Risk Management Framework

Section 1 - Introduction

(1) This Framework has been developed to support the Risk Management Policy. It outlines how risk management is embedded into day-to-day activities, providing tools and guidance for stakeholders to manage risk in a manner that is:

a. Consistent – applying the Council's risk appetite uniformly across diverse University activities.
b. Proportionate – focusing on risks that are material to achieving strategic objectives.
c. Prioritised – enabling clear identification and prioritisation of activities that significantly impact the University of Newcastle (the University) objectives.

Section 2 - Scope

(2) The Framework applies to all staff of the University and its controlled entities.

(3) Controlled entities are expected to align their risk management practices with the University's Risk Management Policy and Framework, ensuring a consistent approach to identifying, assessing, managing, and reporting risk across the University group. Controlled entities may tailor their risk management arrangements to reflect their operating environment and specific compliance obligations, provided they remain consistent with the intent and core requirements of the University's Risk Management Policy and Framework.

Section 3 - Background

(4) The University's Risk Management Policy and Framework is aligned with the international standard for risk management – 'ISO 31000:2018 Risk Management – Guidelines'. The Framework outlines how those principles of effective risk management are applied at the University.

Section 4 - Risk Management at The University of Newcastle

Risk Assessment and Management Process

(5) The risk management process should form part of decision-making across the University and be integrated into structures and processes (See Risk Management Process - Visual). This means adopting a process that incorporates the following attributes:

a. establishing the risk context by defining the environment in which the risks will be managed;
b. assessing and analysing risks based on their consequence and likelihood to determine the risk rating and risk level (risk analysis);
c. evaluating the risks in comparison with the risk appetite, risk threshold and risk tolerance;
d. determining and implementing appropriate treatment of risks (risk treatment);

e. monitoring and review to respond to indicators including changes in controls or emerging risks; and
f. continuously being informed by appropriate consultation, communication, and reporting throughout the process.

Risk Identification

(6) This is the process of capturing risks that may help (opportunity) or prevent (threaten) the achievement of the University's objectives or the objectives of a particular project, research activity or event. The identified risks and opportunities should be documented in risk profiles or in detailed risk assessments.

(7) The source of risk, the event that could trigger the risk (cause) and the impact on the University's objectives (effect) must be considered.

(8) Common risk identification techniques include workshops, process reviews, incident analysis, scenario planning, SWOT analysis, and consultation with subject matter experts.

Risk Analysis

(9) The risk analysis process informs whether risks need to be treated (managed) and if so, how. It supports the prioritisation of risks which may have the most significant impact on achieving objectives.

(10) Risks should be measured by considering the likelihood (frequency or probability of occurrence) and the consequence (impact or magnitude of effect) if the risk occurs.

(11) The assessment of each risk is determined at both the inherent risk (i.e. if there were no controls in place to reduce the risk) and residual risk (the remaining risk with effective controls in place). Understanding the inherent position helps to determine the importance and prioritisation of controls.

(12) Internal controls which are in place to prevent the risk will affect the likelihood of occurrence (preventative controls). Detective internal controls support early identification of issues. Internal controls which support the rectification or lower the impact will affect the consequence (corrective controls). In considering the adequacy of internal controls, effectiveness needs to be considered.

Table 1 - Control effectiveness criteria

Control Effectiveness		
Effective	**Partially Effective**	**Not Effective**
Controls are designed correctly, are in place and are effective. Controls are operating 90-99% of the time. Controls are subject to regular monitoring and review. The existing controls are well designed and addresses the risk. Controls are effective and reliable at all times.	The existing controls have some impact on mitigating the risk. Controls are inconsistent in their application, monitoring and effectiveness. Controls are operating 50-89% of the time. Scope for improved effectiveness. Some additional work is required to ensure operational effectiveness and reliability.	The existing controls are missing or ineffective and do not support the risk mitigation. Controls are poorly communicated and are not subject to monitoring. Controls are operating at <50% of the time. Enhancement required.

Risk Evaluation

(13) Risk evaluation determines whether a risk is acceptable within the University's Risk Appetite Statement or whether further treatment or escalation is required. Evaluation considers the residual risk rating, the effectiveness of existing controls, and the University's risk appetite, tolerance, and thresholds.

(14) Risks outside the approved appetite must be escalated in accordance with the Risk Management Policy.

Risk Treatment

(15) Residual risk ratings guide appropriate prioritisation and allocation of resources for the management of identified risks.

(16) Subject to the University risk appetite, risks may be accepted or treated to reduce likelihood or impact.

