ENTERPRISE RISK MANAGEMENT FRAMEWORK

CONTENTS

1 PURPOSE

1.1 This framework provides the methodology, processes, definitions and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management.

1.2 This policy forms part of the University's financial management practice manual, which contributes towards meeting the University's obligations under the Financial and Performance Management Standard 2019 (Qld), by ensuring the existence of an effective risk management system.

2 SCOPE

2.1 This framework is designed to ensure risk management is integrated into all aspects of the University's business. It does not identify all institutional risk, rather focus on the key risks across the University that can be readily monitored and reported on a regular basis.

2.2 This framework applies to:

- CQUniversity as whole
- all controlled entities and partnerships
- strategic, corporate (University) and project activities
- employees of the University whether permanent, temporary, full-time, part-time or casual, and
- any person who works in any other capacity for the University or is involved in University business.

3 FRAMEWORK

3.1 The University is committed to providing good governance through risk management and identifying and consistently analysing risks and opportunities inherent in the Strategic Plan and in University operations.

3.2 The framework provides a formal process to assist the University in:

- encouraging understanding by managers and their employees of the implications of risk exposures, opportunities and their risk management, in their day-to-day work and in strategic and corporate (University) planning activities
- developing and implementing procedures to ensure that risks are identified, assessed against accepted criteria and that appropriate measures are implemented consistently, and
- defining and documenting processes and responsibilities.

3.3 As with any management process, risk management has its limitations:

- risk management will not make decisions for the business, rather assists to inform decision making processes
- it is impossible to predict all negative consequences. Therefore, risk management will not guarantee independence from all risk, and
- risk assessments will not be all-encompassing and are therefore not fail-safe.

Risk management system

3.4 The major elements of the University's risk management system include:

- **Risk Management Policy** – formally outlines the institutional and individual responsibilities and requirements. It recognises the legislative mandate and the role of the University Council. The policy affirms the University's strategic commitment to building a risk management culture in which risks and opportunities are identified and managed effectively.
- **Risk Appetite Statement** – articulates the University's appetite for risk, and associated tolerance levels.
- Enterprise Risk Management Framework (this document) – outlines the process to guide, direct and assist everyone to better understand and adopt consistent risk assessment processes.
- University **Risk Register/s** – principal repository for recording and tracking risks, including recommendations/agreed actions from auditors, regulators, insurers and relevant agencies.

Risk appetite

3.5 The University's risk appetite refers to the amount and level of risk taking that the University is prepared to accept or avoid to achieve its strategic objectives.

3.6 The Risk Appetite Statement influences and guides decision-making, clarifies strategic intent and helps to ensure choices align with the capacities and capabilities of the University. In pursuing its vision, purpose and strategic goals, the University will accept a level of risk proportionate to the expected benefits to be gained and the impact or likelihood of damage. A summary of the Risk Appetite Statement is shown in Table 1 below.

Risk Drivers	Risk Appetite Range	Risk Approach
• Strategic growth • Research • Student learning and engagement	**High**	An entrepreneurial acceptance to risk taking
• Reputation • Financial sustainability and commercialisation	**Moderate**	A balanced and informed approach to risk taking
• People • Business disruption, systems and data security, and physical assets • Environmental sustainability	**Low**	Accepts as little risk as possible and takes a conservative approach to risk taking
• Culture and values • Health and safety • Legal, compliance and regulatory • Academic integrity	**Very Low**	Unacceptable to take risks with a no compromise approach to risk taking

Table 1: Risk appetite statement summary

Integrating risk management

Strategy

3.7 Risk management is a key component of the University's strategic planning and performance management systems. Institutionally, risk management supports delivery of the University's Strategic Plan; the University's Strategic Risk Register aligns with the University's strategic goals and institutional performance measures.

3.8 At the corporate (University) level, the corresponding risk register directly correlates with, and therefore underpins the management of, the priorities outlined in the University Plan. Similarly, within different enabling programs/projects, risk registers are in place to ensure the effective management of key risks which have the potential to affect areas of strategic importance or the achievement of key milestones.

Performance

3.9 The University's performance measures provide an indicator that helps it achieve its strategic goals. The University Plan is created and implemented based on these measures. Risks are uncertain events, be they opportunities or threats, that impact on the University's performance. The process of forecasting the potential for risks, assessing their impact, and putting in place measures to manage that impact is essential to the University's operations.

Risk assurance: the three lines of defence

3.10 The University adopts the three lines of defence model (outlined in Figure 1 below) in relation to risk assurance.

3.11 The model ensures effective and transparent management of risk by making accountabilities clear. Each of the three lines has a distinct role. The Council, Audit, Risk and Finance Committee, and the Senior Executive, upon recommendation from the University Management Committee, are the primary stakeholders that are served by the established lines and are in a position to ensure that the three lines of defence are reflected in the University's risk management control processes.

<table>
<tr><td rowspan="4">Internal Oversight</td><td colspan="3">University Council</td><td colspan="2">External Oversight</td></tr>
<tr><td colspan="2">• Establishes a governance structure (Council committees, executive responsibilities and risk management and assurance functions).
• Is ultimately responsible for the enterprise risk management framework and oversees its operation by management.
• Sets the risk appetite within which it expects management to operate and approves the Risk Appetite Statement.</td><td>• Approves the organisation's approach to risk management.
• Forms a view of the risk culture of the organisation and the extent to which that culture supports the ability of the organisation to operate consistently with its risk appetite, identifies any desirable changes to the risk culture and ensure the organisation takes steps to address those changes.</td><td rowspan="3">External Auditors</td><td rowspan="3">Regulators</td></tr>
<tr><td colspan="3">Audit, Risk and Finance Committee</td></tr>
<tr><td colspan="3">University Management Committee</td></tr>
<tr><td>Three Lines of Defence</td><td>1st Line of Defence
Risk Owners

Responsible for effectively and efficiently, identifying, assessing, and managing risks.</td><td>2nd Line of Defence
Review and Challenge

Responsible for university-wide risk framework, risk advice and oversight.</td><td>3rd Line of Defence
Internal Audit

Responsible for independent assurance of governance, risk management and internal control processes.</td></tr>
</table>

Figure 1: Three lines of defence model

Risk governance

3.12 The risk governance arrangements ensure that Council, Audit, Risk and Finance Committee, and University Management Committee have the relevant information to oversee and manage the University's risks. The risk governance model (outlined in Table 2 below) depicts the relationship between the three risk types and how risks are captured, reported and may be escalated in line with governance and accountability arrangements.

