Enterprise Risk Management Framework Policy

Section 1 - Purpose and Scope

Context

(1) Risk is the 'effect of uncertainty on objectives'[1] where effect is a deviation from the expected outcome. Risk may be caused by a single event or a set of circumstances that affect, adversely (threats) or beneficially (opportunities), the achievement of objectives.

(2) In the context of Risk Management, uncertainty exists when there is an inadequate or incomplete knowledge or understanding of an event, its likelihood and/or its consequence.

(3) Risk Management refers to the set of principles, framework, culture, processes and coordinated activities to direct and control an organisation with regard to the many risks that can affect its ability to achieve its objectives. Effective risk management increases the likelihood of achieving objectives, identifying and pursuing opportunities and avoiding or minimising unexpected harms.

Risk Management Obligations

(4) Risk Management at the University of Queensland (UQ or the University) is guided by the International Standard ISO31000:2018 – 'Risk Management Guidelines' and seeks to comply with the following state and federal legislation relating to risk management:

a. Financial Accountability Act 2009 – requires the establishment and maintenance of an appropriate system of risk management.
b. Financial and Performance Management Standard 2019 (Qld) – prescribes that UQ's risk management system must provide for mitigating the risk to the University and the State from unacceptable costs or losses associated with the operations of the University, and managing the risks that may affect the ability of the University to continue to provide services.
c. Higher Education Standards Framework (Threshold Standards) 2021 – requires that risks to higher education operations are identified and material risks managed and mitigated effectively.
d. Crime and Corruption Act 2001 – refers to corruption risks and development of prevention strategies.
e. Work Health and Safety Act 2011 (Qld) – requires that risks are eliminated, and if not reasonably practicable to be eliminated, then minimised as far as reasonably practicable.

Risk Management Objectives

(5) Risk Management at UQ is:

a. an enabling management function overseen by the Senate and undertaken by Managers and staff at all levels of the University and in all aspects of its operations; and
b. contextual (i.e. risks are assessed against specific objectives) and recognises that uncertainty could affect objectives adversely and/or beneficially.

(6) UQ's risk management objectives are to facilitate the achievement of its strategic and operational objectives

including:

a. value creation and protection;
b. effective and efficient performance and compliance; and
c. the development, enhancement and protection of its strategic and operational capabilities.

Enterprise Risk Management Framework

(7) UQ's Enterprise Risk Management Framework (ERMF) provides the overall framework, direction and oversight for the systematic, disciplined and consistent identification and assessment of risks (including opportunities) and for their effective and efficient management.

(8) The ERMF comprises this Policy, Senate and management commitment to effective risk management, people and relationships that enable a risk-aware culture and the objectives and strategies that provide the context for risk assessment and management.

(9) The linked diagram highlights the core elements of UQ's Enterprise Risk Management Framework and helps demonstrate that risk management at UQ is:

a. an enabling management function, supported by input from staff at all levels, dedicated to the achievement of UQ's strategic and operational objectives and priorities while operating within the Senate-approved risk appetite and tolerance levels;
b. contextual (i.e. risks are assessed against specific objectives) and recognises that uncertainty could affect objectives adversely and/or beneficially; and
c. built on and supported by the following five 'pillars':
    i. Senate's expectations and risk appetite.
    ii. Management/ leadership commitment and support for risk management function, organisational culture and relationships.
    iii. External compliance obligations relating to risk management.
    iv. Risk management objectives, strategies, mandate and accountabilities.
    v. Risk management resources, plans, processes and activities.

Scope and Application

(10) The ERMF applies to all categories of risk across the whole of UQ, including risks associated with controlled entities, and their operations. It demonstrates the Senate and the Vice-Chancellor and President's commitment to and support for effective and efficient risk management.

(11) In addition to the ERMF, more detailed risk management governance documents with additional requirements exist, addressing specific risk domains, e.g. Health, Safety and Wellness Division and Information Technology Services. These more detailed risk governance documents are consistent with and give further effect to the ERMF.

