1.0 Purpose and Scope

1.1 Context

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.

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.

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.

1.2 Risk Management Obligations

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:

- *Financial Accountability Act 2009* (Qld) – requires the establishment and maintenance of an appropriate system of risk management.
- *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.
- *Higher Education Standards Framework (Threshold Standards) 2021* – requires that risks to higher education operations are identified and material risks managed and mitigated effectively.
- *Crime and Corruption Act 2001* (Qld) – refers to corruption risks and development of prevention strategies.
- *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.

1.3 Risk Management Objectives

Risk management at UQ is:

- 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
- contextual (i.e. risks are assessed against specific objectives) and recognises that uncertainty could affect objectives adversely and/or beneficially.

UQ's risk management objectives are to facilitate the achievement of its strategic and operational objectives including:

- Value creation and protection;
- Effective and efficient performance and compliance; and
- The development, enhancement and protection of its strategic and operational capabilities.

Enterprise Risk Management Framework

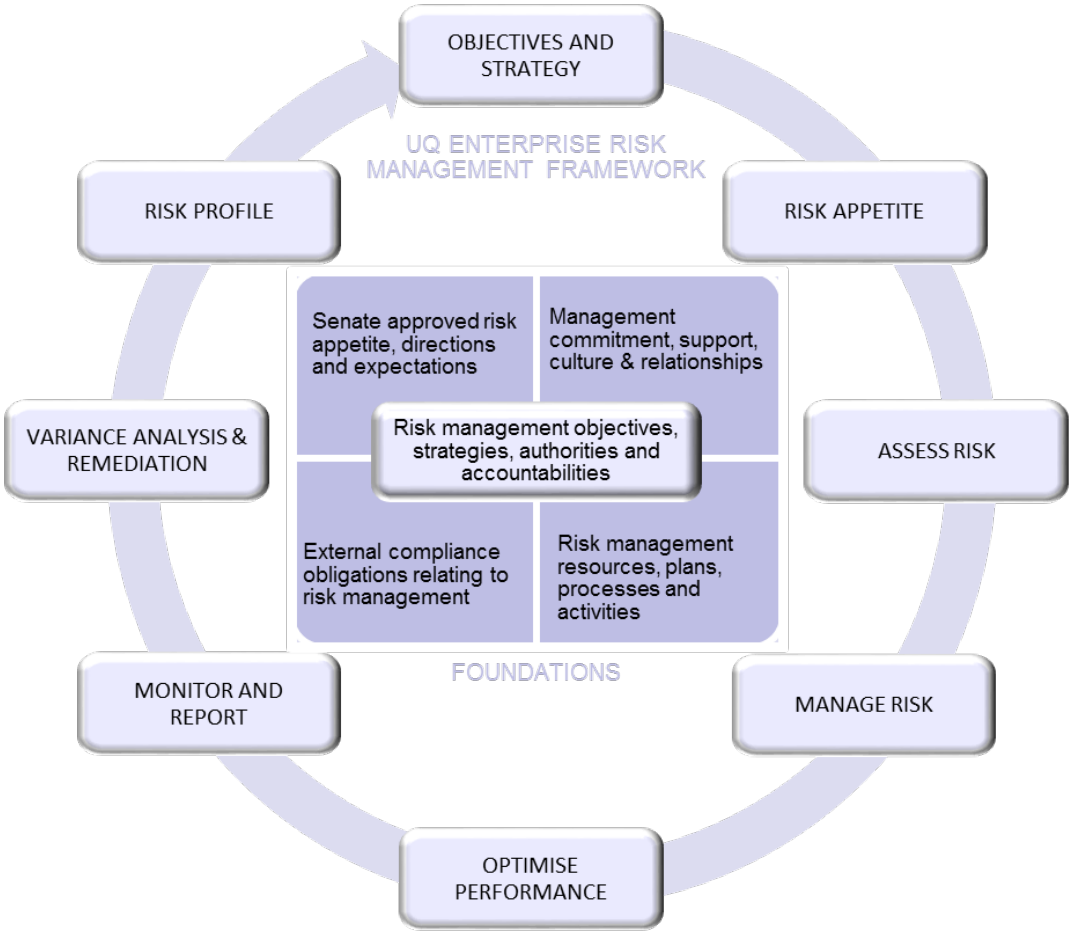
UQ's Enterprise Risk Management Framework (**ERMF**) provides the overall framework, direction and oversight for the systematic, disciplined and consistent identification and assessment of risks (including opportunities) and for their effective and efficient management.