Risk Acceptance

(17) The University acknowledges that accepting some level of risk is necessary to enable innovation and pursue opportunities aligned to the University's strategy. However, risk acceptance must always be based on a clear understanding of potential benefits and consequences, supported by proportionate mitigation measures.

Risk Monitoring and Review

(18) Risks do not remain static, and risk monitoring should be ongoing as well as event driven. This ensures risk information and assumptions remain relevant; controls remain effective, and that changing environmental conditions are considered in risk assessments.

Section 5 - Assessing risk via the Risk Matrix

(19) The risk matrix (See: Risk Matrix) provides a consistent way for staff to assess and rate risks in their day-to-day work. It should be applied to strategic, operational, and project risks. It translates the Council approved risk appetite into defined, quantifiable, and measurable risk thresholds. These thresholds are embedded within consequence definitions, likelihood assessments, risk ratings, and escalation requirements. Residual risk ratings guide appropriate prioritisation and allocation of resources for the management of identified risks.

(20) During the risk analysis process, the likelihood table within the risk matrix must be used to assess the probability of occurrence. The consequence table must be used to assess all potential impacts to the University, with the highest impact rating applied to determine the risk rating.

(21) Risks should be assessed based on the greatest consequence to the University rather than the impact on an individual business unit or project. For example, a serious matter of integrity may cause limited operational disruption, but the reputational impact can be major, leading to erosion of public trust.

(22) Once the likelihood and consequence have been assessed, use the risk map (within the Risk Matrix) to determine the risk rating (for example, likelihood of ‘Possible’ and consequence of ‘Major’, provides a risk rating of ‘Medium’).

(23) Table 2 details the protocols for escalating risks, findings, and issues, along with timeframes for addressing these matters based on their residual risk rating.

Table 2 - Residual Risk Rating and Management Requirements:

(24) Where a risk is rated as outside the Council's risk appetite, Council consideration is required.

Residual Risk Rating	Management Requirements
Extreme	- Council oversight, escalation and consideration is required. - Active risk treatment required with immediate action; cease, redesign, or significantly mitigate activity. – A detailed treatment plan should be developed. - Continuous monitoring of the risk, controls and treatment strategies is required. - Reporting to the Risk Committee is required. - Target remediation should be within 6 months.
High	- Council / Vice-Chancellor oversight, escalation and consideration is required. - Active risk treatment required to reduce risk. A detailed treatment plan should be developed. - Ongoing monitoring of the risk, controls and treatment strategies is required. - Reporting to relevant management and Risk Committee is required. - Target remediation should be within 6 to 12 months.
Medium	- Executive Leader oversight, escalation, and consideration required. - Strengthen controls or reduce exposure and implement targeted treatment plan where feasible based on cost/benefit. - Regular monitoring is required of changes to the nature of risks, controls and treatments. - Target remediation should be within 12 to 18 months.
Low	- Head of Unit or School oversight, escalation, and consideration is required. - Monitor and improve controls where feasible based on cost / benefit. - Managed by established, routine processes / procedures. There is a need to be mindful of changes to nature of risks and controls.
Very Low	- Department Leader oversight, escalation, and consideration is required. - Accept or manage through BAU controls, routine processes / procedures and be mindful of change to nature of risks.

Section 6 - Material Risk Categories

(25) Risk management covers all types of risks across the University's activities, including risks relating to core teaching, learning and research functions, and material strategic and operational risks which impact everyone such as people and capability, health and safety, and information, technology and cyber.

(26) The University's Enterprise Risk Profile identifies the most material risks facing the University that could affect strategic, operational, and financial outcomes. These risks fall into three main categories:

a. Strategic risks – Risks that could affect the University's long-term direction, priorities, or goals. This includes risks from poor decisions, weak implementation, or external changes that impact the strategy.
b. Operational risks – Risks arising from failures in processes, systems, people, or external events that disrupt operations. These risks often have direct financial impacts.
c. Financial risks – Risks related to the University's financial position, including its ability to meet short- and long-term financial and capital objectives.

(27) Each of these categories includes more detailed risk areas under the full risk taxonomy. Categories are not fixed and will change over time as new risks emerge, and circumstances evolve.

(28) Risk management should occur at all levels of the University as part of normal planning and operations (see Section 7). Strategic planning, business planning, and risk management operate as a continuous cycle:

a. Strategy sets the direction.
b. Business plans put it into action.
c. Risk assessments test whether plans are achievable within the University's risk appetite.
d. Risk insights are then used to refine and improve both strategy and planning.