Section 2 - Key Requirements

(12) To demonstrate effective and efficient risk management, UQ will:

Risk Appetite

(13) Manage its risks in alignment with the Risk Appetite Statement (RAS) approved by the Senate and towards the achievement of its strategic and operational objectives. Appendix A contains a link to UQ's RAS. It is important to note

that:

a. the RAS provides direction to management to guide their decision making. Management and staff are expected to be prudent and apply good judgement in interpreting the RAS to make sensible, risk-based decisions in the best interest of the University and its stakeholders;
b. it is acknowledged that in some circumstances the risk appetite statements may result in conflicting risk management objectives. Where this is the case, a trade-off in risk will be required in order to achieve the most beneficial outcome for UQ and Enterprise Risk Services (ER) should be advised;
c. external obligations, budget constraints and the impact of external influences must be considered to determine the optimal treatment plan to manage particular risks; and
d. the RAS is operationalised via the Risk Matrix including the Risk Tolerance and Action Table (Appendix C).

Risk Management Culture

(14) Create and continually enhance a constructive risk management culture in which staff and Managers at all levels are encouraged and supported to raise and respectfully discuss risks, issues and opportunities towards beneficial outcomes.

Enterprise-wide Approach

(15) Adopt an enterprise approach to risk management and ensure its risk management framework, processes and practices:

a. explicitly address “uncertainty” in relation to the achievement of objectives and priorities with a view to reducing the variability of outcomes;
b. are context-driven (i.e. based on specific objectives);
c. recognise the impact of human, cultural and environmental factors on University objectives;
d. are systematic, structured, timely and consistent with UQ’s Governance & Management Framework;
e. are transparent and inclusive i.e. risk assessment and management activities and decisions include perspectives of all stakeholders, not just management’s;
f. enable risk management to be an integral part of management thinking, discussions and decision making and help management find the right balance amongst risk, cost and value;
g. are integrated into all organisational processes, activities and practices including strategic and operational planning, project management and day-to-day operations and that risks are sufficiently documented in relevant plans and reports;
h. help safeguard assets both tangible and intangible (e.g. IP);
i. protect the integrity of financial accounting and reporting;
j. are based on the best available information and recognise any limitations with the underlying data;
k. are dynamic, iterative, responsive to change and continually improving;
l. are efficient and where feasible, harness technology to support risk management; and
m. facilitate the continual improvement and enhancement of the University.

Roles and Responsibilities

(16) Ensure clarity of roles, responsibilities and accountabilities for effective risk management including monitoring, reviews and provision of assurance on risks and controls.

Safety

(17) Build a zero-harm safety culture and implement a risk-based safety management system. Refer to the Health,

Safety and Wellness Policy and suite of supporting procedures for further guidance.

Compliance

(18) Adopt a risk-based approach to demonstrating compliance including coordination of regulatory and compliance matters across the University.

Investments

(19) Embed risk management in its investment processes and decisions to help identify, prioritise, assess and pursue viable opportunities in a systematic and disciplined manner.

Risk Matrix

(20) Assess its risks using the Risk Matrix (Appendix C) and record the risks and controls in the relevant risk register template provided on the ER website.

Risk Mitigation

(21) Select, design, implement, communicate and document risk mitigation strategies to reduce the likelihood of the risk eventuating and/or to reduce the impact on UQ, should the risk eventuate.

(22) Select only those risk mitigations for which the benefit will be greater than the cost of mitigating the risk.

(23) Monitor risk mitigation strategies to ensure continued relevance, appropriate application, effectiveness and efficiency.

General Management Controls

(24) Manage its risks through the design, development and implementation of effective and efficient controls, including General Management Controls (GMCs) as defined in Appendix B. All risks will be managed at a level as low as reasonably practicable and on a legally justifiable and cost/benefit basis with a financial and business outcome focus.

(25) Risk management options include (but are not limited to): risk elimination, risk avoidance, risk transfer (through insurance or contracts) and risk retention or acceptance with proper management.

Risk Events, Incidents, Resilience and Capability

(26) Build resilience and requisite capabilities to anticipate, prepare, respond, rapidly recover and minimise adverse impacts from critical incidents, including possible but hard to predict risks. Refer to the Incident Management Procedure for detailed incident management processes and protocols, including escalation requirements.

