Enterprise Risk Management Framework

Description
This Framework outlines the University’s risk methodology and processes to support a consistent approach to managing risk across the University. It sets out the procedures and guidelines for implementing the principles outlined in the Enterprise Risk Management Policy.

The University’s enterprise risk management is aligned to the principles set out in the universally accepted standards; ISO 31000: 2018 Enterprise Risk Management and 2017 COSO ERM – Integrating with Strategy and Performance.

Related documents

- Enterprise Risk Management Policy
- Risk Appetite Statement
- Business Continuity Management and Resilience Policy
- Business Continuity Management and Resilience Framework
- Compliance Management Framework
- Code of Conduct
- Fraud and Corruption Control Framework
- Fraud Investigation Procedure
- Financial and Performance Management Standard 2009
- Financial Accountability Act 2009
- Health and Safety Policy
- The Responsible Conduct of Research

1. INTRODUCTION

Risk is the effect of an event and its likelihood of occurring. It is the chance of something happening that will have an impact on the achievement of our objectives. This impact may be positive or negative, meaning that risks may present an opportunity or a threat. Therefore, risk management can be value protecting or value enhancing. Minimising the effect of negative risk or threats, protects value. Taking considered risks to enhance growth, transformation and innovation enhances value.

Where risks are proactively identified and effectively managed there is potential for making the most of new opportunities.
Effective risk management supports the University to achieve our strategic and operational objectives. It is an essential part of good governance and helps to:

- Drive a culture where everyone takes responsibility for risk
- Empower our people to make informed decisions
- Enhance performance and organisational resilience

The Enterprise Risk Management Policy (the Policy) is the core document which affirms our commitment to building a robust and ethical risk management culture. The Policy is approved and mandated by the University Council. This Enterprise Risk Management Framework (ERMF) sets out the procedures and guidelines for implementing the principles outlined in the Policy.

2. **RISK MANAGEMENT PRINCIPLES**

Our risk management approach and processes are based on the following principles.

**Risk Management Governance and Culture**

The University’s risk management governance and culture are founded on our vision, mission, values, objectives, strategies and policies. Our risk management governance framework aims to:

- Set the tone for our approach to risk
- Reinforce the importance of managing risk proactively
- Empower our people to take responsibility for risk
- Foster a balanced risk culture

The goal of risk management is to support the achievement of our desired outcomes. Our risk governance and culture are based on:

- The risk management tone set by the University Council and its governing committees
- A values-based approach to risk that embeds risk management and decision making into everything we do
- Our people committing to our core values and principles by proactively managing risk
- Attracting, developing and retaining people who are committed to delivering higher risk-adjusted performance in accordance with our risk appetite

**Strategy and Objective-setting**

The University integrates enterprise risk management, strategy, and objective-setting in the strategic planning process. We establish and align our risk appetite with strategy and organisational objectives, turning strategy into practice while serving as a basis for identifying, assessing, and responding to risk.

**Performance**

We have defined performance measures that help us achieve our strategic objectives. Our operational plans are created and implemented based on these measures. Risks are uncertain events — be they opportunities or threats — that impact on our performance. The process of forecasting the potential for risks, assessing their impact, and putting in place measures to manage that impact is essential to our operations.
Review and Revision
We are committed to improving processes in all that we do. We will periodically review risk management processes to identify opportunities for improvement and increased risk management maturity.

Information, Communication and Reporting
Good communication is essential to effective risk management. It involves constant sharing of information sourced from both inside and outside the University. A timely, considered, and targeted approach to informing key stakeholders helps to foster a stronger risk management culture and informs risk responses.

3. ENTERPRISE RISK MANAGEMENT FRAMEWORK

The University’s ERMF applies to the whole University and our operations. It:

- Aims to influence our culture to better manage risk and opportunity. The ERMF considers our economic, social, regulatory, political and competitive environment locally, regionally and internationally in alignment with our strategic objectives.

- Recognises the influence and expectations of external funders, regulators, auditors and research collaborators. Through enterprise and operational risk management and the internal audit program, the ERMF connects those expectations with what we do.