[1] ISO 31000:2018

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.

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

- 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.
- Contextual (i.e. risks are assessed against specific objectives) and recognises that uncertainty could affect objectives adversely and/or beneficially.
- Built on and supported by the following five 'pillars':
  a. Senate's expectations and risk appetite
  b. Management/ leadership commitment and support for risk management function, organisational culture and relationships
  c. External compliance obligations relating to risk management
  d. Risk management objectives, strategies, mandate and accountabilities
  e. Risk management resources, plans, processes and activities



1.4 Scope and Application

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.

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 and Information Technology Services. These more detailed risk governance documents are consistent with and give further effect to the ERMF.

2.0 Key Requirements

To demonstrate effective and efficient risk management, UQ will:

Risk appetite

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 an overview of 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 (ERS) 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.

d. The RAS is operationalised via the Risk Matrix including the Risk Tolerance and Action Table (**Appendix D**).

Risk management culture

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

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.

m. Facilitate the continual improvement and enhancement of the University.

Roles and responsibilities

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

Safety

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; Workplace Health and Safety - Policies and Procedures Library.

Compliance

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

Investments

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

Assess its risks using the Risk Matrix (**Appendix D**) and record the risks and controls in the relevant risk register template provided on the ERS website.

Risk Mitigation

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.

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

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

General Management Controls

Manage its risks through the design, development, and implementation of effective and efficient controls, including General Management Controls (**GMC**s) as defined in **Appendix C**. 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.

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

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 UQ Incident Management Procedure for detailed incident management processes and protocols including escalation requirements.
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 to be informed when the impact on UQ is rated as ‘Major’ or ‘Extreme’ as per the Risk Consequence Rating Table (**Appendix D**).

Actively monitor and follow up negatively trending or adverse movements in key risk indicators and take appropriate steps to remedy unfavorable 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 will be promptly informed of unfavorable 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 D**).

Reporting

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

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

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

3.0 Roles, Responsibilities and Accountabilities

3.1 Senate

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.

3.2 Senate Risk and Audit Committee

The role of the Senate Risk and Audit Committee (SR&AC) is to oversee the assessment and management of risks. The Committee's responsibilities in relation to enterprise risk include:

1. Review the tone and risk culture of UQ and promote robust discussion around risk appetite and tolerance for risks.
2. 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.
3. Advise Senate on significant issues and changes to the University's risk profile.
4. Receive annual advice upon the effectiveness of the ERMF, including annual advice whether risks are being managed in accordance with RAS.

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

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.

3.4 Vice-Chancellor and USET

The Vice-Chancellor, with support from USET, is responsible for:

- Creating and maintaining a risk-aware culture, including reinforcing commitment to and role modelling risk-informed decision making.
- Exercising management oversight responsibility, ensuring effective risk management practices as per this ERMF, and transparent risk reporting to Senate.

3.5 University Senior Leadership Group (USLG)

Under the ERMF, members of the USLG are responsible for:

1. Assessing and managing the risks to their portfolio's objectives and strategies;
2. Maintaining risk registers in the approved format and ensuring the accuracy and currency of their risk registers;
3. Monitoring and reviewing their risks and controls with sufficient frequency to ensure the currency of their risk profile and ongoing effectiveness of controls;
4. Providing timely and positive assurance on the management of their risks and on the effectiveness of the General Management Controls within their portfolios;
5. Facilitating annual reviews of their material risks and controls by ERS and any other ad hoc reviews of risks and controls that the ERS may undertake to meet SR&AC and/or VCRCC needs, and ensuring that any deficiencies identified through the review and assurance processes are promptly rectified; and
6. Ensuring their direct reports undertake steps 1 to 5 above for their respective areas of responsibility.

3.6 Enterprise Risk Services (ERS)

The ERS 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, ERS is responsible for facilitating the assessment of and providing reports to the VCRCC and the SR&AC, at intervals decided by them, to raise awareness on:

1. 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 ERS, 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.
2. The effectiveness of the General Management Controls.
3. Key emerging risks.
4. UQ's key risk indicators

4.0 Monitoring and Review

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

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***

  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***

  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***

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

5.0 Recording and Reporting

Risk owners will record pertinent information and data relating to their risks and controls in the risk register format prescribed in Appendix E.