(27) Escalate risk events and incidents via business as usual organisational hierarchy and functional (i.e. central divisions and functions) communication processes, and promptly inform Enterprise Risk Services (ER) to be informed when the impact on UQ is rated as ‘Major’ or ‘Extreme’ as per the Risk Consequence Rating Table (Appendix C).

(28) Actively monitor and follow up negatively trending or adverse movements in key risk indicators and take appropriate steps to remedy unfavourable variances and trends including any systemic issues. Such monitoring follow-up and remediation will be undertaken by central functions and central divisions. Enterprise Risk Services (ER) will be promptly informed of unfavourable variances, trends, and systemic issues when the actual or probable impact on UQ is rated as ‘Major’ or ‘Critical’ as per the Risk Matrix Consequence Rating Table (Appendix C).

Reporting

(29) Ensure provision of meaningful and useful reports and assurance to senior management and the Senate on risks and controls. Such reports will include potential systemic, UQ-wide risk exposures and/or risk trends across the enterprise and any material changes to risk profiles and controls over time.

Internal Audit

(30) To the extent feasible, integrate risk management and Internal Audit activities by ensuring that Internal Audit's annual plans and programs of work appropriately consider the primary risks and controls of the University and provide assurance on their effectiveness.

Ongoing Review

(31) Continually review and optimise its risk management function, framework, processes and practices.

Section 3 - Roles, Responsibilities and Accountabilities

Senate

(32) The Senate is the University's governing body and accountable for the effective and efficient governance of the University. The Senate approves this framework including the University's risk appetite.

Senate Risk and Audit Committee

(33) The role of the Senate Risk and Audit Committee (SRAC) is to oversee the assessment and management of risks. The Committee’s responsibilities in relation to enterprise risk include:

a. review the tone and risk culture of UQ, and promote robust discussion around risk appetite and tolerance for risks;
b. receive reports from the Vice-Chancellor's Risk and Compliance Committee (VCRCC) on management’s identification and assessment of risks to UQ’s strategic and operational objectives and the effectiveness of processes to appropriately manage these risks;
c. advise Senate on significant issues and changes to the University’s risk profile; and
d. receive annual advice upon the effectiveness of the ERMF, including annual advice whether risks are being managed in accordance with RAS.

Vice-Chancellor's Risk and Compliance Committee (VCRCC)

(34) The VCRCC provides assurance to the Vice-Chancellor and President and USET on the effectiveness of UQ’s risk management and compliance frameworks and practices and on significant risk or compliance issues. In addition to risk and compliance, the VCRCC also provides oversight of assurance, investigations, research integrity and work health and safety functions.

Vice-Chancellor and President and USET

(35) The Vice-Chancellor and President, with support from USET, is responsible for:

a. creating and maintaining a risk-aware culture, including reinforcing commitment to and role modelling risk-informed decision making; and

b. exercising management oversight responsibility, ensuring effective risk management practices as per this ERMF, and transparent risk reporting to Senate.

University Senior Leadership Group (USLG)

(36) Under the ERMF, members of the USLG are responsible for:

a. assessing and managing the risks to their portfolio's objectives and strategies;
b. maintaining risk registers in the approved format and ensuring the accuracy and currency of their risk registers;
c. monitoring and reviewing their risks and controls with sufficient frequency to ensure the currency of their risk profile and ongoing effectiveness of controls;
d. providing timely and positive assurance on the management of their risks and on the effectiveness of the General Management Controls within their portfolios;
e. facilitating annual reviews of their material risks and controls by ER and any other ad hoc reviews of risks and controls that the ER may undertake to meet SRAC and/or VCRCC needs, and ensuring that any deficiencies identified through the review and assurance processes are promptly rectified; and
f. ensuring their direct reports undertake steps 1 to 5 above for their respective areas of responsibility.

