Risk Management Policy

Section 1 - Purpose

(1) This Policy specifies the University's commitment, approach, and objectives relating to the understanding, identification, and management of risk. This Policy supports staff and affiliates to take informed risks without exposing the University, its assets, staff and affiliates, students, or other stakeholders to unnecessary harm.

Scope

(2) This Policy applies to persons involved in all operations of the University and its controlled entities (the University), including:

a. employees of the University;
b. individuals conducting research under the auspices of the University including but not limited to staff and affiliates, students, visiting academics, and conjoint appointees;
c. members of University governing bodies and committees;
d. emeritus, honorary, visiting, adjunct, conjoint, and clinical title holders; and
e. individuals otherwise engaged in the service of the University. This includes but is not limited to:
    i. consultants;
    ii. individual contractors working for the University;
    iii. employees of contractors providing services to the University; and
    iv. other people who perform public official functions as representatives of the University whose conduct and activities could be investigated by an investigating authority, including volunteers.

(3) All individuals listed in clause 2 are collectively referred to within this Policy and any accompanying documents as staff and affiliates.

Section 2 - Policy

Enterprise Risk Management Framework

(4) The University will adopt an Enterprise Risk Management framework (the Framework) across the University that is consistent with the International Standard on Risk Management (AS ISO 31000:2018) and is aligned with the eight (8) Principles of the Standard, which are that risk management:

a. is integrated into the University's processes;
b. is structured and comprehensive;
c. is customised to the University;
d. is inclusive and transparent;
e. is dynamic, fluid, and responsive to change;
f. considers the best available information;
g. considers human factors and the University culture; and

h. encourages and drives continual improvement.

(5) Identifying and managing risk is the responsibility of all staff and affiliates, who are expected to report any potential risks associated with their activities, and to actively identify, implement and maintain controls to prevent, detect or respond to risks within their area of responsibility.

(6) The University is committed to improving risk management by integrating better risk management practices into all key decision-making processes including strategic and business planning processes, key operational decisions, new activities, and within major projects.

(7) The University's risk management approach will:

a. ensure that significant risks are identified, understood and managed, providing stakeholders with confidence in decisions made and that the University is being effectively governed and managed;
b. reduce negative outcomes by minimising the consequences and/or likelihood of incidents that may result in injuries, financial or property loss, business interruption, audience loss, or damage to reputation;
c. develop a University-wide approach to managing risk, including consistent risk language, while creating an environment where all University staff and affiliates assume responsibility for managing risk; and
d. ensure that significant risks and their key mitigating actions are appropriately documented, monitored, reviewed, and communicated to all relevant staff and affiliates.

Risk appetite and tolerance

(8) The University's risk appetite indicates the types and amount of risk, on a broad level, that the University is willing to accept or retain in the pursuit of its objectives. The University's risk appetite is described in the Macquarie University Risk Appetite Statement.

(9) The University's risk tolerance criteria, indicates the types and levels of risk taking that are acceptable to achieve a specific objective or manage a category of risk, and are further defined in the risk tolerance criteria of the University Risk Assessment Matrix.

Responsibilities

(10) The following roles and responsibilities play a critical role in ensuring the ongoing success of the Framework.

(11) The University Council (Council) is responsible for overseeing risk management and risk assessment across the University in accordance with the Macquarie University Act 1989 and the Charter of Council.

(12) Council oversees risk management and risk assessment primarily through the Audit and Risk Committee. The Audit and Risk Committee reviews major risks to the University and its controlled entities and reports directly to Council (refer Audit and Risk Committee Terms of Reference).

(13) The Vice-Chancellor is responsible for leading and overseeing the implementation of the Framework.

(14) The Vice-President, Finance and Resources (Executive Sponsor) is responsible for:

a. supporting the Framework at the Executive Group;
b. reporting to the Executive Group on the ongoing success of the Framework and component capabilities; and
c. assessing and advising on the availability and budget for resources required for the ongoing management, review, and continuous improvement of the Framework.

(15) The Chief Risk Officer is responsible for:

a. developing, facilitating the implementation and continuous improvement of the Framework and having the role of Responsible Officer for this Policy; and
b. reporting to the Executive Group and the Audit and Risk Committee on the ongoing effectiveness of the Framework.

(16) The Executive Group is responsible for:

a. endorsing the Framework objectives and strategies;
b. agreeing to the roles and responsibilities for risk management activities as defined;
c. actively and visibly promoting and providing business support for risk management activities and initiatives throughout the University;
d. ensuring the implementation of the requirements of this Policy across their respective faculties, portfolios, and entities; and
e. facilitating the completion of the associated risk management activities as directed including ensuring that business risks are identified, managed, recorded, and communicated to the relevant faculty, portfolio, or entity Executive.

(17) Directors, managers, and staff are responsible for:

a. complying with this Policy and associated procedures, including following all reasonable and lawful directions; and
b. ensuring that the relevant faculty, portfolio, or entity risk profile covers all elements of the services and operations it provides.

Risk Assessment

(18) Risks and opportunities associated with University activities must be identified and effectively managed. This includes ensuring compliance with all relevant laws, and University policies, procedures and codes of conduct.