Risk Type	Risk Repository	Approval Authority	Reporting
Strategic Risk **Corporate Risk**	University Risk Register	Council Through the University Management Committee, Academic Board and Audit, Risk and Finance Committee.	Twice-yearly
Project (Activity) Risks	Project Risk Registers	Senior Executive member/Project Sponsor (or nominee) Through the University Management Committee, Academic Board and Audit, Risk and Finance Committee *(if applicable).*	As determined by the approval authority

Table 2: Risk governance model

3.13 The University recognises the critical importance of aligning risk management with performance management to ensure the effective pursuit of its strategic ambitions. As part of this integrated approach, the University Risk Register is scheduled to be reported concurrently with the University's performance against its institutional measures. This coordinated reporting framework aims to provide a comprehensive overview of the University's progress towards its goals while acknowledging and mitigating associated risks.

3.14 Significant or emerging risks may be reported to Council, through the Audit, Risk, and Finance Committee, outside of the regular reporting schedule if they are a new risk, the existing risk escalates in severity, or external factors necessitate immediate attention.

Organisational processes

3.15 Risk management should be embedded within University systems and processes to ensure that it is part of everyday decision-making. In addition to the University's strategic planning and performance management systems, risk management is to be embedded in the following key processes:

- **Annual planning and budgeting processes** – risk identification should occur as part of the annual planning cycle to inform planning and budgeting for the following year. Costs of implementing the annual plans, including consideration of costs associated with controls or treatments required to be incorporated into the budgeting process.
- **Project and program management** – as part of good project management practice, risks are actively identified, managed, escalated and reported throughout the lifetime of the project.
- **Development and review of University policy documents** – University policy documents specify the approach and expected actions required to manage a variety of risks, including those associated with legislative compliance, academic management, quality and equivalence, people management, finance and asset management.
- **Procurement and asset management** – risk management must be factored into decision-making for significant procurement and asset management related processes.

Risk management process

Overview

3.16 Risk management is a necessary consideration each time a decision is made – whether to make an investment or binding commitment, start a new project, develop a new relationship, or invest in or acquire assets in plant, equipment, technology or infrastructure. Activities and decision-making must be aligned with objectives and outcomes that help the University reach its strategic goals or successfully execute University plans. This is risk management.

3.17 The University's risk management process (outlined in Figure 2 below) is based on the International Standard - ISO 31000:2018 Risk management – Guidelines. The process and steps described are intended to help manage risk, taking into account the unique and special environments in which the University operates.

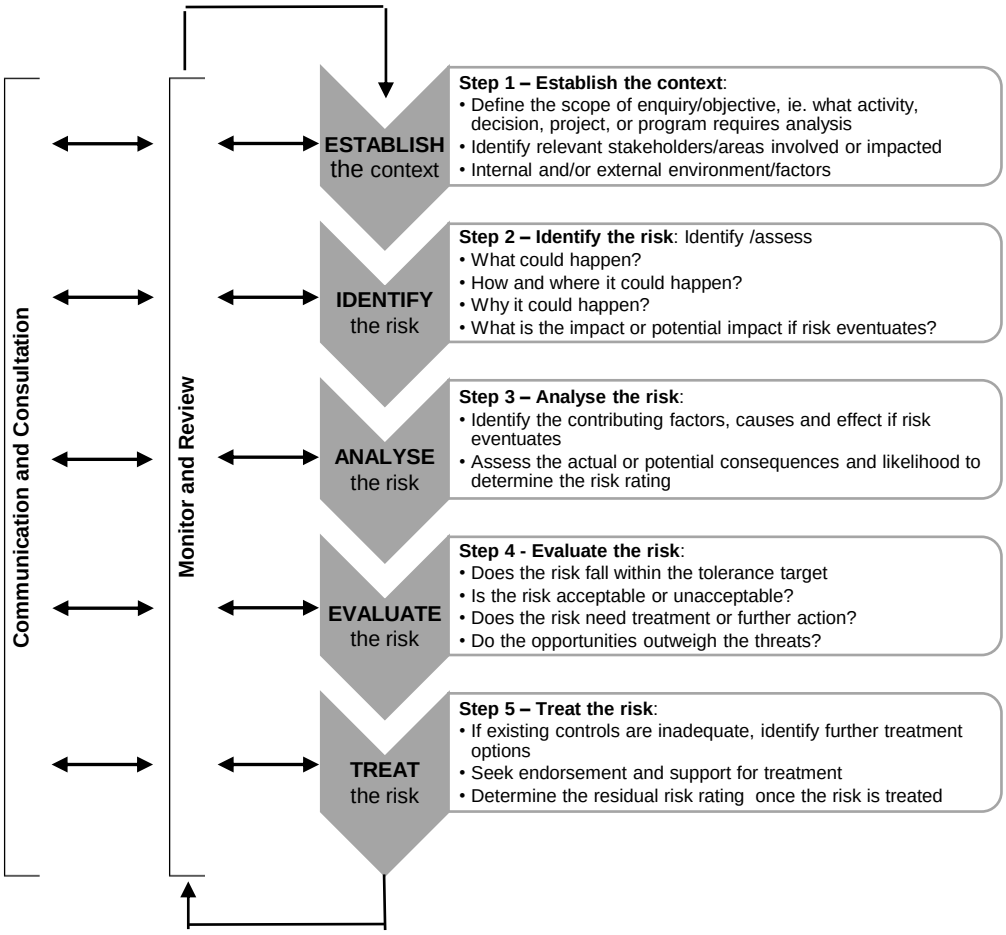

Figure 2: Risk management process

Establish the context

3.18 The scope, objectives and parameters of the activity where the risk management process is to be applied should be established. The context may vary according to the activity under review and may involve an evaluation of the internal and external context.