Enterprise Risk Services (ER)

(37) The ER is responsible for ensuring that the ERMF is implemented across the University and effective oversight is maintained through regular reporting on material risks. More specifically, ER is responsible for facilitating the assessment of and providing reports to the VCRCC and the SRAC, at intervals decided by them, to raise awareness on:

a. UQ's Top Risks based on Managed Risk Levels (MRL) (i.e. the level of risk remaining after considering the effectiveness of the existing controls or risk treatments) and their management. UQ's Top Risks are developed by ER, and approved by USET, with reference to lower level Top Risks registers (e.g. identification of common themes and trends), targeted management consultation, consideration of changes in both the University's internal and external environment, risk events and incident data.
b. The effectiveness of the General Management Controls.
c. Key emerging risks.
d. UQ's key risk indicators.

Section 4 - Monitoring and Review

(38) Management is responsible for effective risk management with the ER being an enabling function, and Internal Audit providing objective assurance.

(39) Under the direction of Senior Executives and the Senate, the following three cohorts within the University will undertake monitoring and review activities to assess and ensure effective and efficient risk management and controls. While each group has its own monitoring and review objectives and scope consistent with their respective roles in the organisation, there will be ongoing communication and consultation amongst them to ensure effective and efficient monitoring and reviews at each level and avoidance of duplications.

Management

(40) Managers will monitor and review their operational activities, risks and controls to ensure effective and efficient performance, governance, risk management and compliance. Monitoring and reviews performed at this level will be the most detailed and generally embedded in the routine processes, procedures, systems and activities of front line operating management.

Heads of Enabling Functions

(41) In addition to their 'Management' obligations noted above, Heads of Enabling Functions and Divisions (COO portfolio and DVCs' support services) will monitor and review their function-specific risks across the University and ensure the ongoing effectiveness of the related controls including policies and procedures.

Internal Audit

(42) Internal Audit is responsible for providing objective assurance on the adequacy and effectiveness of risk management.

Section 5 - Recording and Reporting

(43) Risk owners will record pertinent information and data relating to their risks and controls in the risk register format provided on the ER website.

(44) The following reports on risks and controls will be produced:

Report Title	Report Content	Report Producer	Report Recipient	Frequency
Top Risks	The key risks of the University based on their Managed Risk Levels (current risk levels) at the time of reporting, including the specific controls managing these risks and any additional proposed controls to reduce the risks to Target Risk Levels (acceptable risk levels).	ER in consultation with VCRCC and USET	VCRCC, USET and SRAC	Yearly full review, half yearly progress updates, and quarterly any major changes to the risk profile
Key Emerging Risks	The key emerging risks of the University and what preparatory work or pre-emptive actions (if any) management has decided to take.	ER in consultation with VCRCC and USET	VCRCC, USET and SRAC	As necessary, with yearly full review
Key Risk Indicators	The key risk indicators measuring UQ's compliance with the RAS.	ER in consultation with VCRCC and USET	VCRCC, USET and SRAC	Yearly
General Management Controls (GMCs)	The effectiveness of the GMCs per each USET member and overall, at University level.	ER in consultation with VCRCC and USET	VCRCC, USET and SRAC	On a rolling basis and thereafter annually

Section 6 - Appendix

Appendix A - Risk Appetite Statement (RAS)

(45) See linked: Risk Appetite Statement.

Appendix B - General Management Controls (GMCs)

(46) The GMCs are inherent to the general management functions of leading, directing, planning, organising, staffing, coordinating and controlling any organisation. These controls form the foundations of the University's internal control system and help provide a robust, systematic and perpetual defence against threats to achieving the University's objectives. The GMCs should be implemented and assessed for their effectiveness at the UQ level and any of the lower levels including faculties, schools, institutes, controlled entities, functions, divisions, teams and projects.

