following fields in Riskware must be completed:

a. Description: Treatment plan descriptions should clearly outline the deliverable of the treatment plan and how this will mitigate the identified exposure
b. Responsible: Staff member who is responsible for completion of the treatment plan
c. Due Date: Date at which the treatment plan is expected to be completed
d. % Complete: Progress against treatment plan deliverables updated quarterly by the treatment plan owner (or delegate)
e. Target Risk Rating: The level of residual exposure once the treatment plan has been implemented.

(43) The treatment plan design should be approved by the relevant risk owner(s) to confirm they are comfortable that the treatment plan design mitigates the control gaps identified.

(44) A treatment plan is required in the following circumstances:

a. Tier 1 risks - treatment plans are required when the current level of control for a cause is below the target level of control for a cause
b. Tier 2 risks - treatment plans are required for controls assessed as ineffective.

(45) If a treatment plan is not required or cannot be implemented (i.e. no funding or resourcing), risk acceptance processes must be followed, and approval sought from the relevant source to accept the risk. These approval levels are:

a. Tier 1 risks – Approval is required from the relevant risk domain owner
b. Tier 2 risks – Approval is required from the relevant tier 1 risk owner and risk domain owner.

(46) Evidence of approval of risk acceptance will be provided via email and attached in Riskware by the Risk Owner (or delegate).

(47) Any amendments to due dates for a treatment plan are processed in Riskware by the treatment plan owner (or delegate) and following approval from the following sources:

a. For treatment plans mitigating low or medium rated risks (both tier 1 and tier 2), amendments to due dates must be approved by the risk owner
b. For treatment plans mitigating high rated risks (both tier 1 and tier 2), amendments to due dates must be approved by the risk owner and relevant tier 1 risk owner
c. For treatment plans mitigating critical rated risks (both tier 1 and tier 2), amendments to due dates must be approved by the risk owner, relevant tier 1 risk owner and relevant risk domain owner.

(48) Evidence of approval is provided via email and attached to the treatment plan in Riskware by the treatment plan owner (or delegate).

(49) At the request of the relevant risk owner, Enterprise Risk Management can activate automated notifications from Riskware to inform the risk owner (or other relevant personnel) when a treatment plan mitigating risks they own have become overdue or are complete.

(50) To ensure completed treatment plans have been implemented as designed, and mitigate the control gaps previously identified, the following verification will occur:

a. Treatment plans linked to low rated risks are verified by the treatment plan owner

b. Treatment plans linked to medium rated risks are verified by the relevant risk champion
c. Treatment plans linked to high or severe rated risks are verified by Enterprise Risk Management.

(51) Evidence confirming the treatment plan has been completed will be attached in Riskware by the treatment plan owner (or delegate), and evidence of the above verification will be attached in Riskware by the risk champion.

(52) Enterprise Risk Management will perform sample checking on a periodic basis to confirm that treatment plans linked to low and medium rated risks have been closed in line with the above requirements and mitigate the identified risk.

Reporting and Monitoring

(53) Enterprise Risk Management will report (via the Director Risk Report) to relevant governance committees on the following:

a. Any changes to the current risk ratings for risk domains or tier 1 risks
b. Any risk domains or tier 1 risks which are outside of appetite and the proposed treatment plans and timeframes to bring these within appetite
c. Number of due date extensions per risk domain, tier 1 risk and tier 2 risks, the average length of these extensions and the impact of extensions on enterprise risk exposure
d. Overdue Treatment Plans that are linked to risks rated medium or above.

Status and Details

Status	Current
Effective Date	22nd February 2024
Review Date	1st January 2029
Approval Authority	Vice-Chancellor's Executive
Approval Date	12th February 2024
Expiry Date	Not Applicable
Policy Owner	Fiona Notley Chief Operating Officer
Policy Author	Shah Abdul-Rahman Executive Director, Health, Safety and Risk
Enquiries Contact	Enterprise Risk Management

Glossary Terms and Definitions

"RMIT Group" - RMIT University and its controlled entities (RMIT Europe, RMIT Online, RMIT Vietnam, RMIT University Pathways)