- Includes the following documents:
  - **Enterprise Risk Management Policy (The Policy):** The Policy sets out the purpose, scope, risk principles, risk culture, approach, and roles and responsibilities for enterprise risk management across the University.
  - **Enterprise Risk Management Framework (ERMF):** The ERMF outlines our risk appetite statements and risk methodology and processes. It helps us to take a consistent approach to managing risk and sets out the procedures and guidelines for implementing the Policy. The ERMF ensures that significant risks are assessed, escalated and managed using the enterprise risk category criteria. The ERMF is approved by the Finance, Resources and Risk Committee (FRRC) and is intended to direct and assist staff to better understand the principles of risk management and use consistent guidelines and processes for risk management.
  - **Risk Appetite Statement (RAS):** The RAS is an essential component of the ERMF and provides the details of the appetite and type of risk that the University is willing to pursue, retain, accept, or tolerate in pursuit of our strategic and operational objectives. The RAS is approved by the FRRC.
  - **University Risk Registers:** These are central records of risks that have been identified across the University. They are used to profile risks, monitor controls, and prioritise how we treat risks. The risk registers help to report risks in a standard way, consistent with our governance framework. The University Council approves the Corporate Risk Register. The FRRC approves the Group and Division, Fraud, and Academic Fraud Risk Registers.

Several discipline specific frameworks exist across the University with each having their own distinct criteria and processes. They support, rather than override or replace the ERMF. Examples include:

- Health, Safety and Wellbeing
- Information Technology
- Compliance Management
4. RISK CATEGORIES

We can most effectively manage risks when they are clearly identified, and their impact can be measured. To help us identify and manage risks consistently, they are grouped together in enterprise-level categories and sub-categories.

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
- Linking key components of the ERMF to a risk category, which provides a clear view of how these interact with 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

In working towards our strategic and operational objectives, we assess and manage risks in alignment with the RAS.

For each risk category, sub-risk categories may be added. Sub-risk categories may fall within one or more enterprise risk categories. For example, damage to physical assets could have an operational and financial component.

The table below outlines our risk categories and sub-categories.

<table>
<thead>
<tr>
<th>Risk Categories</th>
<th>Sub-Categories</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>STRATEGIC RISK</td>
<td>Reputation</td>
<td>Activities or circumstances that impact the University’s image, or the long-term trust placed in us by our stakeholders. This may occur as a result of factors such as performance, strategy execution, or an activity, action or stance taken by the University and/or individuals aligned with the University</td>
</tr>
<tr>
<td></td>
<td>Students</td>
<td>Activities or circumstances that impact our objective to provide an excellent educational experience to students, such as: • Attraction, recruitment and retention activities • Teaching and learning activities • Student employability • Overall student experience</td>
</tr>
<tr>
<td></td>
<td>Research</td>
<td>Activities or circumstances that impact our research performance and through this, our ability to deliver social dividends, such as: • Research capabilities, including staffing and adequate funding • Research outcomes • Research integrity and ethics • Safety and security of research facilities and experiments</td>
</tr>
<tr>
<td></td>
<td>Innovation, Growth and Commercialisation</td>
<td>Activities or circumstances that impact innovation, growth and commercialisation, 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</td>
</tr>
<tr>
<td>Risk Categories</td>
<td>Sub-Categories</td>
<td>Descriptions</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OPERATIONAL RISK</td>
<td>Business Disruption and System Failure</td>
<td>Activities or circumstances that impact the continuity of business systems and operations, such as access to enterprise level critical systems or information.</td>
</tr>
</tbody>
</table>
|                                     | Physical Assets                             | Activities or circumstances that impact our physical assets, such as facilities, buildings, and infrastructure, such as:  
|                                     |                                             | • Natural events (e.g. fire, flood, etc)  
|                                     |                                             | • Security  
|                                     |                                             | • Utilisation of facilities  
|                                     |                                             | • Maintenance  
|                                     | People / Human Resources                    | Activities or circumstances that impact our people, such as:  
|                                     |                                             | • Attraction, recruitment and retention  
|                                     |                                             | • Managing, motivating and developing our people  
|                                     |                                             | • Organisational culture  
|                                     | Fraud (Internal and external)               | Activities or circumstances that impact our integrity, such as:  
|                                     |                                             | • Unethical behaviour  
|                                     |                                             | • Corruption  
|                                     |                                             | • Theft  
|                                     |                                             | • Embezzlement  
|                                     |                                             | • Money laundering  
|                                     |                                             | • Bribery  
|                                     |                                             | • Extortion  
|                                     | Information Technology / Cyber Security     | Activities or circumstances that impact our technology and cyber security, such as:  
|                                     |                                             | • Adequate systems and processes that protect critical and sensitive data  
|                                     |                                             | • Adequate IT resources  
|                                     | Health, Safety and Wellbeing               | Activities or circumstances that impact the health, safety and wellbeing of our staff, students, and visitors, such as:  
|                                     |                                             | • Maintaining a safe, healthy and secure environment for students, staff, contractors, and visitors  
|                                     |                                             | • Providing resources to support mental health  
|                                     |                                             | • A strong safety culture  
|                                     |                                             | • Maintenance of physical buildings and facilities  
| 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  
| 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 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.  

