Enterprise Risk Management Policy

Section 1 - Purpose

(1) The University has a statutory obligation to undertake risk management that is established under the University of Wollongong Act 1989 (the Act).

(2) The University of Wollongong (the University)recognises that managing risk is an essential part of everyone's role to support the achievement of strategic and operational objectives.

(3) Effective risk management enables the University to achieve its objectives more effectively and efficiently by managing uncertainty, leading to better informed decision making.

(4) Effective risk management enables:

a. an understanding of the range of social, political, cultural and environmental factors that may impact the University's objectives;
b. the identification, evaluation and management of threats and opportunities to ensure the University is conscious of the risks it faces;
c. the management of complex and shared risks, including identification of their causes, impacts/consequences, and controls;
d. improved quality of information for decision making;
e. improved University performance and resilience;
f. clear reporting and transparency of information; and
g. accountability, assurance and effective governance.

(5) The purpose of this Policy is to:

a. state the overall intentions and directions of the university in relation to risk management;
b. define responsibilities and structures to ensure risk management practices are integrated into all aspects of strategic and operational activities and that these practices undergo continuous improvement;
c. create a strong risk culture where all staff are encouraged to proactively manage and/or report risks in their day-to-day activities, and feel safe in doing so;
d. promote an environment where informed decisions to identify and manage the University's risks are made in an open and transparent manner and in accordance with the University's Risk Appetite Statement;
e. ensure all areas across the University apply a consistent approach to risk and opportunity management providing assurance on the effectiveness and reliability of controls and other activities designed to manage risk; and
f. ensure that risks and the University's risk appetite is understood and that this informs decision-making.

Section 2 - Application and Scope

(6) This Policy applies to all of UOW and all activities conducted by, or on behalf of the University, including:

a. work, health and safety activities;
b. commercial activities;
c. major projects, change initiatives, strategic and planning activities;
d. formal and informal research activities, with specific attention to international collaboration;
e. teaching activities;
f. critical and crisis management incidents;
g. third-party engagement and activities on behalf of the University;
h. any activity where there is potential for fraud, corruption, modern slavery, foreign interference, or risks to national security; and,
i. any other activity directed by legislation, regulation or informed by national policy.

(7) This Policy should be read in conjunction with the Enterprise Risk Management Procedures and Risk Appetite Statement.

(8) This Policy is supported by a range of documents that inform health, safety and risk management systems and practices across the University. These documents must be consistent with the broad direction of this Policy.

Section 3 - Principles

(9) The University acknowledges that risk management is:

a. integrated, with risk considered in all business activities and decision-making processes throughout the University;
b. dynamic, as risks can emerge, change or be closed as the University's internal and external environment changes. All risks, across all aspects of the University's operations, should be understood, considered, assessed, and documented;
c. inclusive, where communication and consultation with stakeholders at all levels of the university enables a diverse range of knowledge, views, and perceptions of risk, resulting in informed risk management;
d. based on the best available information at that point in time, and includes historical and current information as well as future expectations and forecasts; and,
e. continually improved through learning and experience, to support staff in recognising and understanding their risk management obligations through the provision of education, training, and information.

Section 4 - Enterprise Risk Management Framework

(10) The University has an Enterprise Risk Management Framework (ERMF) that supports informed decision-making in pursuit of achievement of objectives, which is proportionate to its strategy and operational model.

(11) The ERMF supports effective risk management by integrating it into activities and functions across the University.

(12) The ERMF is consistent with the International Standard - AS ISO 31000:2018, Risk Management – Principles and Guidelines.

(13) The ERMF consists of:

a. Risk Culture, which refers to the University's attitude to risk management and the expected behaviour for staff and leadership that influences the ability to effectively identify, understand, openly discuss, escalate and act on risks in a timely manner and is characterised by:
    i. an appropriate 'tone from the top' set, modelled and championed by the University Council and University Executive; Clearly defined roles and responsibilities, acknowledging that all staff are responsible for the management of risk within their areas of responsibility;
    ii. a safe 'speak-up' environment, where employees feel empowered to report concerns without fear of retaliation; Transparency and accountability, ensuring potential issues are addressed promptly, promoting a proactive approach to risk management;
    iii. a clearly articulated and well understood risk management framework and supporting procedures to allow for a structured and consistent approach to risk management at all levels across the University; and,
    iv. University staff who are set up for success and able to identify and are equipped to manage risks.
b. Risk Governance, which refers to the oversight and management of risk through:
    i. Council and its committee structure and appropriate Terms of Reference;
    ii. The Risk, Audit and Compliance Committee (RACC) of Council and its independence from management;
    iii. University Executive (UE) and its oversight of risks, ensuring risk-taking activities are aligned with the University's strategic objectives and ensuring risk management is resourced appropriately;
    iv. the Risk Advisory Group, and its advice on risk prioritisation to University Executive;
    v. approved Risk Appetite Statement and Enterprise Risk Management Policy in addition to a broader suite of policies and procedures, including the Delegations of Authority Policy; and,
    vi. the incorporation of risk management in internal policy development.
c. Systems and Procedures, which refer to the consistent and systematic identification and assessment of risk across the University to inform risk versus reward decision-making.
d. Continuous Review, improvement and training, which involves developing annual risk management plans, evaluating maturity, and the performance of the Risk Management Framework and Policy.
e. Communication, Consultation, and Escalation, involves detailed workshops, that are inclusive of all staff fostering a proactive and transparent approach to managing risks.