#	Control Objective	Principal Question (All 'Yes' responses must be supported by verifiable evidence)
1	Clarity of objectives, strategies and KPIs	Have the objectives and strategies been clearly defined, aligned, prioritised and communicated to those who need to know?
2	Stakeholder management	Have the primary stakeholders been identified and strategies put in place to recognise and protect their rights and develop respectable, equitable and mutually beneficial relationships with them?
3	Enabling organisational structure	Does the organisational structure facilitate the effective and timely implementation of the strategy and the monitoring, measuring and reporting of performance?
4	Proper plans and budgets	Are there approved plans and budgets for all objectives, strategies, initiatives/projects and have these plans and budgets been communicated to those who need to know?
5	Clarity of roles, responsibilities and accountabilities (Note 3)	Are the roles, responsibilities and accountabilities for the delivery of prioritised objectives and outcomes clearly articulated and assigned to individuals or teams?
6	Capable staff	Are the management and other pivotal/critical roles staffed by competent people?
7	Authority and delegations	Do Managers and staff have appropriate authorities/delegations and mandate to achieve the objectives/outcomes expected of them?
8	Supportive culture	Do Managers and staff behave in accordance with UQ Values and the Staff Code of Conduct Policy?
9	Safety	Are processes and protocols in place to protect people from harm?
10	Compliance	Is there a robust process in place to demonstrate compliance with applicable laws and regulations and are regulatory breaches (if any) recorded, reported and promptly rectified?
11	Security of assets	Is there effective security over assets including systems, information and vital records?
12	Performance monitoring and reporting	Are portfolio/area and staff performances against their respective KPIs and plans measured, monitored and reported on and timely actions taken to remedy any gaps in performance?
13	Responsible use of resources	Are there controls in place to ensure responsible, sustainable use and management of University resources including natural resources?
14	Appropriate records and reports	Are records and reports required for business and/or legal/regulatory reasons produced and are they relevant, reliable, timely and adequately retained?
15	Continuity of operations	Are there robust plans and processes in place to ensure continuity of business-critical operations?
16	Supervision, Monitoring and Reviews of Internal Controls	Is there effective supervision, monitoring and review of the effectiveness of implemented controls related to staff compliance with (local) operating procedures, systems and processes, including prompt remediation of any unfavourable variances?
17	Management Assurance	Does management provide reliable assurance and/or evidence to demonstrate effective and efficient performance, governance, risk management and compliance?

Note 3:

Accountability refers to the decision maker's obligation to explain the use of delegated authority towards the achievement of agreed objectives and outcomes.

Responsibility refers to the obligation to perform specific actions, under the instruction of and/or for the accountable party, towards the achievement of agreed objectives and outcomes.

Appendix C - Risk Matrix

(47) See linked: Risk Matrix.

Appendix D - Definitions, Terms and Acronyms

Term	Definition
ERMF	Enterprise Risk Management Framework
RAS	Risk Appetite Statement
ER	Enterprise Risk Services
GMCs	General Management Controls
IRL	Inherent Risk Level (It is the level of risk assuming there are no controls specifically designed and implemented to manage that particular risk)
MRL	Managed Risk Level (It is the level of risk taking into consideration the total effectiveness of all the existing controls or risk treatments that act upon that risk)
TRL	Target Risk Level (It is the desired (or acceptable) level of risk considering the University's risk appetite and tolerance levels, to be achieved via implementation of proposed controls)
SRAC	Senate Risk and Audit Committee
VCRCC	Vice-Chancellor's Risk and Compliance Committee
USET	University Senior Executive Team
USLG	University Senior Leadership Group
Systemic Issue	An issue that meets ALL the following conditions: • It is a problem or an event that has negative consequences which has occurred or is inevitable; and • Is a materialised risk or an issue that will result in further risk exposure/s; and • It is a confirmed (verified) irregularity, deficiency, or vulnerability, not just speculation or hearsay; and • If left unmanaged, it will continue to exist (and probably deteriorate); and • It is demonstrably prevalent across UQ, organisational area or function, depending on the context.

[1] ISO 31000:2018 Risk Management – Guidelines

Status and Details

Status	Current
Effective Date	30th August 2024
Review Date	22nd June 2026
Approval Authority	Director, Governance and Risk
Approval Date	30th August 2024
Expiry Date	Not Applicable
Policy Owner	Joanna Spanjaard Director, Governance and Risk
Enquiries Contact	Governance and Risk Division