OPERATIONAL RISK: Activities carried out or circumstances relating to the day-to-day business of the University. They may be associated with structure, systems, people, services or processes. Managing operational risk protects value by avoiding adverse impacts. It also creates value by optimising positive outcomes.
5. **THE RISK MANAGEMENT PROCESS**

Risk management is an important part of University decision-making. It supports our activities and ensures operational plans align with strategic goals. The University applies the ISO 31000 Standard to manage risk, as outlined below. *(See Annexure A)*

![Risk Management Process Diagram]

6. **ROLES AND RESPONSIBILITIES**

The Policy formally outlines the roles and responsibilities for enterprise risk management across the University.

7. **RISK MANAGEMENT ACTIVITY PLAN**

How we approach and conduct the risk management activities within an annual cycle is documented in the Enterprise Risk Management Activity Plan. *(See Annexure B)*. Oversight of the plan is the responsibility of the office of the Director, Audit, Risk and Compliance and the Manager Risk and Business Continuity Planning.

8. **ERMF REVIEW**

Our risk management capability and risk environment are constantly changing and evolving. The ERMF is reviewed at least every three years to identify opportunities for improvement and to enhance our risk management maturity.
STEP 1: ESTABLISH THE CONTEXT

Establish the context by identifying the objectives of the activity or circumstance and then consider the internal and external parameters within which the risk must be managed.

Understanding the external and internal environment is the first step in the risk management process. It considers challenges and opportunities in the context of our vision and objectives, operating environment, and key stakeholders.

**Process:**

- **Set the scope** for the risk assessment by clearly identifying what you are assessing – for example, is it a new partnership, program, project, or perhaps an event?

- **Define the broad objectives.** Identify the reason for the risk assessment – perhaps a legislative change, a request from a regulator, alignment with strategic performance, implementing best practice or an operational change or review.

- **Identify the relevant stakeholders.** Aim for an appropriately inclusive process from the outset. Identify the areas that are, or might be, impacted and seek their input.

- **Gather background information.** Having proper information is important. Ask the right people and identify the information that is available. Sometimes it is useful to identify information that is not available (immediately) but may be necessary. Consider:
  - Strategic and business plans
  - Previous events, investigations or reports
  - Surveys, questionnaires and checklists
  - Insurance claim reports
  - Local or international experience
  - Expert judgment (internal University and/or external expertise)
  - Structured interviews
  - Focus group discussion

Where possible, consider both the strategic context and operational context, so you have a complete picture of the situation.

**Establishing the context** sets the framework for undertaking the risk assessment, makes clear the reasons for carrying out the risk assessment, and provides the backdrop of circumstances against which you can identify and assess risks.
The next three steps — Identify the risk, Analyse the risk and Evaluate the risk — form the Risk Assessment phase of the risk management process.

Risk Registers

The Risk Register (See Appendix 1) has been designed to capture risks and facilitate management and reporting of risks across the University.

We use the risk register to:

- Record risks
- Facilitate risk assessment
- Monitor and review risks
- Generate risk reports based on standardised templates

By using the register individual areas will, over time, build and maintain their risk profile. The University will also be able to generate reports for internal committees, auditors and external stakeholders seeking assurance that risks are being managed.

Appendix 1: The Risk Register Template

STEP 2: IDENTIFY THE RISKS / OPPORTUNITIES

Identify the risks and/or opportunities that might have an impact on the objectives of the University, Group, Division, School or Area.

Identify the sources of risk, areas of impact, events (including changes in circumstances), and their causes and potential consequences. Describe those factors that might create, enhance, prevent, degrade, accelerate or delay the achievement of your objectives. You should also aim to identify the issues associated with not pursuing an opportunity — that is, the risk of doing nothing and missing an opportunity.

In identifying the risk, consider these kinds of questions:

- **What could happen?** What are the potential outcomes, intended and unintended, both positive and negative? What might go wrong, or what might prevent the achievement of the relevant goals? What events or occurrences could threaten the intended outcomes?

- **How could it happen?** Is the risk likely to occur at all or happen again? If so, what could cause the risk event to recur or contribute to it happening again? Where could it happen? Is the risk likely to occur anywhere or in any environment/place? Or is it a risk that is dependent on the location, physical area or activity?

- **Why might it happen?** What factors would need to be present for the risk to happen or occur again? Understanding why a risk might occur or be repeated is important if the risk is to be managed.

- **What might be the impact?** If the risk were to eventuate, what impact or consequences would, or might this have? Will the impact be felt locally, or will it impact the whole University? Areas of impact to consider include: education or research program/activity, human impact, service delivery, financial consequences, legal or contract compliance, impact on reputation, and impact on achieving our strategic objectives.