3.19 Internal context:

- Strategic and/or operational goals of the University and activity.
- University structure, culture, roles and responsibilities.
- Policy documents (including policies, procedures, and guidelines).
- Capabilities and resources.
- Information flows and decision-making processes (both formal and informal).
- Reports, surveys, questionnaires, business plans, audits, records and data or people that could provide expert judgement or knowledge.

3.20 External context:

- The social, cultural, political, legal, regulatory, financial, technological, economic, environmental, and competitive environment in which the activity occurs.
- Key drivers and trends.
- Stakeholder interests and perceptions.

The next three steps – Identify the risk, Analyse the risk and Evaluate the risk – form the risk assessment phase of the of the risk management process.

Identify the risk

3.21 The aim of this step is to generate a comprehensive list of risks based on events that might enhance, prevent, accelerate or delay the achievement of strategic or operational objectives. The identification process should include all significant risks, regardless of whether the source of the risk is under the control of the University.

3.22 In this step, identify sources of the risk, areas of impact, events (including changes in circumstances) and their causes and potential effect. Describe those factors that might cause, enhance, prevent, degrade, accelerate or delay the achievement of your objectives. Aim also to identify the effect associated if the risk eventuates.

3.23 Where possible, include sources of quantitative or qualitative data in the identification process to assist in the analysis of the risk and the application of risk ratings i.e. past records, industry practice, knowledge experts, and performance indicators.

Analyse the risk

3.24 Once the risk has been identified and the context, causes, contributing factors and effect have been described, look at the strengths and weaknesses of existing systems and processes designed to help control or mitigate the risk. Knowing what controls are already in place, and whether they are effective, helps to identify what, if any, further action is needed. Then determine the inherent risk (original) rating by:

- Assessing the consequence – the consequences or potential impact if the risk event occurred are described as insignificant, minor, moderate, major or extreme (refer Appendix 1).
- Assessing the likelihood – the likelihood of the risk occurring is described as rare, unlikely, possible, likely, or almost certain to occur (refer Appendix 2).
- Rating the level of risk – use the University Risk Rating Matrix (refer Appendix 4) to assess the consequence and likelihood levels; the risk matrix then determines whether the risk rating is low, medium, high or extreme.

3.25 The level of inherent risk refers to the consequence and likelihood of the risk occurring within the parameters of existing controls and is taken as the original risk rating prior to treatment.

Evaluate the risk

3.26 After determining the inherent risk rating, the risk should be evaluated to assess if the risk requires treatment and in what order of priority. Decisions should be made in accordance with legal and regulatory requirements and include a consideration of available resourcing and the University's appetite for risk, particularly in terms of potential financial and reputational impact.

3.27 Risk evaluation should also consider the degree of control over each risk and the cost impact, benefits and opportunities presented by the risk.

Treat the risk

3.28 Risk treatment involves selecting one or more options for modifying risks and implementing those options. Options for treating risks are not mutually exclusive and may include the following approaches:

- Avoid – do not start or continue with the activity that gives rise to the risk (for example, not entering a new market, not pursuing an opportunity).
- Transfer or share risk – through contracts, partnerships, risk financing, insurance etc.
- Reduce – implement controls and other treatments to reduce the impact or likelihood of an event.
- Accept – retain the risk by informed decision and develop a contingency plan if appropriate to minimise the impacts should they arise.

3.29 The following questions may also help to decide the options to treat risks:

- What is the feasibility of each treatment option and cost of implementing versus the benefits?

- What are the resources needed (employees, funds, technical)?
- Do the risk treatments comply with legal requirements, government and organisational policies including those concerning access, equity, ethics and accountability?
- What opportunities are created by the risk?

3.30 After careful consideration, risk treatments may also involve decisions to take or increase the risk to pursue an opportunity for the University. The most appropriate treatment option involves balancing costs against benefits together with due regard to legal, regulatory and other requirements such as social responsibility, the vision and the strategic goals of the University and the safety of employees and students.

3.31 Once the risk has been treated, assess the level of residual risk. Even when a risk has been treated and the controls are in place the risk may not be completely eliminated. The level of residual risk refers to the consequence and likelihood of the risk occurring after the risk has been treated. If the controls are effective, the residual risk rating should be lower than the inherent risk rating.

3.32 If, after treatment, there remains an unacceptably high residual risk, a decision should be taken about whether to retain this risk, repeat the risk treatment process, or continue to monitor and review the risk.

Monitor and review

3.33 Monitoring and review is an essential and ongoing component of the risk process and is undertaken in order to:

- detect any changes in the internal or external context
- identify emerging risks
- assess the performance of treatment options, and
- assess if a risk has changed and requires escalation or is no longer valid and can be archived.

3.34 The reviews may be self-initiated or undertaken by independent assessors such as internal or external auditors.

Communication and consultation

3.35 Communication and consultation with internal and external stakeholders should take place at all stages of the risk management process to communicate risks, causes, consequences, and treatments that should be developed. This will help to:

- ensure the interests of stakeholders are understood
- bring different areas of expertise together to better analyse risk and reduce uncertainty
- assist with the development of risk criteria, and
- secure endorsement and support for the treatment of risk.

Risk assessment

3.36 Risk assessment involves consideration of the sources of risk, the consequences, the likelihood of those consequences being realised, and the controls in place (and their actual effect). It is determined by the relationship between the consequence (impact or magnitude of the effect) and the likelihood (frequency and probability) if the risk occurs to produce a level of risk (risk rating).

3.37 A risk rating is determined for both the inherent and residual levels of risk. The residual risk rating relates to the final level of risk tolerability.