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).	ERS in consultation with VCRCC and USET	VCRCC, USET, and SR&AC	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.	ERS in consultation with VCRCC and USET	VCRCC, USET, and SR&AC	As necessary, with yearly full review
Key Risk Indicators	The key risk indicators measuring UQ's compliance with the RAS.	ERS in consultation with VCRCC and USET	VCRCC, USET, and SR&AC	Yearly
General Management Controls (GMCs)	The effectiveness of the GMCs per each USET member and overall, at University level.	ERS in consultation with VCRCC and USET	VCRCC, USET, and SR&AC	On a rolling basis and thereafter annually

6.0 Appendix

6.1 Appendix A – Risk Appetite Statement (RAS)

UQ's overall attitude towards risk is that of a **prudent risk taker**.
That is:

1. UQ has a **HIGH APPETITE** for risks that meet all of the following conditions:
    a. The risk is associated with initiatives, operations and activities that support UQ's strategic goals and priorities and have a credible prospect of providing moderate to high net returns or contributions to its objectives; and
    b. UQ has the capabilities to manage the risk effectively and efficiently to acceptable levels, or demonstrable risk capacity to sustain the loss should the risk materialise; and
    c. Any negative impact/s on risk categories for which UQ has a low or nil appetite can be managed to a tolerable level (see below).

2. UQ has a **LOW OR NIL APPETITE** for risks that meet one or more of the following conditions:
    a. The risk has the potential to significantly erode or cause intolerable damage or harm to the health and safety of our people, UQ's culture, reputation, operational resilience, financial viability, and/or social and legal licence to operate; or
    b. UQ does not have the capabilities to manage the risk effectively and efficiently, nor does UQ have the capacity to sustain the loss or negative consequence should the risk materialise.

Tolerance and treatment of risks with LOW or NIL appetite

In some cases, despite having a low or nil appetite for some risks, UQ may have to **tolerate** those risks at higher levels because:

a. It is impossible, impracticable and/or cost prohibitive to eliminate those risks or reduce them to low levels; and
b. Those risks cannot be avoided as they are inherent to initiatives, operations and activities that are essential to UQ given its objectives and strategy.

In such circumstances where UQ has no choice but to tolerate a higher risk level, the risk exposure will be reduced to as low as reasonably practicable (**ALARP**) via application of robust, cost-effective and affordable controls.

Examples (non-exhaustive list):

- Health and safety risks
- Compliance risks
- Foreign interference risks
- Cyber security risks
- Risks to reputation
- Fraud risks

6.2 Appendix B - Risk Categories

The following table can be used to assist with the identification of risks to facilitate the development of a risk assessment and management plan (non-exhaustive).

#	Exposure	Description
Focus area categories		
1.	Research & Innovation	▪ Research & innovation strategic targets, outputs, performance and outcomes (includes partnerships, commercialisation, investments, etc) ▪ Research resources and capabilities including staff, financial sustainability and funding diversification ▪ Quality of research outcomes ▪ Competitiveness including funding diversification, market share, demand and capabilities ▪ Investment projects and programs ▪ Adaptability and change management – operational agility ▪ Innovation and opportunities, including with partners ▪ Partner reputation, reliability, credit risks, etc. ▪ Intellectual property, including encumbrances, licences, commercialisation activities, etc. ▪ Research integrity and ethics ▪ Security, availability, performance, quality/reliability of research facilities, infrastructure, experiments, systems, data and research samples ▪ Safety of research activities including experiments, travel and use of materials facilities and equipment ▪ Legal and regulatory compliance, including retention of licences, permits, foreign relations, national security risks, export controls, sanctions, information security, privacy, personal information, jurisdiction (domestic & international) obligations, etc ▪ Insurable activities
2.	Teaching & Learning	▪ Teaching & learning strategic targets, outputs, and outcomes ▪ Teaching resources and capabilities including staff and funding ▪ Quality of teaching outcomes ▪ Teaching integrity and ethics ▪ Assessment integrity and ethics ▪ Student employability, including work integrated learning quality and availability ▪ Teaching facilities, infrastructure, data and systems' availability, security, performance, quality/reliability ▪ Legal and regulatory compliance as well as program accreditation by professional bodies ▪ Partnerships
3.	Students	▪ Students' related strategic targets, outputs and outcomes ▪ Student experience and retention ▪ Student outcomes including employability ▪ Student behaviour/conduct, safety, security and well being ▪ Student diversification
4.	Stakeholders, Relationships and Reputation	▪ Brand /image, credibility/trust, attractiveness ▪ Constructive, respectful and mutually beneficial relationships ▪ Actual and potential benefits – donations/endowments, support, etc. ▪ External engagement ▪ Other partnerships
Operational categories		
5.	Staff	▪ Equity and diversity ▪ Recruitment and selection ~~rigour~~ ▪ Capabilities, productivity and performance e.g. workforce and succession planning ▪ Retention, development and progression ▪ Industrial relations including employer and employee conduct