- **Who does or can influence this activity?** How much is within the University’s control or influence? Make sure that those with delegations, control, influence, resources and budgets are at least informed if not actively involved.

Wherever possible, provide quantitative and/or qualitative data to describe the risk or support the risk rating. Sources of information may include past records, staff expertise, industry practice, literature and expert opinion.
STEP 3: ASSESS / ANALYSE THE RISKS

Develop a detailed understanding of the risk.

This step is important for separating minor risks from major ones. Once the risk has been identified and the context, causes, contributing factors and consequences have been described, look at the strengths and weaknesses of existing systems and processes designed to help control the risk. Knowing what controls are already in place and whether they are effective helps to identify what – if any – further action is needed.

Process:

- Start with **Inherent Risk**, which is the risk that an activity or event would pose if no controls or other mitigating factors were in place.
- **Assess the likelihood (See Appendix 2)**. The likelihood of the risk occurring is described as rare, unlikely, possible, likely, or almost certain to occur.
- **Assess the consequence (See Appendix 3)**. The consequences or potential impact if the risk event occurred are described as insignificant, minor, moderate, major or catastrophic.
  
  The assessment of likelihood and consequence is mostly subjective, but can be informed by data or information collected, audits, inspections, personal experience, institutional memory of previous events, insurance claims, surveys and a range of other available internal and external information.
- **Rate the level of inherent risk** by using the University Risk Matrix (See Appendix 4) to assess the likelihood and consequence levels. The risk matrix will determine whether the risk rating is low, medium, high or extreme.
- **Identify and record the controls that are in place to mitigate the inherent risk**. Controls may include legislation, policies or processes/procedures, staff training, segregation of duties, personal protective measures and equipment, and structural or physical barriers, etc.
- **Rate the Residual Risk** which is the risk that remains after controls are considered (i.e. the net risk or risk after controls). Once the controls have been identified an assessment is again made of the likelihood and the consequence of the risk occurring. This produces an accurate, albeit subjective, assessment of the residual level of risk — or risk rating — and helps in the next step to determine whether risks are acceptable or need further treatment.
- **Evaluate the effectiveness of existing controls (See Appendix 4)**. Determine what controls are already in place to mitigate the impact of the risk. Controls may be strong or weak and can be measurable and repeatable.
- **The escalation protocol (See Appendix 5)**. Identifies the management action required for the various risk ratings. The expectation is that any ‘High’ or ‘Extreme’ risks should be escalated appropriately for consideration.

- **Appendix 2: The Likelihood Table**
- **Appendix 3: The Consequence Tables**
- **Appendix 4: The Risk Matrix and Control Effectiveness Table**
- **Appendix 5: The Response/Treatment Table**
STEP 4: EVALUATE THE RISKS

Decide whether the residual risk is acceptable or unacceptable. The RAS will inform the level of tolerance that is acceptable and whether the risk is outside of our appetite.

Whether a risk is acceptable or unacceptable relates to a willingness to tolerate the risk — that is, the willingness to bear the risk after it is assessed in order to achieve the desired objectives.

**Process:**

- Decide on the **Target Residual Risk Rating** in the Risk Register which is the desired level of risk after the assessment of the residual risk.
- If the residual risk is not acceptable or tolerable or if the desired target risk rating is different to the residual risk then the risk should be treated (in accordance with the next step, Step 5 ‘Treat the Risk’).
- If the risk is acceptable or tolerable then no further action is needed. A risk could be acceptable even in the following circumstances:
  - No treatment is available
  - Treatment costs are prohibitive (particularly relevant with lower ranked risks)
  - The level of risk is low and does not warrant using resources to treat
  - The opportunities involved significantly outweigh the threats.

STEP 5: TREAT THE RISK

Ensure that effective treatment plans are in place to minimise the frequency and severity of the identified risk. Develop actions and implement treatments that aim to control the risk and achieve the desired target rating.

**Process:**

- **Work out what kind of treatment is desirable for this risk.** Determine what the goal is in treating this particular risk. For example, it could be to:
  - **Mitigate** the risk with further controls — The mitigation actions can be further dissected into four different types of controls:
    - **preventative controls** – designed to stop, discourage, pre-empt or limit the possibility of an undesirable event before it occurs. Preventive controls are proactive. e.g. Processing a requisition only after it has been properly approved.
    - **corrective controls** – designed to correct errors or undesirable events which have occurred and will prevent further occurrences. e.g. Automatic removal of malicious code by antivirus software.
    - **directive controls** – designed to encourage a desirable event. e.g. Written policies and procedures or training to assist in the accomplishment of area goals and objectives.
    - **detective controls** – designed to search for and identify errors or undesirable events after they have occurred so that corrective actions can be taken. As they are “after the fact/ event” controls, they are only appropriate when it is possible to accept the loss or damage incurred. e.g. Reviewing the monthly Statement of Account for activity in your area’s general ledger.
  - **Transfer the risk** — e.g. to someone else such as an insurer or contractor
  - **Avoid/terminate** it completely — e.g. drop the project
  - **Accept the level of risk** based on existing information — e.g. take the opportunity