(14) Risks associated with the University's activities must be identified and assessed.

(15) All risks are to be assessed using the methodology as specified in the Risk Management Procedures and relevant guidelines.

(16) Specialised risk guidelines, e.g. for WHS or information security management, must be consistent with the broad directions of this policy and the risk management procedures as a minimum.

(17) Risk and Control Self-Assessments are required for all activities as outlined in the scope and application of this Policy.

(18) Control management and assurance activities will be conducted in accordance with any relevant regulatory requirements, standards or guidelines, and the University's Risk Management Procedures.

(19) An important component of Risk Management is:

a. consultation, ensuring stakeholders across all levels of the organisation are engaged in identifying and assessing risks and controls;
b. communication, ensuring relevant stakeholders and governance bodies are appraised of risk information throughout the life of a project or activity;

c. escalation, ensuring risks that are rated ‘High’, ‘Extreme’ or outside risk appetite are brought to the attention of the appropriate Senior Executive and Chief Risk and Assurance Officer (CRAO), and are reported to the appropriate governance body, such as RACC, Controlled Entity boards, or project steering groups.

(20) An annual risk management plan will be developed and implemented to systematically identify, assess and mitigate risks while improving the University’s overall risk management maturity.

(21) The maturity and performance of the risk management practices will be regularly evaluated through independent reviews and internal audits, ensuring the Risk Management Framework and Policy are fit for purpose.

(22) The University will foster a resilient and proactive approach to risk management by continuously enhancing and adapting practices based on audit findings and evolving risk landscapes.

Section 5 - Reporting and Response Requirements

(23) The University relies on timely analysis and reporting by stakeholders and other sources for the identification and management of risks and emerging threats.

(24) All staff must ensure risk and controls self-assessments are undertaken, and that corresponding mitigations are reviewed in accordance with the Enterprise Risk Management Procedures.

(25) Risks evaluated as requiring treatment must be mitigated, and the risk and mitigation plan escalated to the relevant Senior Executive.

(26) Where risks are outside of the University’s Risk Appetite, but no treatment is available or the costs outweigh the benefits, the acceptance of the risk can be approved by the Vice-Chancellor and President or Vice-President Operations. All approvals must be made in accordance with the authority set out in the Delegations of Authority Policy.

(27) Referral for the acceptance of risks outside of appetite where there is no treatment available or the costs outweigh the benefits must be made in writing via the Chief Risk and Assurance Officer, to the Vice-Chancellor and President or Vice-President Operations. All approvals must be made in accordance with the authority set out in the Delegations of Authority Policy.

(28) Where risks outside of appetite are approved to be ‘accepted’ they must be reviewed every 3 months to ensure that the conditions that existed that led to the exception are still valid, where the conditions have changed, treatment plans must be developed in accordance with the Enterprise Risk Management Procedures for treatment.

(29) Emerging threats will be incorporated into the University’s Enterprise Risk Management (ERM) System once the threat is measurable and becomes an assessable risk.

(30) Assurance mapping is used to identify and assess assurance activities across the University to ensure that risks are effectively managed, and controls are properly monitored.

(31) The Risk and Assurance Division (RAD) will provide a Risk Management Report to the Risk Advisory Group (RAG), University Executive (UE), Risk, Audit and Compliance Committee (RACC) and Council in accordance with the relevant Terms of Reference (TOR). These may include, but are not limited to:

a. regular reporting of top risks and emerging threats, and progress of mitigation plans;
b. any risk/s that are outside the University’s risk appetite, including risks that are ‘accepted’ as described in the Enterprise Risk Management Procedure;
c. any risk where implementation of the mitigation plan exceeds the agreed maximum timeframe as per the Enterprise Risk Management Procedure;

d. control management, to ensure key controls are working effectively and undergoing appropriate levels of testing;
e. root cause analysis, to understand trends and identify any systemic issues that need to be addressed; and
f. measurable outcomes that demonstrate the performance of the risk management framework and the maturity of the University's risk culture.