Section 7 - Risk Governance

(29) The University's risk governance structure is a multi-faceted, depicted by the 'Enterprise Risk Management Ecosystem' which includes the Policy and this Framework, the Risk Matrix, and the Risk Appetite Statement and strategy detailed above. Additionally, the University's approach to risk governance includes the following risk profiles:

a. Enterprise Risk Profile – identifies and reports major strategic and operational risks. These are reviewed by the Executive and approved by the Risk Committee and Council.
b. Operational Risk Profiles – used by Colleges, Schools, Divisions, and Units to identify and manage their risks, with support from Risk Services.
c. Specialised Risk Profiles – relate to specific projects or technical areas (e.g. health and safety, construction, regulatory change). These are managed by the relevant business area and aligned to the overall Risk Framework.
d. Controlled Entity Risk Profiles – maintained by controlled entities and approved by their Boards. These are considered as part of the University's overall risk exposure.

(30) Managing risk is a shared responsibility. All staff are responsible for identifying and managing risks, with specific roles outlined in the Risk Management Policy.

Section 8 - Review

(31) This Framework will be reviewed every three years.

Section 9 - Appendices

(32) Enterprise Risk Management Ecosystem - Depiction.

(33) Risk Management Process - Visual

(34) Risk Matrix (Consequence & Likelihood Tables)

Status and Details

Status	Current
Effective Date	11th November 2026
Review Date	11th November 2029
Approval Authority	Risk Committee
Approval Date	16th October 2026
Expiry Date	Not Applicable
Responsible Executive	Morven Cameron Chief Operating Officer
Enquiries Contact	Virginia McKay Director, Risk Services Legal and Governance Services

Glossary Terms and Definitions

"Council" - The governing authority of the University established under section 8A of the University of Newcastle Act 1989.

"University" - The University of Newcastle, a body corporate established under sections 4 and 5 of the University of Newcastle Act 1989.

"Risk" - Effect of uncertainty on objectives. Note: An effect is a deviation from the expected, whether it is positive and/or negative.

"Risk management" - The co-ordinated activities of assessing, controlling, monitoring, and reviewing risk in the pursuit of the University's objectives.

"Risk appetite" - Risk appetite is the amount and type of risk that an organisation (or individual) is willing to accept or pursue in order to achieve its objectives.

"Risk assessment" - The overall process of risk identification, risk analysis, and risk evaluation.

"Risk profile" - A comprehensive and structured assessment that outlines the types, sources, likelihood, and potential impact of risk. It provides a snapshot of the current exposure to risks and highlights areas of vulnerability, control effectiveness, and risk mitigation priorities. A Risk Profile is used to inform decision-making, allocate resources, and ensure alignment with the organisation's risk appetite.

"Level of risk" - Magnitude of a risk or combination of risks, expressed in terms of the combination of their impact and likelihood.

"Controlled entity" - Has the same meaning as in section 16A of the University of Newcastle Act 1989.

"Research" - As defined in the Australian Code for the Responsible Conduct of Research, or any replacing Code or document.

"School" - An organisational unit forming part of a College or Division, responsible for offering a particular course.

"Staff" - Means a person who was at the relevant time employed by the University and includes professional and academic staff of the University, by contract or ongoing, as well as conjoint staff but does not include visitors to the

University.

"College" - An organisational unit established within the University by the Council.

"Risk matrix" - Quantitative statements or risk thresholds that express the risk appetite in measurable terms that can be consistently interpreted and applied by stakeholders. These are displayed in the Impact and Likelihood Tables.

"Risk identification" - Process of finding, recognising and describing risks.

"Inherent risk" - Inherent risk is the amount of risk that an activity would pose if no controls or other risk mitigations were in place.

"Residual risk" - The level of risk that remains after implementation of risk mitigation measures and controls.

"Risk analysis" - Means the process to comprehend the nature, likelihood and consequences of risk to determine its level.

"Risk evaluation" - Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

"Risk treatment" - Risk treatment is a risk modification process. It involves selecting and implementing one or more treatment options. The risk treatment options are accept, or treat the risk. Formally accepting the risk should occur when residual risk is outside appetite and is accepted by a committee/role with appropriate delegated authority.

"Risk tolerance" - Refers to how much risk fluctuation or exposure is acceptable in practice, before management action is required.

"Risk threshold" - The specific, measurable limit beyond which a level of risk becomes unacceptable and requires action or escalation.

"Preventative control" - An action designed to stop something from happening and reduces the likelihood of occurrence.

"Corrective control" - An action designed to fix something that has happened and reduces the impact of a risk.

"Risk rating" - The assessed level of a risk, determined by evaluating its likelihood and consequences against approved risk criteria.