



# **JCU Risk Management Framework and Plan**

Document Contact: Chief of Staff

Approved by Council (4/24) 1 August 2024

## Contents

1.	RISK MANAGEMENT FRAMEWORK .....	2
1.1	General .....	2
1.2	What is Risk? .....	2
1.3	Why Should We Manage Risk? .....	2
1.4	Objectives.....	3
1.5	Risk Management Policy .....	3
1.6	Risk Management Plan.....	3
2.	RISK MANAGEMENT PROCESS.....	3
2.1	How Can We Manage Risk? .....	3
2.2	Overview .....	4
2.3	Communication and Consultation .....	4
2.4	Establish context.....	4
2.5	Defining Risk Criteria .....	5
2.5	Risk identification .....	5
2.6	Risk Analysis.....	6
2.7	Risk Evaluation .....	6
2.8	Risk Treatment.....	7
2.9	Monitoring and Review .....	8
2.10	Recording and Reporting .....	8
3.	RISK MANAGEMENT PLAN.....	9
3.1	Risk Management Responsibilities .....	9
	Council .....	9
	Audit, Risk and Compliance Committee .....	9
	Other Council Committees .....	9
	Vice Chancellor.....	9
	University Executive .....	9
	Chief of Staff (Risk Management Co-ordinator) .....	10
	Risk and Compliance Officer .....	10
	Manager Internal Audit.....	10
	All Managers and Staff (Risk Owners) .....	10
	Risk Champions .....	11
3.2	Risk Management Framework Review .....	11
3.3	Risk Register Establishment and Review .....	11
	University Level.....	11
	Division Level.....	11
	Project Level .....	11
	Activity Level.....	11
3.4	Risk Management Plan Progress Reports .....	12
3.5	Training .....	12
3.6	Summary of Key Risk Management Plan Activities.....	13
	Appendix A – Likelihood Ratings.....	14
	Appendix B – Consequence Ratings .....	16
	Appendix C – Risk Rating Matrix.....	19
	Appendix D – Control Effectiveness Ratings.....	20
	Appendix E – Risk Management Glossary .....	21

# 1. RISK MANAGEMENT FRAMEWORK

## 1.1 General

James Cook University recognises that risk management is an integral part of good governance and management practice and is committed to its application at all management levels within a university-wide framework.

JCU's risk management framework provides the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. The two key elements of JCU's framework are its Risk Management Policy, which establishes a mandate and commitment for managing risk, and the Risk Management Plan which details the procedures and processes by which risk management will be implemented within the organisation.

The JCU Risk Management Framework has been developed to meet three primary objectives:

1. To provide consistency to business risk management practices throughout the University.
2. To provide assurance that all key risks within the business are being identified and managed appropriately and to ensure the University, including management and the Council, are aware of key business risks.
3. James Cook University (JCU) as a Person Conducting a Business or Undertaking (PCBU) is required to demonstrate that it has done everything reasonable and practical in addressing WHS risks and this is operationally delivered via the JCU Officers. The Officers are required to demonstrate positive steps to exercise "due diligence" by definition of the *Work Health and Safety Act 2011* (the Act). This includes the identification of hazards and the elimination and mitigation of the associated risks.

JCU also recognises its risk management oversight responsibilities in respect of its controlled entities and non-controlled entities in which it has a significant interest. This includes the Singapore campus, which operates out of a different jurisdiction.

## 1.2 What is Risk?

The International Standard on Risk Management AS/NZS ISO 31000:2018 defines risk as "*the effect of uncertainty on objectives*". This definition highlights risk as an uncertainty of outcome. This uncertainty can relate to either a threat or an opportunity and risk management can relate to how we ensure threats don't result in negative consequences and how we ensure opportunities are realised.

## 1.3 Why Should We Manage Risk?

ISO 31000 defines risk management as "*coordinated activities to direct and control an organization with regard to risk*". It is the systematic and ongoing process of risk identification, assessment, treatment and monitoring. It can be applied at any level of the University including strategic, operational and at project level. It is not solely about limiting risk but rather about fully appreciating and recognising the risks we carry and balancing risk and reward in an informed manner.

Properly applied, risk management should:

- improve the likelihood that University objectives will be achieved
- reduce the likelihood of unwanted 'surprises'
- help the University maximise opportunities

- provide information to support University decision making
- provide a basis for effective resource allocation
- help the University meet compliance and governance requirements
- improve overall stakeholder confidence in the University
- reduce the likelihood of injury and illness throughout our facilities and across all activities.

The overarching objective of risk management is to ensure that risk identification, assessment and management occurs continuously in accordance with changes in the internal and external environment and that the University has processes in place to enable it to provide assurance to University management, the Council and the external community that processes are effective in controlling risk.

## **1.4 Objectives**

In support of the achievement of strategic and operational goals, the objective of the University's risk management plan is to provide a framework for all levels of management to enable, support and promote:

- awareness and understanding of the real and significant business risks and their impact;
- demonstration of due diligence in decision-making;
- exercise of appropriate duty of care;
- innovation through the taking of calculated risks in pursuit of business opportunity and excellence; and
- provision of assurance that business risks are properly managed, commensurate with their level of threat or exposure; and
- ensure that information about such risks and their management is properly communicated.