(19) Risk Assessment involve identification, analysis, evaluation and treatment of risks and opportunities that may impact on the objectives of an activity. Risk assessment must be undertaken by those responsible for the activity, in consultation with key stakeholders. Assessments must be regularly reviewed and updated whenever there are significant changes to the activity (proactive) or changes which require a response (reactive). The Risk Assessment process is described in Section 3 - Procedures.

(20) Risk Assessment templates are used to record and communicate risk information through the life of a project or activity or may be specialised for a particular activity and embedded within the process. Risk Assessment documentation should be maintained in an accessible location in the appropriate document storage system for the type of risk assessment conducted and updated as and when required.

Consultation, communication and escalation

(21) An important function of Risk Assessment is for communicating risk information through the life of a project or activity, communicating risk information and treatments to all those affected and sharing with other areas to build a common risk knowledge base.

(22) Shared risks are those extending beyond a single entity, which require shared oversight and management. Those responsible for the management of shared risks must include any risks that may involve third party providers or partners, or others within the sector, industry, or community, and implement arrangements for third parties or others to understand and contribute to the management of shared risks.

(23) Key risks, those that are rated ‘High’ or more, or those that may have a broad or significant adverse effect on the

University, should be upwardly referred at the time of the assessment for the development of appropriate treatment strategies at the appropriate level. Key risks and their ongoing management must be communicated in appropriate management reporting, such as to Council, controlled entity Boards, governance and management committees, or project steering committees.

Risk management capability

(24) The University must maintain an appropriate level of capability to implement the Risk Management Framework and manage its risks. The nature and scale of this capability will be considered in the context of the University's current resource and capability profile and be commensurate with the characteristics and complexity of its risk appetite and risk profile.

(25) Continuous improvement of risk management practices will include regular review of the University's risks, the Risk Management Framework, the application of risk management practices, and implementation of improvements arising out of such reviews.

Section 3 - Procedures

(26) Risk management involves:

a. defining the scope and context of the risk assessment;
b. identifying and describing the risk/s;
c. analysing risk/s against agreed risk tolerance criteria as indicated in the risk assessment matrix; and
d. evaluating whether a risk is adequately controlled and acceptable, or whether it may need additional controls to further manage the risk to a more appropriate level or escalating to a more senior position for a review, ownership, or a decision on its management.

(27) If a risk is assessed as being unacceptable because the residual risk (after taking into account existing control measures in place) is considered too high (also known as 'beyond tolerance level') then appropriate action(s) need to be identified and a plan developed. The plan should specify the action to be completed, the officer responsible (and or the action officer), and the timeframe for completion. The plan and information within it must be recorded and reported as appropriate.

(28) Communication, monitoring and reviewing the risk status must occur over an appropriate timeframe to ensure the risk is managed to a more acceptable level.

(29) The risk assessment process is explained in more detail on the Group Risk website.

Section 4 - Guidelines

(30) Nil.

Section 5 - Definitions

(31) The following definitions apply for the purposes of this Policy:

a. Enterprise Risk Management (ERM) means where risk management processes are integrated across the organisation, at all levels, particularly in all key decision-making areas.
b. Risk means the effect of uncertainty on objectives, causing a deviation from the expected, which may be

positive (opportunities) or negative (risks). Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances or knowledge) and the associated likelihood of occurrence.

c. Risk Appetite means the amount of risk the University is willing to accept or retain to achieve its objectives. It is a statement or series of statements that describes the organisation's attitude toward risk taking.
d. Risk Assessment means the process of risk identification, analysis and evaluation; and provides an understanding of risks, their causes, consequences, likelihood and controls. Risks can be assessed at a University, faculty, portfolio, entity, function, department, program, project, or activity level.
e. Risk Controls means any process, policy, device, practice or other actions within the University environment that modifies the likelihood or consequences of a risk.
f. Risk Management means coordinated activities to direct and control the University in regard to risk, including culture, structure, and processes that are directed towards ensuring that opportunities are maximised, and all potential losses minimised for all activities.
g. Risk Management Framework refers to the components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing, and continually improving risk management throughout the University.
h. Risk Management Plan refers to the plan within a Risk Management Framework, program, or project specifying the approach, management components, and resources to be applied to the management of risk.
i. Risk Profile means a set of risks related to the whole or part of the University (e.g. faculty, portfolio, entity, function) or as otherwise defined (e.g. project or event).
j. Risk Tolerance means the levels of risk taking that are acceptable to achieve a specific objective or manage a category of risk as described in the risk assessment matrix risk rating criteria.
k. Risk Tolerance Criteria means terms of reference against which the significance of a risk is evaluated, and is measured in terms of likelihood (or frequency or probability) and consequence (or impact).

Status and Details

Status	Current
Effective Date	14th May 2023
Review Date	15th May 2026
Approval Authority	Vice-President, Finance and Resources
Approval Date	15th May 2023
Expiry Date	Not Applicable
Responsible Executive	Robin Payne Vice-President, Finance and Resources
Responsible Officer	Kylie McKiernan Chief Risk Officer
Enquiries Contact	Kylie McKiernan Chief Risk Officer