The type of risk treatment chosen will often depend on the nature of the risk and the tolerance for that risk.
• **Document the risk treatment plan.** Once the treatment options have been identified, a risk treatment plan should be prepared. Treatment plans should identify responsibilities for action, time frames for implementation, budget requirements or resource implications and review process where appropriate.

• **Implement agreed treatments.** Once any options requiring authorisation for resourcing, funding or other actions have been approved, treatments should be implemented. The person assigned with the primary responsibility for the risk, is ultimately accountable for the treatment of the risk.

**STEP 6: MONITOR AND REVIEW THE RISK**

Monitor changes to the source and context of risks, the tolerance for certain risks, and the adequacy of controls. Ensure processes are in place to review and report on risks regularly.

To ensure structured reviews and regular reporting, we encourage you to identify a process that allows key risks within your area to be monitored.

Given the diverse and dynamic nature of our environment, it is important to be alert to emerging risks as well as monitoring known risks.

**Process:**

• **Continuous monitoring.** Once risks have been identified, recorded, analysed, and agreed treatments implemented, an appropriate monitoring and reporting regime should be established to keep track of how effective the treatment is in controlling the risk. Some risk treatments will become embedded into daily practices and methods of work.

• **Group, Division, School, or Area review.** Managers need to ensure there is a process for reviewing risk profiles and activities in their area of responsibility. Wherever possible, risk management should become an agenda item on management meetings or committees rather than a separate process.

  The aim of reviewing regularly is to identify when new risks arise and monitor existing risks to ensure that treatments or controls are still effective and appropriate. How frequently a review process and reporting cycle occurs will depend on the risk appetite and level of risk tolerance.

• **Risk Liaison Officers.** The Group and Division Risk Liaison Officer is the person who will share and discuss significant and emerging risks. They also serve on the forum for University-wide engagement and collaboration.

• **Risk Reporting.** The Manager Risk and Business Continuity Planning is responsible for facilitating the analysis and aggregation of risk reporting to the Executive Group and the FRRC. The format and structure of the risk report may vary, but in principle includes:

  o A summary of the most significant risks the University faces, including any changes in risk profile
  o Updates on treatment plans for all significant risks
  o The University’s performance against tolerance
  o Systemic / risk themes identified
  o New and emerging risks and changes to the previous risk profile

**STEP 7: COMMUNICATE AND CONSULT**

Effective communication and consultation enhances risk management. It is essential for all parties to understand each other's perspectives and, where appropriate, be actively involved in decision-making.
<table>
<thead>
<tr>
<th>#</th>
<th>Risk Title</th>
<th>Risk Description Concise description of the risk</th>
<th>Risk Category e.g. Operational</th>
<th>Inherent Risk</th>
<th>Current Key Controls/ Mitigating Actions</th>
<th>Residual Risk</th>
<th>Target Residual Risk Rating</th>
<th>Are any further treatment plans / actions required to improve the mitigation of the risk</th>
<th>Treatments/ Actions towards Achieving Target Residual Risk Rating</th>
<th>Proposed Completion Date</th>
<th>Accountable Person</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Q1</td>
<td>Q2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Y  N
## Likelihood Table

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost Certain</td>
<td>The event is expected to occur and possibly frequently.</td>
</tr>
<tr>
<td>Likely</td>
<td>The event will probably occur.</td>
</tr>
<tr>
<td>Possible</td>
<td>The event might occur, but occasionally.</td>
</tr>
<tr>
<td>Unlikely</td>
<td>The event is unlikely to occur, however could be a possibility.</td>
</tr>
<tr>
<td>Rare</td>
<td>The event is remote, and improbable, and may only occur in typical circumstances.</td>
</tr>
</tbody>
</table>
## Enterprise Risk Management Framework

### Strategic Risk
- **Key stakeholders:**
  - Government; all levels of domestic and foreign governments
  - Unions
  - Community

### Reputation
- **Key stakeholders:**
  - Students
  - Staff
  - Alumni
  - Government; all levels of domestic and foreign governments
  - Unions
  - Community