3.38 The following diagram (outlined in Figure 3 below) summarises the risk assessment criteria:

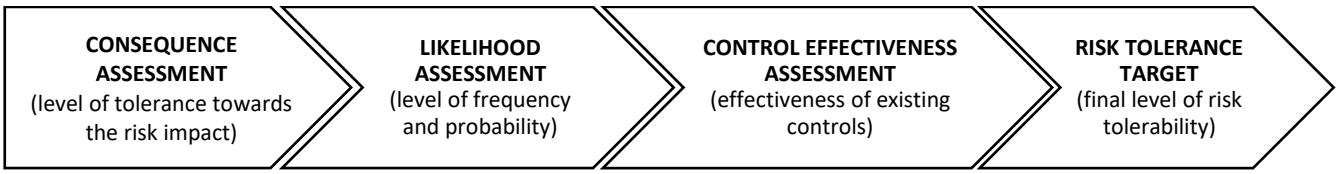

Figure 3: Risk assessment criteria

Consequence assessment

3.39 Various consequences can arise from a risk occurring. When determining the consequence level, to safeguard from the unnecessary application of treatments and costs, the consequence rating applied should be the most plausible, not the most extreme worst-case scenario.

3.40 The University's Risk Consequence Table (refer Appendix 1) illustrates the University's tolerance towards the impact of these consequences. In this way, it reflects the University's risk appetite. This approach provides a more accurate and robust overview of the true potential impact of a risk on the University and ensures clarity and consistency across risks and risk registers. It provides clear guidance as to the types of risk consequences and their corresponding rating.

3.41 The University measures the impact of consequence against the enterprise-level risk categories outlined in the risk categories section.

Likelihood assessment

3.42 The likelihood of a risk occurring is influenced by the frequency, probability and adequacy of the current controls in place to manage the risk. The most readily used approach to determining likelihood tends to be guided by experience to make an explicit judgement of the controls adequacy, which subsequently informs the likelihood of a risk being realised.

3.43 The University measures the likelihood rating of a risk occurring using the definition most appropriate to the context and risk under consideration and is outlined in the Risk Likelihood Table (refer Appendix 2). The table supports a process to determine how likely the University will be exposed to each specific risk, before and after considering current internal controls and considering factors such as:

- anticipated frequency
- the external environment (eg. regulatory, economic, competition, community expectations and market issues)
- the procedures, tools and skills currently in place, and
- history of previous event, both at the University and other providers.

Control effectiveness assessment

3.44 Throughout the consequence and likelihood assessments, the effectiveness of existing controls to mitigate risk is considered. To determine the quality of existing controls, consider what systems, procedures or practices currently exist to control the risk in question.

3.45 Once the controls have been identified, and their effectiveness analysed, the next step is to determine whether the risk is acceptable or needs further treatment.

3.46 The University's Control Effectiveness Table (refer Appendix 3) provides an assessment of the overall effectiveness of the controls in place that are mitigating the risk.

Risk tolerance target

3.47 Once all controls have been identified and the residual risk rating has been established, the risk tolerance target needs to be determined. This target informs the final level of risk tolerability that the University is willing to accept. The target may be lower than the residual risk rating and therefore further treatment is recommended to reduce the residual risk rating to the risk tolerance target.

3.48 If no further treatment is practical, and the option to either avoid, transfer, or reduce is not feasible, the University, through the Audit, Risk and Finance Committee and Council, must decide whether to accept the risk.

3.49 The Risk Tolerance/Treatment Table (refer Appendix 5) outlines the management action required for the various risk ratings. The expectation is that any significant risks should be escalated appropriately for consideration.

Risk registers

3.50 Risk registers identify and record the risks facing different areas of the business. Risk registers allow the University to assess the risk in context with the overall University strategy and help record the controls and treatments of those risks. Risk registers are based on the risk types of strategic, corporate (University), and project risks.

3.51 Each risk record captured in a risk register is subsequently recorded.

3.52 Information on reporting of risk registers is in the risk governance section of this document.

University risk register

3.53 The University Risk Register includes risks that need to be taken into account to achieve the medium to long term goals of the Strategic Plan, or which may impede delivering on the University Plan. It outlines the risks relating to the University's relationship with the broad external environment/ community.

3.54 The Register outlines the risks relating to the University's capabilities by considering:

- opportunities and threats associated with the local, regional, state and global economic, social, political, cultural, environmental, regulatory and competitive environments
- key focus areas of stakeholder strategies
- strengths and weaknesses of the University in attaining strategic goals and exercising a state of influence amongst local and national universities
- organisational structure and culture
- the identity and nature of interaction with key stakeholders
- the existence of any operational constraints
- operational goals and key performance indicators
- business resilience vulnerabilities
- relevant issues relating to recent change management risk, performance or audit reviews
- relevant stakeholder community concerns or requirements
- regulatory and contractual requirements and constraints, and
- business management systems.

3.55 The Strategic Planning and Risk Management Office is responsible for coordinating input and developing the University Risk Register and ensuring the register is reviewed and reported on (refer to the risk governance section of this document for reporting timelines).

Project (activity) risk registers

3.56 Major projects and activities of significance that contribute to achieving the objectives of the Strategic Plan must assess their potential exposure to associated risks. The risk assessment must be commensurate with the scale of the project or initiative and documented as part of the business case or by using the risk register template that is applied at the strategic and corporate risk level.

3.57 Project risk registers are developed and maintained by the Project Sponsor (or nominee) and must be reviewed and reported as determined by the approval authority.

3.58 Business areas should document operational risks that either currently affect or are anticipated to affect business processes, adhering to the project risk register processes and governance outlined in this document.

Risk categories

3.59 The University has identified enterprise-level risk categories and sub-risk categories (outlined in Table 3 below) in efforts to manage risks consistently. Risk categories and sub-risk categories are based on the type of risk, its source, and how it will be managed. Grouping risks in categories enables:

- a consistent way to identify, measure and manage risks
- a clear view of how risk categories and sub-risk categories interact with the risk appetite
- risks to be grouped so that they do not overlap with multiple risk types
- a consistent way to report risks across the University so that they can be easily reviewed to provide feedback and guidance.