## **1.5 Risk Management Policy**

JCU has an adopted Risk Management Policy. This policy outlines the expectations that the Council and University Executive have with respect to risk management, and establishes the risk management responsibilities of the Council, Council committees, management and staff.

## **1.6 Risk Management Plan**

This Risk Management Plan specifies the approach, the management components and resources to be applied to the management of risk. It details the procedures, practices, assignment of responsibilities, sequence and timing of activities to help all people within the organisation manage risk. This plan is supported by other guidelines and procedures offering more detailed information on the management of specific types of risk, the management of risk within particular areas and the use of risk management tools.

# **2. RISK MANAGEMENT PROCESS**

## **2.1 How Can We Manage Risk?**

Inherent within any decision making is consideration of the various risks facing the University and coordinated response(s) to these risks. A rigorous and systematic approach to identifying and adequately managing risks and integrating this process into significant activities and function is essential.

Risk management is an ever-present management responsibility. All staff are required to be conversant with risk management concepts and practices and be able to utilise and demonstrate application of risk management principles within their areas of control. Staff familiar

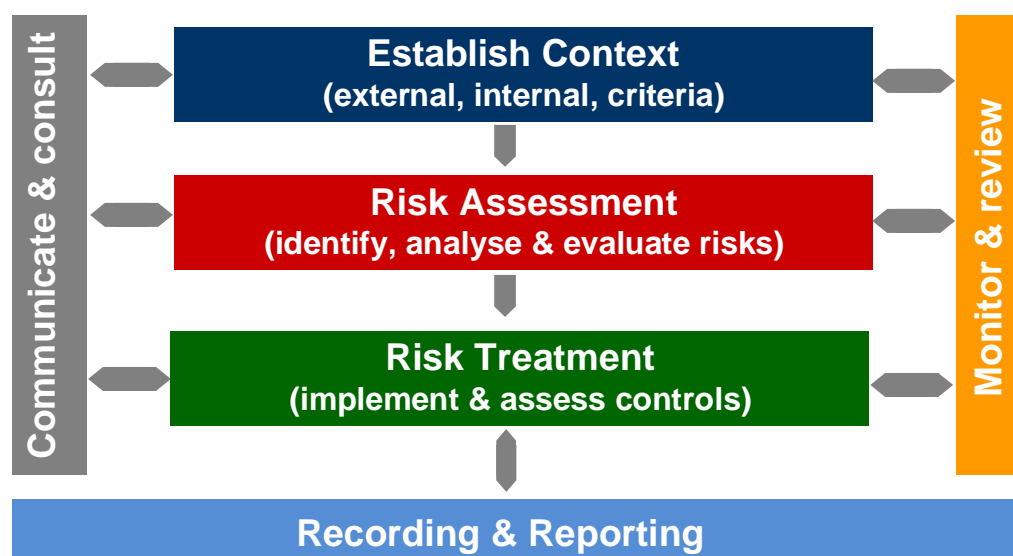
with the work undertaken in specific areas are well placed to identify risks in their own areas and recommend suitable strategies for controlling the impact of those risks.

## 2.2 Overview

Integrating risk management into an organization is a dynamic and iterative process, and needs to be customized to the organization's needs and culture. Risk management should be a part of, and not separate from, the organizational purpose, governance, leadership and commitment, strategy, objectives and operations.

The University's Risk Management process complies with AS/NZS ISO 31000:2018. Under this approach, there are six key stages to the risk management process.

1. Communicate and consult - with internal and external stakeholders
2. Establish context - the scope, boundaries and criteria
3. Risk Assessment - identify, analyse and evaluate risks
4. Treat Risks - implement and assess controls to address risk
5. Monitoring and review - risk reviews and audit
6. Recording and Reporting – effective governance



*Figure 1: JCU risk management approach using AS/NZS ISO 31000:2018 Risk Management Standard*

## 2.3 Communication and Consultation

Effective communication and consultation with key stakeholders regarding risk management processes, issues and initiatives is critical to the success of JCU's risk management framework. Staff must ensure that relevant stakeholders are consulted and informed of risk management activities. This will be done through means such as training, continuous professional development activities, standard agenda items on team meetings, dissemination of policies and procedures and through inviting feedback on key documents.

## 2.4 Establish context

Establishing the context of risk management at JCU is designed to customise the risk management process, enabling effective risk assessment and appropriate risk treatment.

Context is established by the risk leadership team and involves setting boundaries around the depth and breadth of risk management efforts to relevant matters required to achieve the

strategic intent of the University, and should reflect the specific environment of the activity to which the risk management process is to be applied.

Important considerations when determining context include:

- JCU's external environment – social factors, demographics, political, economic, environmental.
- JCU's stakeholders – students, customers, regulators, employers, politicians, media, insurers, service providers and suppliers, staff and volunteers.
- JCU's internal environment – goals, objectives, culture, risk appetite, organisational structures, systems, processes, resources, key performance indicators and other drivers.