### Operational Risk
- **Risk Categories**
  - Insignificant: No material effect on objectives
  - Minor: Temporary or inconvenient delay in objectives
  - Moderate: Marginal underachievement or material impediment to achieving objectives
  - Major: Significant under achievement or major delay in achieving objectives
  - Catastrophic: Non-achievement of objectives

### Business Disruption and System Failure
- **Risk Categories**
  - Insignificant: Ad hoc mentions or rumours of a negative event on social media
  - Minor: Adverse local and social media coverage for a brief time
  - Moderate: Extended negative attention / concern from the public, State media or stakeholders
  - Major: Significant continuous attention / concern from the public, national media or stakeholders
  - Catastrophic: Prolonged and adverse national or international media coverage, undermining public confidence in the University

### Damage to Physical Assets
- **Risk Categories**
  - Insignificant: Limited loss of critical assets (up to 2 hours)
  - Minor: Loss of critical systems leading to business disruption (more 2 hours but less than 8 hours)
  - Moderate: Loss of critical systems leading to business disruption (up to one day)
  - Major: Loss of critical systems leading to business disruption (more than one day but less than 3 days)
  - Catastrophic: Loss of critical systems leading to business disruption (more than 3 days)

### Consequence / Impact Table

<table>
<thead>
<tr>
<th>Risk Categories</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strategic Risk</strong></td>
<td>Some loss but immaterial. Existing controls &amp; procedures should cope with event or circumstance</td>
<td>Event with consequences that can be readily absorbed but requires management effort to minimise the impact</td>
<td>Significant event or circumstance that can be managed under normal conditions</td>
<td>Critical event or circumstance that can be endured with proper management</td>
<td>Critical event/circumstance with potentially disastrous impact on business sustainability</td>
</tr>
<tr>
<td><strong>Reputation</strong></td>
<td>Ad hoc mentions or rumours of a negative event on social media</td>
<td>Adverse local and social media coverage for a brief time</td>
<td>Extended negative attention / concern from the public, State media or stakeholders</td>
<td>Significant continuous attention / concern from the public, national media or stakeholders</td>
<td></td>
</tr>
<tr>
<td><strong>Operational Risk</strong></td>
<td>Insignificant impact on operations</td>
<td>Minor and brief impact on non-critical operations</td>
<td>Significant impact on critical operations</td>
<td></td>
<td>Significant, irrecoverable impact on critical operations</td>
</tr>
<tr>
<td><strong>Business Disruption and System Failure</strong></td>
<td>Loss of critical systems leading to business disruption (up to 2 hours)</td>
<td>Loss of critical systems leading to business disruption (more 2 hours but less than 8 hours)</td>
<td>Loss of critical systems leading to business disruption (up to one day)</td>
<td>Loss of critical systems leading to significant business disruption (more than one day but less than 3 days)</td>
<td>Loss of critical systems leading to severe or ongoing business disruption (more than 3 days)</td>
</tr>
<tr>
<td><strong>Damage to Physical Assets</strong></td>
<td>Localised damage to a single general asset which can be remediated within a short timeframe</td>
<td>Localised damage to a single critical asset which can be remediated over a short timeframe</td>
<td>Localised damage to a single critical asset which can be remediated over a long timeframe</td>
<td>Localised damage to several general assets which can be remediated over a short timeframe</td>
<td>Widespread damage to several critical assets which can be remediated over a long timeframe</td>
</tr>
<tr>
<td></td>
<td>Widespread damage to several general assets which can be remediated over a short timeframe</td>
<td>Widespread damage to several general assets which can be remediated over a long timeframe</td>
<td></td>
<td></td>
<td>Total and permanent destruction of one or more critical assets</td>
</tr>
</tbody>
</table>
## CONSEQUENCE TABLE