#	Exposure	Description
		▪ UQ Values, Code of Conduct ▪ Resilience / continuity of HR operations (e.g. payroll)
6.	Health, Safety and Wellness	▪ Health and safety of students, staff, volunteers, and visitors ▪ Staff wellbeing
7.	Strategic	▪ Statutory functions and powers as defined by the UQ Act ▪ Operating Model ▪ Performance, achieving Strategic Plan KPIs
8.	Financial	▪ Financial position / resilience ▪ Financial performance ▪ Budgeting and forecasting ▪ Accounting, Reporting and Disclosure integrity ▪ Resilience / continuity of operations
9.	Governance, Legal and Compliance	▪ Statutory approvals, licences, permits and certificates ▪ Legal and contractual rights and powers ▪ Oversight, monitoring, review and assurance activities and capabilities ▪ Ethics and integrity, (corrupt conduct, fraud) ▪ Resilience / continuity of operations
10.	Facilities and infrastructure	▪ Security ▪ Quality/Integrity /Reliability ▪ Availability / operational capabilities, including utilities ▪ Performance (optimum utilisation) ▪ Resilience / continuity of operations
11.	Systems and Information Management	▪ Authenticity/ integrity / reliability of systems and information; ▪ Security and accessibility; ▪ Availability and useability; ▪ Productivity ▪ Agility (future needs) ▪ Resilience / continuity of operations

6.3 Appendix C – General Management Controls (GMCs)

The GMCs are inherent to the general management functions of leading, directing, planning, organizing, 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 Code of Conduct?
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.*

6.4 Appendix D - Risk Matrix

Consequence Rating Table

(Where there are multiple types of impacts, use the highest rating for scoring risk)