Risk Categories	Sub-Categories	Descriptions
Strategic risk Potential events or circumstances that affect or are created by the University's strategic vision, goals and priorities. These circumstances may impact the University positively or negatively. Strategic activities are essential to meet our objectives to provide world-class, inclusive education, training and research and accept these activities may carry higher risk that needs to be managed accordingly.	**Strategic growth**	Activities or circumstances that impact the University's strategic growth, such as: • Collaborating with external partners • Investing in research projects and programs • Strategic and competitive positioning • Educational offerings • Organisational systems and structures • Commercialisation of research outcomes • Competent human resources.
	Research	Activities or circumstances that impact the University's research performance and ability to deliver, such as: • Research capabilities and capacity, including staffing and adequate funding • Research outcomes • Research integrity and ethics • Safety and security of research facilities and experiments.
	Student learning and engagement	Activities or circumstances that impact the University's objective to provide an excellent educational experience to students, such as: • Attraction, recruitment and retention activities • Learning and teaching activities • Student employability • Overall student experience.
	Reputation	Activities or circumstances that impact the University's image, or the long-term trust placed in the University by its stakeholders. This may occur due to factors such as performance, strategy execution, or an activity, action or stance taken by the University and/or individuals aligned with the University.

Risk Categories	Sub-Categories	Descriptions
Corporate risk Activities carried out or circumstances relating to the business of the University. They may be associated with structure, systems, people, services, or processes.	**Business disruption and system failure**	Activities or circumstances that impact the continuity of business systems and operations, such as access to enterprise level critical systems or information.
	Physical assets	Activities or circumstances that impact the University's physical assets, such as facilities, buildings, and infrastructure, such as: • Natural events (e.g. fire, flood, etc) • Security • Utilisation of facilities • Maintenance.
	People and culture	Activities or circumstances that impact the University's people, such as: • Attraction, recruitment and retention • Managing, motivating and developing our people • Organisational culture.
	Safety and health	Activities or circumstances that impact the health, safety and wellbeing of the University's employees, students, and visitors, such as: • Maintaining a safe, healthy and secure environment for students, employees, contractors, and visitors • Providing resources to support mental health • A strong safety culture • Maintenance of physical buildings and facilities.
	Information and communications technology/cyber and data security	Activities or circumstances that impact the University's technology and cyber and data security, such as: • Adequate systems and processes that protect critical and sensitive data • Adequate information and communication technology (ICT) resources.
	Fraud (internal and external)	Activities or circumstances that impact the University's integrity, such as: unethical behaviour, corruption, theft, embezzlement, money laundering, bribery, extortion, etc.
Financial risk	N/A	Activities carried out, or circumstances related to physical assets or financial resources, such as: government support, research funding, budget, accounting, reporting and disclosure, including internal control requirements, investments, capital and cash management, insurance, audit, financial investment decisions, etc.
Environmental risk	N/A	Activities carried out, or circumstances related to protecting and preserving the environment. Conversely, activities or circumstances that significantly degrade the environment, such as: pollution, impairment of ecosystem, etc.
Legal, compliance and regulatory risk	N/A	Activities carried out, or circumstances related to compliance with laws and regulations. Conversely, activities or circumstances that do not comply with laws and regulations and result in adverse impacts, such as: fines, reputational damage, material financial loss, sanctions, penalties, stakeholder risk, loss of operating licences/mandates, civil claims or liability, criminal prosecution or inability to enforce contracts, etc.
Major project risk	N/A	Activities or circumstances that impact the delivery of major projects, such as: time, cost, quality, resources, etc. They may be associated with strategic growth, systems, services or infrastructure.

Table 3: Risk categories and sub-categories

Emerging risks

3.60 The University's risk profile can change rapidly because of a crisis or event, or it could change more gradually over time. Some emerging risk issues that require monitoring in the current environment include:

- societal polarisation
- global risks and geopolitical tensions
- artificial intelligence, disruptive innovations and technology, and
- environmental, social and corporate governance (ESG).

Risk culture

3.61 The Senior Executive and University Management Committee members teams have an important role in developing a risk culture. The University will positively encourage a risk culture where understanding, managing and calculating a prudent level of risk is part of the everyday decision-making process.

3.62 The elements that will contribute to a positive risk culture are:

- leadership, clearly defined responsibilities and the University's appetite for risk as articulated in the Risk Appetite Statement
- communicating the benefits of risk management
- prioritise 'managing risks' (the objective) over 'risk management' (the process), and
- integrating risk management with other business processes and systems so the task of managing risk is perceived as a component of day-to-day business activities.

3.63 Innovation is a key driver for economic and technological growth. As risk-taking is a necessary feature of most types of innovation, this framework encourages a 'risk aware' approach to innovation that counters 'risk-averse' behaviour. Therefore, a greater awareness of uncertainties increases the chances of successfully implementing innovative solutions.

Annual risk workplan

3.64 To support the Audit, Risk and Finance Committee in executing its terms of reference and the University in implementing an integrated enterprise-wide risk management and planning and performance management approach and risk culture, a series of activities take place within an annual cycle that is captured within the following Annual Risk Workplan (outlined in Figure 6 below).