(32) Risk Owners will provide any detailed risk reports as requested by the Chief Risk and Assurance Officer (CRAO), Vice-Chancellor and President (VC) and/or the Chair of the Risk, Audit and Compliance Committee (RACC).

Section 6 - Policy Breaches

(33) Breaches of this Policy are considered a failure to comply with the University's Code of Conduct and will be managed in line with the Code.

Section 7 - Roles and Responsibilities

University Council

(34) The University Council is the governing authority for the University and, as such, has responsibility under the University of Wollongong Act 1989 for oversight of risk management and risk assessment activities across the institution.

Risk, Audit and Compliance Committee

(35) The Risk, Audit and Compliance Committee (RACC) assists Council in fulfilling its corporate governance and independent oversight responsibilities in relation to the University's management of risk, compliance with legislation and standards, management of internal controls, and, audit requirements in accordance with its Terms of Reference.

Vice-Chancellor and President

(36) The Vice-Chancellor and President is responsible for:

a. ensuring a risk management system is established, implemented and maintained in accordance with this policy in any designated functional area or activity;
b. ensuring systems are in place so that risk owners are held responsible for implementing, monitoring and reporting risks that are within their area of responsibility;
c. fostering a positive risk culture where risk management practice is integrated and its value is recognised;
d. providing leadership relating to the University's risk appetite and acceptable risk exposure; and
e. the assignment of responsibilities in relation to risk management.

Senior Executives and Executive Deans

(37) Senior Executives and Executive Deans are responsible for:

a. implementation of this policy;
b. championing a risk management culture and supporting the enhancement of risk management practices across the University;
c. the formal identification of risks that may impact upon achievement of the University's objectives;
d. prioritisation and allocation of resources to mitigate unacceptable risks;

e. the provisions of risk management guidance to their stakeholders;
f. oversight of University, portfolio, faculty and divisional risk and control assessments, and/or activity registers;
g. monitoring the adequacy of controls and mitigation plans; and
h. overseeing the management of risks that have been escalated from within their respective areas of responsibility, including any controls to mitigate adverse impacts or maximise opportunities as described in the University's risk appetite statement.

Directors, Faculty Executive Managers, Directors of Research Institutes and Project Managers

(38) Directors, Faculty Executive Managers, Directors of Research Institutes and Project Managers are, within their respective areas of responsibility, responsible for:

a. implementation of this Policy;
b. championing a risk management culture and supporting the enhancement of risk management practices across the University;
c. managing risks, which includes identifying, assessing, monitoring, reviewing, communicating and reporting any risks that may impact on achievement of objectives;
d. ensuring a local risk register for their area of responsibility is developed and regularly reviewed and maintained;
e. maintaining effective internal controls;
f. the development and implementation of appropriate and effective mitigation plans;
g. regular reporting of risks and progress of mitigation plans;
h. reporting to their Senior Executive or Executive Dean any new high-risk issues as soon as practicable after the risk has been identified;
i. reporting any new and emerging threats - in their area or in other areas of the institution - through the Risk and Assurance Group; and
j. ensuring medium and high residual risks for commercial activities, major projects, third parties and any other major initiatives and activities are registered, managed and used to inform their local risk register.

Chief Risk and Assurance Officer (CRAO)and Risk and Assurance Division

(39) The Risk Management function is responsible for:

a. facilitating development and implementation of the University's risk management approach and associated policies, framework, systems and guidelines;
b. ensuring the review and continuous improvement of the University's risk management framework;
c. maintaining the University Enterprise Risk Management (ERM) System;
d. training of University staff in relation to risk management practice; and
e. reporting on the University's risk environment and position to the relevant Group or Committee.

(40) The internal audit function is responsible for:

a. testing and validating the effectiveness of the risk management framework; and
b. providing assurance over the control environment, evaluating, the design adequacy and operating effectiveness of controls in place to mitigate the risks associated with key University activities.

(41) The Chief Risk and Assurance Officer will have direct and independent access to the Risk, Audit and Compliance Committee (RACC) Chair and members as needed to escalate concerns related to the operations and efficacy of this Policy.

Controlled Entities

(42) In accordance with the Controlled Entity Policy, the controlled entity and its subsidiaries must:

a. ensure the effective management of risk and safety, including development in consultation with the University's Chief Risk and Assurance Officer and Risk, Audit and Compliance Committee (RAAC), as appropriate, a risk management plan which is appropriate for the controlled entity and congruent with the University's risk management framework; and
b. establish systems of governance, internal controls, and risk management which are appropriate for its business, align with the strategic, operational and risk management plans of the University.

All Staff

(43) Every staff member of the University is responsible for the effective identification and management of risks including the identification and reporting of new and emerging threats.