<table>
<thead>
<tr>
<th>Risk Categories</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Some loss but immaterial. Existing controls &amp; procedures should cope with event or circumstance</td>
<td>Event with consequences that can be readily absorbed but requires management effort to minimise the impact</td>
<td>Significant event or circumstance that can be managed under normal conditions</td>
<td>Critical event or circumstance that can be endured with proper management</td>
<td>Critical event/circumstance with potentially disastrous impact on business sustainability</td>
</tr>
<tr>
<td>People / Human Resources</td>
<td>Increased turnover of personnel or absenteeism of &lt;5%</td>
<td>Increased turnover of personnel or absenteeism of &gt;5% but &lt;10%</td>
<td>Localised employee dissatisfaction resulting in a staff satisfaction rating drop of &gt;10% but &lt;15%</td>
<td>Localised employee dissatisfaction resulting in a staff satisfaction rating drop of &gt;15%</td>
<td>Widespread employee dissatisfaction resulting in staff satisfaction rating drop of &gt;10%</td>
</tr>
<tr>
<td></td>
<td>No medical treatment required. Insignificant impact on physical, psychological or emotional wellbeing</td>
<td>Any injury which requires first aid treatment – no lost time. Minor impact on physical, psychological or emotional wellbeing</td>
<td>Any injury requiring medical treatment and/or lost time of &lt;5 days. Moderate impact on physical, psychological or emotional wellbeing</td>
<td>Any injury requiring medical treatment and/or lost time of &gt;5 days. Total or permanently disabled. Major impact on physical, psychological or emotional wellbeing</td>
<td>Loss of life where the University is potentially at fault or liable</td>
</tr>
<tr>
<td>Health, Safety and Wellbeing</td>
<td>&gt;2% but &lt;4% negative impact on EBITDA. Internal control weakness that meets ‘materiality’ threshold for possible financial statement disclosure</td>
<td>&gt;4% but &lt;6% negative impact on EBITDA. Adjustment to financial statement disclosure</td>
<td>&gt;6% but &lt;10% negative impact on EBITDA. Multiple significant internal control deficiencies</td>
<td>&gt;10% negative impact on EBITDA. Multiple material weaknesses and financial report restatement</td>
<td></td>
</tr>
<tr>
<td>Financial Risk</td>
<td>1% - 2% negative impact on EBITDA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal, Compliance and Regulatory Risk</td>
<td>A one-off breach of a policy or procedure with negligible impact to the University’s operating environment identified through immaterial breakdown of control and identified through operating processes.</td>
<td>A minor breach of policies and procedures, 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</td>
<td>A breach of any laws, regulations, contracts or licenses, including notifiable incidents resulting in recommendations active monitoring by a regulator. A significant breach in operating policies or procedures and result in significant breakdown of control environment</td>
<td>A major continued breach of policy and or process discovered by audit review. A major breach resulting in: o Civil penalties &lt;$1M o Show cause notices from Regulator o Loss of licence o Enforceable undertaking o Significant and system breach of University policies and procedures</td>
<td>A total systemic system failure and breach resulting in: o Prosecution with the potential for executives to be imprisoned o Civil penalties &gt;$1M o Loss of critical license/accreditation</td>
</tr>
</tbody>
</table>

---

**Appendix 3**

The breach requires some modification to the operating environment. A significant breach in operating policies or procedures 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 policies and procedures
- A total systemic system failure and breach resulting in:
  - Prosecution with the potential for executives to be imprisoned
  - Civil penalties >$1M
  - Loss of critical license/accreditation
## RISK MATRIX and CONTROL EFFECTIVENESS TABLE

### Risk Matrix

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Extreme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost Certain</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Extreme</td>
<td>Extreme</td>
</tr>
<tr>
<td>Likely</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Extreme</td>
</tr>
<tr>
<td>Possible</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Rare</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>

### Control Effectiveness

<table>
<thead>
<tr>
<th>Control Effectiveness</th>
<th>Qualification Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very good</td>
<td>Risk exposure is effectively controlled and managed</td>
</tr>
<tr>
<td>Good</td>
<td>Majority of risk exposure is effectively controlled and managed</td>
</tr>
<tr>
<td>Satisfactory</td>
<td>There could be room for some improvement</td>
</tr>
<tr>
<td>Weak</td>
<td>Some of the risk exposure appears to be controlled, but there may be major deficiencies</td>
</tr>
<tr>
<td>Unsatisfactory</td>
<td>Control measures are ineffective</td>
</tr>
<tr>
<td>Non-Assessed</td>
<td>Controls are not assessed</td>
</tr>
</tbody>
</table>
## Risk Response / Treatment Table

<table>
<thead>
<tr>
<th>Risk Ratings</th>
<th>Risk Response / Treatment Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Extreme Risk</strong></td>
<td><strong>Unacceptable / No Tolerance</strong></td>
</tr>
<tr>
<td></td>
<td>Immediate / Urgent action required</td>
</tr>
<tr>
<td></td>
<td>Escalate to the Vice Chancellor / Executive Group</td>
</tr>
<tr>
<td><strong>High Risk</strong></td>
<td><strong>Highly Cautious</strong></td>
</tr>
<tr>
<td></td>
<td>Within 4 months / Action plan required</td>
</tr>
<tr>
<td></td>
<td>Requires escalation to Senior Managers and / or Heads of Groups/Divisions</td>
</tr>
<tr>
<td><strong>Medium Risk</strong></td>
<td><strong>Tolerable / Conservative</strong></td>
</tr>
<tr>
<td></td>
<td>Assess the risk and determine if current controls are adequate</td>
</tr>
<tr>
<td></td>
<td>Management responsibility must be specified</td>
</tr>
<tr>
<td><strong>Low Risk</strong></td>
<td><strong>Acceptable</strong></td>
</tr>
<tr>
<td></td>
<td>Manage through routine procedures</td>
</tr>
<tr>
<td></td>
<td>Unlikely to need specific application of resources.</td>
</tr>
</tbody>
</table>
### RISK MANAGEMENT ACTIVITY PLAN