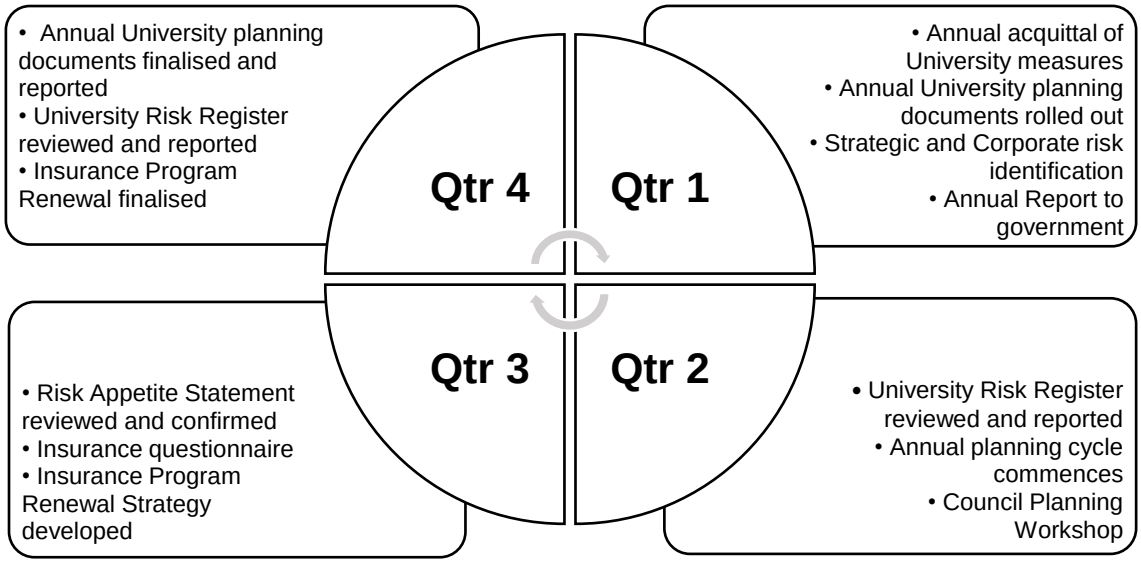

Figure 6: Annual Risk Workplan

4 RESPONSIBILITIES

Compliance, monitoring and review

4.1 Council is responsible for:

- defining risk appetite and risk tolerance
- approving key risk management documents such as the Risk Management Policy, this framework, and the Risk Appetite Statement, and
- considering risk management issued contained in Council reports.

4.2 Audit, Risk and Finance Committee is responsible for:

- providing advice on the appropriateness of the risk management processes implemented by the University for identifying, assessing and mitigating risk
- annually review the University's risk appetite and providing recommendations to Council
- monitoring and reviewing the risk management and mitigation strategies at appropriate intervals, and
- providing feedback to management on important risk management matters/issues raised by management.

4.3 Academic Board is responsible for:

- providing academic oversight to assure the quality of teaching, learning, research and research training, including by monitoring of potential academic risks, and
- advising Council on academic standards and practices.

4.4 Management committee/s are responsible for:

- providing feedback to the Director Strategic Planning, Risk and Insurance on risk management and mitigation strategies at appropriate intervals, and
- advising the Director Strategic Planning, Risk and Insurance on potential and emerging risks.

4.5 The Vice-Chancellor and President is responsible for:

- creating a control environment that promotes prudent risk management practices, calculated risk taking and effective internal controls
- escalating all known potential risks, emerging risks or major incidents to the Audit, Risk and Finance Committee in a timely manner
- ensuring the Risk Management Policy and this framework are being effectively implemented, and
- ensuring sufficient funds are prioritised to support effective management of risk across the University.

4.6 Senior Executives are responsible for:

- maintaining sound risk management processes and structures within their area of responsibility to conform with the University's Risk Management Policy and support arrangements
- identifying, recording and periodically evaluating risks
- developing and monitoring risk treatment plants to treat higher level risks in a timely manner
- maintaining up-to-date risk registers through periodic review and updates
- ensuring all major incidents or issues are reported and resolved in a timely manner
- complying with and monitoring employee compliance with policy documents and designated authorities, and
- incorporating risk treatments into business processes as required.

4.7 Project and contract managers are responsible for ensuring all aspects of risk management are appropriately identified, recorded and controlled for the project, including but not limited to financial, project delivery and contract management (tasks, high risk activities, qualifications and training).

4.8 Risk owners are responsible for identifying and managing all risks that are included in a relevant risk register. A risk owner is a nominated person responsible for:

- overseeing the effective and timely management of a specific risk
- selecting appropriate risk treatment strategies to address a specific risk
- continual monitoring and reporting of a specific risk, and
- confirming mitigation controls are operating effectively and adequately address the risk exposure.

4.9 Director Strategic Planning, Risk and Insurance is responsible for:

- supporting the University's risk-taking initiatives and helping the Council and Senior Executives manage a wide range of opportunities and risk
- designing and implementing an overall risk management process for the University
- analysing current risks and identifying potential strategic risks
- tailoring risk reporting to the relevant reporting audience
- maintaining and communicating up-to-date information and documentation for key risk areas
- maintaining records on insurance policies and claims, and
- building risk awareness amongst employees by providing supporting and training within the University.

4.10 Employees are responsible for:

- assisting in identifying risk s and controls
- conducting risk assessment as required
- seeking appropriate clarification on issues, problems and concerns identified
- reporting emerging risks, known risks, control breakdowns, fraud, issues, breaches, near incidents and incidents to their management and/or the Director Strategic Planning, Risk and Insurance, and
- following policy documents at all times to ensure compliance and maintaining the University's reputation.

4.11 The Director Strategic Planning, Risk and Insurance are responsible for implementing, monitoring, reviewing, and ensuring compliance with this framework.

Reporting

4.12 No additional reporting is required.

Records management

4.13 Employees must manage records in accordance with the Records Management Policy and Procedure. This includes retaining these records in a recognised University recordkeeping information system.

4.14 University records must be retained for the minimum periods specified in the relevant Retention and Disposal Schedule. Before disposing of any records, approval must be sought from the Records and Privacy Team (email records@cqu.edu.au).

5 DEFINITIONS

5.1 Terms not defined in this document may be in the University glossary.

Terms and definitions

Consequence: the outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

Control: any action taken by management, the Council, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.

Enterprise risk management: the culture, capabilities, and practices, integrated with strategy-setting and its performance that the University relies on to manage risk in creating, preserving, and realising value.
Inherent risk: the actual risk before any controls have been implemented. High inherent risks that are well controlled may fall out of view if only the residual risk is assessed. The purpose of assessing inherent risk is to ensure the University maintains focus on compliance with controls.

Likelihood: used as a qualitative description of frequency and/or probability of a risk occurring.

Residual risk: the remaining risk after controls have been put into place or after management has acted to alter the risk's likelihood or consequence.