IMPACT TYPE:	INSIGNIFICANT	MINOR	MODERATE	MAJOR	CRITICAL (potential RAS breach within 1 year)
HEALTH AND SAFETY Physical & Psychosocial	·Near miss event. ·No first aid or medical treatment required.	·First Aid injury or illness.	·Injury or illness requiring medical intervention or treatment. ·Reversible, temporary impairment.	·Serious injury or illness requiring hospitalisation. ·Ongoing impairment with functional restriction.	·Permanent impairment with significant functional restriction. ·Fatality / fatalities.
CULTURE / UQ VALUES	Some non-supervisory staff unaware of and/or their behaviour occasionally inconsistent with UQ Values, Code of Conduct, and/or local safety procedures.	Middle management not appropriately responding to staff behaviour that is inconsistent with UQ Values, Code of Conduct and/or safety procedures.	·Noticeable reduction in staff morale at a faculty, institute, or central divisional level. · Widespread staff perception that senior management does not appropriately respond to staff breaching UQ Values, Code of Conduct Principles and/or safety procedures.	·Noticeable reduction in staff morale across UQ. ·Sustained inability to fill essential roles and/or attract sought-after potential staff in a timely manner. ·Persistent failure to retain valued staff for desired periods of time. · Widespread staff perception that UQ does not appropriately respond to senior management staff breaching UQ Values, Code of Conduct Principles and/or safety procedures.	·Students and/or staff lose trust in UQ's commitment and ability to abide by its Values. ·Majority of internal stakeholders believe UQ's culture is corrosive and/or noticeably detrimental to UQ's success, and to the success of its staff and students.
COMPLIANCE and LEGAL RISK (Compliance with laws, regulations, contracts, licenses, court judgements, UQ policies and procedures)	·Award of damages or negotiated settlement less than $100K net outlay (not regulator related). ·Breach of a local standard operating procedure but not of any UQ policy or procedure.	·Minor corrective actions from regulator on non-essential matters. ·Award of damages or negotiated settlement between >$100K - $500K net outlay (not regulator related). ·Minor breach of a UQ policy or procedure.	·Court or regulator-imposed fines and penalties less than $500K. ·Breach of law/regulation/license but without the consequences described in 'Major' or 'Critical'. ·Award of damages or negotiated settlement between >$500K-$1M (net loss) ·Significant but ad hoc breach of a UQ policy or procedure.	·Court or regulator-imposed fines and penalties >$500K - $10M. ·Show cause notice, major adverse finding or enforceable undertaking issued by regulator. ·Award of damages or negotiated settlement between >$1M - $10M (net loss). ·Significant and systemic breaches of UQ policies or procedures.	·Criminal conviction of UQ and/or its executive/s in their official capacity. ·Court imposed fines and penalties >$10M. ·Loss of mission-essential licence /accreditation. ·Award of damages against UQ or negotiated settlement costing UQ >$10M (net loss).
REPUTATION Key stakeholders: · Students and Staff (current and prospective) · Alumni / Donors / Partners / Peers · Government; all levels · Research Investors / Customers · Community; domestic and international · Suppliers, Unions	·Negligible impact. ·Ad hoc negative mentions or rumours of a negative event on social media.	·Adverse conventional or social media coverage for a brief time. ·Limited ability to meet some legitimate but insignificant student, staff and/or other stakeholders' demands and expectations.	·Regular adverse conventional or social media coverage. ·Students and staff (including unions) frequently and publicly express their disapproval and disappointment at UQ. ·Short-term failure to meet legitimate and significant student, staff and/or other stakeholders' demands and expectations.	·Ongoing criticism of UQ in conventional or social media gradually undermining public perception of UQ. ·Sustained long-term failure to meet legitimate and significant student, staff and/or other stakeholders' demands and expectations.	·Strong, sustained and largely unanimous criticism of UQ by key stakeholders or general public, via conventional or social media. ·Very public and rapid withdrawal of support for, and trust in, UQ by its key stakeholders.
STRATEGIC *Strategic KPIs are the highest priority KPIs included in UQ's Strategic Plan*	Negligible but has potential to adversely impact UQ's strategic KPIs.	Negative but acceptable variations in less than 10% of UQ's strategic KPIs when assessed on an annual basis or against annual milestones.	Significant but acceptable negative variations in >10%-20% of UQ's strategic KPIs when assessed on an annual basis or against annual milestones.	Significant or unacceptable negative variations in >20%-30% of UQ's strategic KPIs when assessed on an annual basis or against annual milestones.	Significant or unacceptable negative variations in more than 30% of UQ's strategic KPIs when assessed on an annual basis or against annual milestones.
FINANCIAL (Note 1) *Measured as adverse impact on budgeted annual EBIT*	Net adverse EBIT impact of less than 1% of budgeted total income: *this equates to negative EBIT impact of <$20M for 2021*	Net adverse EBIT impact of 1%-2.5% of budgeted total income: *this equates to negative EBIT impact of $20M -$50M for 2021*	Net adverse EBIT impact of >2.5%-5% of budgeted total income: *this equates to negative EBIT impact of >$50M -$100M for 2021*	Net adverse EBIT impact of >5%-10% of budgeted total income: *this equates to negative EBIT impact of >$100M - $200M for 2021*	Net adverse EBIT impact of greater than 10% of budgeted total income: *this equates to negative EBIT impact of >$200M for 2021*
OPERATIONS (Note 1) • Functions refer to Academic activities, i.e. research, teaching, learning • Support services refer to Non-Academic activities e.g. COO portfolio, professional services	Insignificant impact on the delivery or performance of non-essential functions and/or support services; issue/s quickly resolved.	·Minor, unplanned negative impact on the delivery or performance of non-essential functions and/or support services. ·Some damage, loss or contamination of non-essential facilities, infrastructure, resources (incl. research samples, data, information assets), systems or operational capabilities.	·Moderate, unplanned negative impact on the delivery or performance of essential functions and/or support services. ·Significant damage, loss or contamination of non-essential facilities, infrastructure, resources (incl. research samples), systems or operational capabilities. · Some damage, loss or contamination of essential facilities, infrastructure, resources (incl. research samples, data, information assets), systems or operational capabilities.	·Significant and/or sustained, unplanned impact on the delivery or performance of essential functions and/or support services during a less operationally critical time. ·Significant damage, loss, or contamination of essential facilities, infrastructure, resources (incl. research samples, data, information assets), systems or operational capabilities that **<u>can</u>** be replaced, repaired, or recovered from.	·Significant, unplanned negative impact on the delivery or performance of essential functions and/or support services during an operationally critical time and for an unacceptable period. ·Significant damage, loss, or contamination of essential facilities, infrastructure, resources (incl. research samples, data, information assets), systems or operational capabilities that **<u>cannot</u>** be practicably replaced, repaired, or recovered from.