The University’s risk management activities take place within an annual cycle that is captured within the following Risk Management Activity Plan:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Details</th>
<th>Outputs</th>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
</tr>
</thead>
</table>
| **Emerging Priorities – Executive Group** | • Review of changes in the business environment  
   • Update on Griffith strategy  
   • Revisit Internal Audit (IA) Plan to ensure ongoing alignment to strategic priorities and adjust where necessary | • Updated Issues List         |    |    |    | ✔  |
| **Alignment of Risk, Strategy and Performance** | • Strategy setting workshops and appetite and tolerance setting | • RAS dashboard                  |    |    | ✔  |    |
| **Risk Reporting**             | • Tracking and reporting of the risks, including emerging risks, to Executive Group and the Council via the FRRC | • Dashboard report              | ✔  | ✔  | ✔  | ✔  |
| **Risk Register Update**       | • Review of Risk Registers to ensure Business as Usual (BAU) risk profile is still representative | • Updated Risk Registers         | ✔  | ✔  | ✔  |    |
| **Risk Liaison Network Meeting** | • Manager Risk and Business Continuity Planning to facilitate the Risk Liaison Network meeting at least bi-annually | • Share best practices, discussing risks and issues (including emerging risks), mitigation plans, monitoring and reporting risks and improving risk awareness levels in their Groups / Divisions | ✔  |    | ✔  |    |
| **Group-Level Support**        | • Allocation of budget to undertake a deep-dive on a specific function / business activity to assist management with the application of better risk management practices, e.g. within a project or program of work, new business initiative or as part of operational business planning | • Dependent upon the activity   |    |    |    |    |

- ✔ indicates the activity is completed in the specified quarter.
- As required indicates the activity is completed when required.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequence</td>
<td>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.</td>
</tr>
<tr>
<td>Enterprise risk management</td>
<td>The culture, capabilities, and practices, integrated with strategy-setting and its performance that we rely on to manage risk in creating, preserving, and realising value.</td>
</tr>
<tr>
<td>Inherent risk</td>
<td>The actual risk before any controls have been implemented. High inherent risks that are well controlled may fall out of our field of view if only the residual risk is assessed. The purpose of assessing inherent risk is to ensure that we maintain focus on compliance with controls.</td>
</tr>
<tr>
<td>Likelihood</td>
<td>Used as a qualitative description of probability or frequency of a risk occurring.</td>
</tr>
<tr>
<td>Residual risk</td>
<td>The remaining risk after controls have been put into place or after management has acted to alter the risk's likelihood or consequence.</td>
</tr>
<tr>
<td>Risk</td>
<td>The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of consequence and likelihood.</td>
</tr>
<tr>
<td>Risk analysis</td>
<td>A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.</td>
</tr>
<tr>
<td>Risk appetite</td>
<td>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.</td>
</tr>
<tr>
<td>Risk assessment</td>
<td>The overall process of risk analysis and risk evaluation.</td>
</tr>
<tr>
<td>Risk identification</td>
<td>The process of determining what can happen, why and how.</td>
</tr>
<tr>
<td>Risk liaison officer</td>
<td>Designated professionals selected from within the Groups or Divisions who support enterprise risk management activities and represent the enterprise risk management viewpoint.</td>
</tr>
<tr>
<td>Risk management</td>
<td>The coordinated activities to direct the University towards realising potential opportunities whilst managing adverse effects of risks.</td>
</tr>
<tr>
<td>Enterprise risk management framework</td>
<td>The set of components that provide the methodology, processes, definitions and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management.</td>
</tr>
<tr>
<td>Risk management processes</td>
<td>Processes to identify, assess, manage, and control potential events or situations, to provide reasonable assurance regarding the achievement of the organisation's objectives.</td>
</tr>
<tr>
<td>Risk plan</td>
<td>A plan outlining a program of activities undertaken within a defined period to address key risk management objectives.</td>
</tr>
<tr>
<td>Risk register</td>
<td>The summarised record of all individual risks within each assessment. It includes: risk ratings (inherent, residual and targeted), levels of control, risk decisions, responsible officer, and summary of key controls and/or mitigating actions.</td>
</tr>
<tr>
<td>Tolerance</td>
<td>The boundaries of acceptable variation in performance related to achieving business objectives.</td>
</tr>
</tbody>
</table>