Risk: the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of likelihood and consequence.

Risk analysis: a systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.

Risk appetite: the amount or level of risk, that the University is willing to accept in pursuit of value. The University pursues various objectives to add value and should broadly understand the risk it is willing to undertake in doing so.

Risk assessment: the overall process of risk analysis and risk evaluation.

Risk evaluation: the process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.

Risk identification: the process of determining what can happen, why and how.

Risk management: the coordinated activities to direct the University towards realising potential opportunities whilst managing adverse effects of risks.
Risk management processes: processes to identify, assess, manage, and control potential events or situations, to provide reasonable assurance regarding the achievement of the organisation's objectives.

Risk register: the summarised record of individual risks within each assessment. It includes risk ratings (inherent, residual and targeted), levels of control, risk decisions, responsible risk owner, and summary of key controls and/or mitigating actions.

Significant risk: a potential threat or hazard that, if realised, could have a notable impact on the University's ability to achieve its objectives or operate effectively and are risks identified as 'high' or 'extreme' against the risk assessment criteria.

Tolerance: the boundaries of risk taking outside of which the organisation is not prepared to venture in the pursuit of its long term objectives.

6 RELATED LEGISLATION AND DOCUMENTS

Financial Accountability Act 2009 (Qld)

Financial and Performance Management Standard 2009 (Qld)

Higher Education Standards Framework (Threshold Standards) 2021 (Cwlth)

International Standard ISO 31000:2018 Risk management – Guidelines

Risk Appetite Statement

Risk Management Policy

Standards for Registered Training Organisations (RTOs) 2015 (Cwlth)

Work Health and Safety Act 2011 (Qld)

Work Health and Safety Regulation 2011 (Qld)

Work Health and Safety Codes of Practice

7 FEEDBACK

7.1 Feedback about this document can be emailed to policy@cqu.edu.au.

8 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Council
Delegated Approval Authority	N/A
Advisory Committee	Audit, Risk and Finance Committee
Required Consultation	N/A
Administrator	Director Strategic Planning, Risk and Insurance
Next Review Date	15/05/2027

Approval and Amendment History	Details
Original Approval Authority and Date	Council 23/06/2020.
Amendment Authority and Date	Editorial amendment 27/02/2023; Editorial amendments 28/02/2024; Council 15/05/2024; Chief Operating Officer 06/08/2024.
Notes	

9 APPENDICES

Appendix 1: Risk consequence table

Consequence/Impact Table					
Risk Categories	**Insignificant** *Some loss but immaterial. Existing controls and procedures should cope with event or circumstance*	**Minor** *Event with consequences that can be readily absorbed but requires management effort to minimise the impact*	**Moderate** *Significant event or circumstance that can be managed under normal conditions*	**Major** *Critical event or circumstance that can be endured with proper management*	**Extreme** *Critical event/circumstance with potentially disastrous impact on business sustainability*
Strategic risk	• No material effect on objectives.	• Temporary or inconvenient delay in objectives.	• Marginal under achievement or material impediment to achieving objectives.	• Significant under achievement or major delay in achieving objectives.	• Non-achievement of objectives.
Reputation *Key stakeholders:* • *Students* • *Employees* • *Alumni* • *Government; all levels of domestic and foreign governments* • *Unions* • *Community*	• Ad hoc mentions or rumours of a negative event on social media. • Complaint by one or several un-associated members of the general public.	• Adverse local and social media coverage for a brief time. • Complaint by a group from the community which escalates into the public arena.	• Extended negative attention/concern from the public, State media or stakeholders.	• Significant continuous attention/concern from the public, national media or stakeholders.	• Prolonged and adverse national or international media coverage, undermining public confidence in the University. • Government intervention. • Irreparable damage to brand. • Key stakeholders disassociate themselves from the University.
Corporate risk	• No impact on operations • No impact on student numbers.	• Minor and brief impact on non-critical operations. • Up to 1% impact on student numbers.	• Minor and brief impact on critical operations. • Between 1% to 5% impact on student numbers.	• Significant impact on critical operations. • Between 5% to 10% impact on student numbers.	• Significant, irrecoverable impact on critical operations. • Greater than 10% impact on student numbers.
Business disruption and system failure	• Loss of critical systems leading to business disruption (up to 2 hours). • Some inconvenience to localised operations. • The incidence is absorbed by routine processes and management.	• Loss of critical systems leading to business disruption (more than 2 hours but less than 8 hours). • Inconvenient to localised area but tolerable period. • The incidence is contained and absorbed by management intervention.	• Loss of critical systems leading to business disruption (up to one day). • Inconvenient to several business areas for a protracted time but tolerable period. • The incidence requires management intervention.	• Loss of critical systems leading to significant business disruption (more than one day but less than 3 days). • Restricted ability to deliver critical services. • The incidence requires Senior Executive intervention.	• Loss of critical systems leading to severe or ongoing business disruption (more than 3 days). • Inability to deliver services. • Disruption causing campus closure/key business closure for more than one week. • Requires immediate Vice-Chancellor and President/Chancellor intervention.