(44) Every staff member is responsible for participating, as required, in training, workshops and information sessions in relation to risk management practice provided by the University to ensure they:

a. understand the value and importance of risk management;
b. promote a positive risk culture and understand the methodology and approach to identifying, assessing, and managing risks in day-to-day operations, decision making and business planning; and
c. understand and adhere to the reporting processes within the University's governance framework in relation to risk management.

Section 8 - Definitions

Word/Term	Definition
Assurance Map	Process that identifies, assesses, and aligns assurance activities across an organisation to ensure that risks are effectively managed, and controls are properly monitored.
Commercial Activity	As defined in the Commercial Activities Guidelines.
Consequence	Outcome of an event affecting objectives. Noting an event can lead to a range of consequences, consequences can be certain or uncertain, positive, or negative, qualitative, or quantitative and can be risks unto themselves, also known as knock-on effects.
Control	Any measure, action, or mechanism that is put in place to prevent or detect, the impact or likelihood of the identified risk.
Emerging Threat	An emerging threat refers to a new or evolving risk, danger, or challenge that is in the process of developing or gaining prominence.
Enterprise Actions Register	The central repository to record and monitor agreed management actions and remediations of risk, controls, internal audit, and reviews across the university.
Enterprise Risk Management	The integration of risk management processes across the university at all levels and in key decision-making areas.
Inherent Risk	The worst-case scenario of a risk without consideration of controls.
Internal Audit	Independent, objective assurance activity designed to add value and improve the university's operations by identifying risks and control operating effectiveness.
Level of Risk	The magnitude of a risk expressed as a combination of consequence and likelihood. Also known as the risk rating, which could be inherent or residual.
Likelihood	Chance of something happening

Word/Term	Definition
Risk, Audit and Compliance Committee (RACC)	In accordance with Section 16 of the University of Wollongong Act 1989, the Council is charged with overseeing risk management and risk assessment across the University. The Council Risk, Audit and Compliance Committee assists the Council in fulfilling its corporate governance and independent oversight responsibilities in relation to the University's management of risk, compliance with legislation and standards, its internal control structure and audit requirements, and its external reporting responsibilities.
Residual Risk	The current or typical risk based on control environment.
Risk	The effect of uncertainty on objectives, causing a deviation from the expected outcome, which may be positive (opportunities) or negative (risks). Risk is measurable by the combination of the consequences and the associated likelihood of the risk occurring.
Risk Acceptance	The informed decision to take a particular risk, this can occur without risk treatment or during the process of treatment. Accepted risks are subject to monitoring and review.
Risk Advisory Group (RAG)	The Management body responsible for providing advise to UE on the prioritisation of top risks and emerging threats to the university.
Risk Analysis	Process to comprehend the nature of risk and determine the level (size) of risk. Risk Analysis provides the basis for risk evaluation and treatment.
Risk Assessment	Is the overall process for risk identification, risk analysis and risk evaluation.
Risk Appetite	Risk appetite is the total, amount, and a type, of risk that the university is willing to accept in pursuit of its objectives
Risk and Control Self-Assessment (RCSA)	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, business unit, entity, function, program, project, or activity level.
Risk Evaluation	Process of comparing the results of risk analysis and risk appetite to determine whether the risk is acceptable or requires treatment.
Risk Management Framework	The components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing, and continually improving risk management throughout the University.
Risk Management	Coordinated activities to direct and control the University regarding risk.
Risk Matrix	A tool used for ranking (by risk level) and displaying risks by defining ranges for consequence and likelihood
Risk Owner	The person who is accountable for the management of the risk as it relates to their objective.
Risk Register	The central register of the University's risks that may be filtered to view risk at a local level.
Risk Sponsor	The executive or entity with the accountability and authority to manage a category of risk
Risk Treatment	The process to modify risks that is deemed 'unacceptable or outside of appetite', also referred to as risk mitigation, risk elimination, risk prevention or risk reduction. Its important to note that risk treatment can creates new risks or modify existing risks.
Target Risk	Desired level of risk after risk treatment
University Executive Committee	The University Executive Committee makes recommendations to the Vice-Chancellor and President in the exercise of their delegated authority for university-wide planning, decision-making and oversight. It reports to Council on the prosecution and management of initiatives under the University's strategic plan, and on the academic and financial health of the University.

Status and Details

Status	Current
Effective Date	12th December 2024
Review Date	12th December 2027
Approval Authority	University Council
Approval Date	6th December 2024
Expiry Date	Not Applicable
Responsible Executive	Stephen Phillips Vice-President Operations
Responsible Officer	Robert Oldfield Chief Risk and Assurance Officer
Enquiries Contact	Risk and Assurance Division