Risk Tolerance & Action Table

Overall Assessed MRL at Enterprise Level	Recommended Action	Immediate Response to WHS Risk *(Refer to WHS Risk Management Procedure for specific action requirements)*	Sign-off/ Reporting level
Extreme	·If the MRL indicates a potential breach of Senate approved RAS, advise ERS immediately. ·Develop a Risk Management Action Plan and implement proposed controls/treatments as soon as practicable to lower the MRL to an acceptable TRL. ·Confirm effectiveness and timely implementation to ERS as per agreed action plan.	Task must not proceed. Appropriate and prompt action must be taken to reduce the risk to an acceptable level.	Vice Chancellor, VCRCC & SR&AC
High	·If MRL within RAS, accept risk and document the reasons. ·If outside of RAS, develop a Risk Management Action Plan and implement proposed controls/treatments as soon as practicable to lower the MRL to the TRL. ·Confirm effectiveness and timely implementation to ERS as per agreed action plan.	Task can only proceed in extraordinary circumstances**, provided it is within RAS, and there is authorization by relevant Head of Function* and a plan is in place to promptly reduce the risk to an acceptable level.	Relevant USLG member (the risk may be reported by ERS to VCRCC, USET and SR&AC, depending on the impact on UQ)
Medium	·If MRL within RAS, accept risk and document the reasons. ·If outside of RAS, develop a Risk Management Action Plan and implement proposed controls/treatments as soon as practicable to lower the MRL to the TRL. ·Regularly review existing controls for effectiveness and introduce new or changed controls if cost is justifiable. ·Develop and implement action plan, if new or changed controls are proposed, followed by re-assessment of new risk level after implementation.	Task can proceed upon approval of the risk assessment by relevant Line Manager or Supervisor is received. Implementation of a review cycle to review the risks and mitigate further wherever possible.	Relevant USLG member and relevant Head of Function*
Low	·Maintain and monitor existing controls to ensure they continue to be effective; ·Monitor internal and external changes in the portfolio's environment.	Task can proceed upon approval of the risk assessment by relevant Line Manager or Supervisor is received.	Relevant Line Manager or Supervisor

At each organisational level (e.g. faculty, institute, school, controlled entity, project, function, division), management has to identify their portfolio's or project's top risks and demonstrate the effective management of these risks.

** Relevant Head of Function; Head of school, Institute Deputy Director or Division Director*
*** Extraordinary circumstances are opportunities for the University that align with its strategic mission and RAS.*

Risk Level Calculator

Insignificant [1]	Minor [2]	Moderate [3]	Major [4]	Critical [5]
Medium	Medium	High	Extreme	Extreme
Low	Medium	High	High	Extreme
Low	Low	Medium	High	Extreme
Low	Low	Medium	Medium	High
Low	Low	Low	Medium	High

Likelihood Table

Likelihood of the risk materialising		Definition	Probability
5	**Very High**	Almost certain; extremely likely	> 90%
4	**High**	Very Likely; will probably occur	60% - 90%
3	**Medium**	Likely to happen	40% - 59%
2	**Low**	Possible but unlikely	10% - 39%
1	**Very Low**	Conceivable but extremely unlikely	<10%

'Essential' in the matrix above refers to those activities, staff, means, conditions, and resources that are of such importance that without these the university will be unable to deliver its core functions of teaching, learning and research.

Note 1; to provide meaningful risk ratings for risk assessments other than at UQ level (e.g. faculty, institute, school, function, division), the reference to budgeted total income in the 'Financial' impact line can be replaced by <u>local</u> budgeted total income. For projects, the 'Financial' and 'Operations' impact levels may be adjusted to better reflect the project specific impacts and tolerances. If lower level and/or adjusted consequence levels for Financial and/or Operations impact types have been used, the total risk rating needs to be reported by stating the organisational level of the assessment before the risk rating; e.g. Faculty-High, Project-Medium, School-Extreme, etc.

6.5 Appendix E®® – Definitions, Terms Acronyms

ERMF – Enterprise Risk Management Framework

RAS – Risk Appetite Statement

ERS – 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)

SR&AC – 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.

7.0 Meta Data for Document Management

Web Links	The University of Queensland Act 1998 Financial Accountability Act 2009 TEQSA Risk Assessment Framework
Approval Authority	Senate The Chief Operating Officer has the authority to update this document for administrative changes
Last Approval Date	22 June 2021
Next Review Date	5 years from last approval date
Audience	Whole of UQ
Notes	June 2021: major update to the Risk Appetite Statement (Appendix A) and the Risk Matrix (Appendix D)