Damage to physical assets	• Localised damage to a single general asset which can be remediated within a short time timeframe.	• Localised damage to a single general asset which can be remediated over a long timeframe. • Widespread damage to a single general asset which can be remediated over a short time timeframe.	• Localised damage to a single critical asset which can be remediated over a short timeframe. • Widespread damage to several general assets which can be remediated over a short timeframe.	• Localised damage to a single critical asset which can be remediated over a long timeframe. • Widespread damage to several general assets which can be remediated over a long timeframe.	• Widespread damage to several critical assets which can be remediated over a long timeframe. • Total and permanent destruction of one or more critical assets.
People and culture	• Increased turnover of personnel or absenteeism of <5%.	• Increased turnover of personnel or absenteeism of >5% but <10%.	• Localised employee dissatisfaction resulting in an employee satisfaction rating drop of > 10% but <15%. • Widespread employee dissatisfaction resulting in employee satisfaction rating drop of <5%. • Increased turnover of personnel or absenteeism of >10% but <15%.	• Localised employee dissatisfaction resulting in an employee satisfaction rating drop of >15%. • Widespread employee dissatisfaction resulting in employee satisfaction rating drop of >5% but <10%. • Increased turnover of personnel or absenteeism of >15% but <25%.	• Widespread employee dissatisfaction resulting in employee satisfaction rating drop of >10%. • Increased turnover of personnel or absenteeism of >25%.
Safety and health	• No medical treatment required. • Insignificant impact on physical, psychological or emotional wellbeing.	• Any injury which requires first aid treatment – no lost time. • Minor impact on physical, psychological or emotional wellbeing.	• Any injury requiring medical treatment and/or lost time of <5 days. • Moderate impact on physical, psychological or emotional wellbeing.	• Any injury requiring medical treatment and/or lost time of >5 days. • Total or permanently disabled. • Major impact on physical, psychological or emotional wellbeing.	• Loss of life where the University is potentially at fault or liable.
Financial risk	• Financial loss up to $100K.	• Financial loss between $100K to $300K. • Internal control weakness that meets 'materiality' threshold for possible disclosure.	• Financial loss between $300K to $2M. • Adjustment to financial statement disclosure.	• Financial loss between $2M to $10M. • Multiple significant internal control deficiencies.	• Financial loss in excess of $10M • Multiple material weaknesses and financial report restatement.
Environmental risk	• Brief pollution. • No impact or measurable impairment.	• Transient harm. • Minor impact.	• Moderate harm. • Measurable impact but not affecting ecosystem function.	• Significant harm. • Serious impact with some impairment of ecosystem function.	• Long term harm. • Very serious impact with significant impairment of ecosystem function.

Legal, compliance and regulatory risk	• A one-off breach of a policy document with negligible impact to the University's operating environment identified through immaterial breakdown of control and identified through operating processes.	• A minor breach of policy documents, occurring more than once which results in a warning but not of a breach of laws and/or a regulator warning. • The breach requires some modification to the operating environment.	• A breach of any laws, regulations, contracts or licenses, including notifiable incidents resulting in active monitoring by a regulator. • A significant breach in operating policy documents and result in significant breakdown of control environment.	• A major continued breach of policy and or process discovered by audit review. • A major breach resulting in: ○ Civil penalties <$1M ○ Show cause notices from Regulator ○ Loss of licence ○ Enforceable undertaking ○ Significant and system breach of University policy documents.	• A total systemic system failure and breach resulting in: ○ Prosecution with the potential for executives to be imprisoned ○ Civil penalties >$1M ○ Loss of critical licence/ accreditation.
Major project risk	• <1% of project budget. • Little or no delay. • Either party is irritated but no formal complaints.	• 1 to 5% of project budget. • Short delay/duration increased >2%. • Resolved at working level.	• 5 to 10% or project budget. • Significant delay / duration increased >10%. • Resolved at head of business area level.	• 10 to 25% of project budget. • Major delay/duration increased >25%. • Senior Executive intervention.	• >25% of project budget. • Project halted. • Major delay/duration increased >50%. • Legal recourse initiated.

Appendix 2: Risk likelihood table

Likelihood Rating

9.1 The number of times within a specified period in which a risk may occur either as a result of the external environment (e.g. regulatory, economic, competition, community expectations and market issues), business operations or through failure of operating systems, policy documents or history of previous events.

Level	Rating	Description	Frequency	Probability
A	**Almost Certain**	Expected to occur in most circumstances	Multiple / 12 months	> 80%
B	**Likely**	Will probably occur in most circumstances	Once / 12 months	61 – 80%
C	**Possible**	Might occur within a 5 year time period	Once / 12 months – 5 years	41 – 60%
D	**Unlikely**	Could occur during a specified time period	Once / 5 – 10 years	21 – 40%
E	**Rare**	May only occur in exceptional circumstances	Once / > 10 years	< 20%

Appendix 3: Control effectiveness table

Control Effectiveness Rating

9.2 Internal controls which are in place to support the early identification and rectification or lower the impact of the consequence (detective controls) or internal controls which are in place to prevent the risk will affect the likelihood of occurrence (preventative controls).

Level	Rating	Level of Protection/Mitigation
A	**Non-existent**	No identified or planned controls.
B	**Insufficient**	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.
C	**Sufficient**	The existing controls have some impact on mitigating the risk. Controls are inconsistent in their application, and monitoring and effectiveness. Controls are operating 50-79% of the time. Scope for improved effectiveness.
D	**Good**	Most controls are designed correctly, are in place and are effective. Controls are operating 80-99% of the time. Some additional work is required to ensure operational effectiveness and reliability.
E	**Excellent**	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. No improvement possible.

Appendix 4: Risk rating matrix

9.3 Risks within the University are rated using a common scale that assesses:

- the likelihood of the University being impacted in that way, and
- the potential consequences if the risk were to occur.

9.4 The risk rating is determined by combining the consequence and likelihood as shown as follows:

Likelihood	Consequence				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
Almost certain (5)	Medium	High	High	Extreme	Extreme
Likely (4)	Medium	Medium	High	High	Extreme
Possible (3)	Low	Medium	Medium	High	High
Unlikely (2)	Low	Low	Medium	Medium	High
Rare (1)	Low	Low	Low	Medium	Medium

Appendix 5: Risk tolerance/treatment table

9.5 The table below outlines the level of risk tolerance and treatment depending on the overall level of risk rating:

Risk Ratings	Risk Tolerance/Treatment Required
Extreme Risk	**Unacceptable/No Tolerance** Immediate/Urgent action required Escalate to the Vice-Chancellor and President/Senior Executive Group
High Risk	**Highly Cautious** Within 4 months/Action plan required Requires escalation to Senior Managers and/or applicable Senior Executive member
Medium Risk	**Tolerable/Conservative** Assess the risk and determine if current controls are adequate Management responsibility must be specified
Low Risk	**Acceptable** Manage through routine procedures Unlikely to need specific application of resources.