## **2.5 Defining Risk Criteria**

It is important that JCU understands the amount and type of risk that it may or may not take, relative to objectives. Within the University's risk appetite statement, risk capacity and tolerances are expressed against a number of key risk indicators against categories of risk (refer Section 2.5). *Risk capacity* being the amount of risk an organisation can afford to take or sustain, and *risk appetite* being the amount and type of risk that the organisation is willing to take in order to meet their strategic objectives.

A range of appetites exist for different risks and these may change over time.

JCU is not averse to accepting, managing or reducing risk provided a thorough risk assessment has been carried out and when appropriate contingency plans and mitigation strategies have been developed.

In particular, JCU recognises that in order to achieve its objectives and capitalise upon opportunities during a period of significant change and uncertainty in the tertiary education sector, it will need to accept some level of well managed risk inherent in:

- Continuing to pursue academic and research excellence
- Investment in the re-profiling of courses and facilities to meet JCU's Corporate Strategy and the imperatives of a competitive market
- Pursuing innovative new methods, new approaches and new technologies
- Increased reliance on partnerships with the private and public sector
- The management and commercial exploitation of the University's land holdings and buildings

Whilst all risks require appropriate management, risks that may:

- compromise the health and safety of staff, students and visitors; and/or
- compromise the University, its staff and students through inadvertent legislative breaches and consequent penalty; and/or
- compromise national security; and/or
- result in sustained damage to the organisation's reputation;

will require very thorough evaluation, receive additional management scrutiny and be mitigated as far as reasonably possible.

JCU's Risk Appetite Statement is a quantitative and qualitative statement reviewed annually by the Executive and Council, with key risk indicators reported on quarterly and annual bases.

## **2.5 Risk identification**

Risk identification is the process of identifying risks facing JCU. This involves thinking through the sources of risks, the potential hazards, the possible causes and the potential exposure.

The aim of this step is to generate a comprehensive list of risks based on those events that

might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity.

Risk identification occurs within the following categories of risk that are aligned with the Appetite Statement:

- Strategic risks;
- Sustainability risks;
- Financial risks;
- Reputational risks;
- Legal and Regulatory (Compliance) risks;
- Work Health and Safety risks;
- Business disruption risks;
- People risks;
- Technology risks; and
- Academic (Education and Research) risks

The key questions when identifying risks are what, where, when, why and how can it happen, what is the impact and who is responsible for managing the risk?

The University can use a range of techniques for identifying uncertainties that may affect one or more objectives. The following factors, and the relationship between these factors, should be considered:

- tangible and intangible sources of risk
- causes and events
- threats and opportunities
- vulnerabilities and capabilities
- changes in the external and internal context
- indicators of emerging risks
- the nature and value of assets and resources
- consequences and their impact on objectives
- limitations of knowledge and reliability of information
- time-related factors.

## **2.6 Risk Analysis**

Once risks have been identified, they are then analysed. Risk analysis involves consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. Risk analysis should consider factors such as:

- the likelihood of events and consequences;
- the nature and magnitude of consequences;
- complexity and connectivity;
- time-related factors and volatility;
- the effectiveness of existing controls;
- sensitivity and confidence levels.

JCU's likelihood and consequence tables are shown at Appendix A and Appendix B.

## **2.7 Risk Evaluation**

Risk evaluation involves comparing the level of risk found during the analysis process with the established risk appetite to determine where additional action is required.

This can lead to a decision to:

- do nothing further and maintain existing controls (accept the risk);
- consider risk treatment options (mitigate the risk);
- undertake further analysis to better understand the risk and whether the risk can be

- transferred to another party or insurance (transfer the risk)
- reconsider objectives or not proceed with the activity (avoid the risk).

At JCU, for the various levels of risk, the following treatment strategies are required:

- High:** Requires immediate action as it has the potential to be damaging to the organisation.
- Medium:** Requires treatment with routine or specific procedures.
- Low:** Continue to monitor and re-evaluate the risk, ideally treat with routine procedures.

Decisions should take account of the wider context and the actual and perceived consequences to external and internal stakeholders. The output of the risk evaluation is a prioritised list of risks for further action. This is achieved through application of a numbered scale within the 3-tier risk matrix for each risk level (refer Appendix C – Table 5b).

If any further treatment required to reduce risks to an acceptable level will take some time to implement, the risk should generally be avoided until such time as the required treatment is in place. Where this is not practical, a conscious and informed decision needs to be made and recorded as to whether alternative short term treatments may be appropriate or whether the risk should still be accepted in its pre-treatment form (refer Table 1, Section 3.4)

## 2.8 Risk Treatment

Risk treatment involves selecting one or more options for avoiding, transfer or mitigate risks, removing the source, changing likelihood or consequence and implementing those options. It involves identifying and evaluating existing controls and management systems to determine if further action (risk treatment) is required. Existing controls are identified and then assessed as to their level of effectiveness. The selection of risk treatment options should be made in accordance with the University's objectives, risk criteria or appetite, and available resources.

JCU will utilise the control effectiveness ratings shown in Appendix D.

**Current risk** is the level of risk after considering existing controls. It is determined by applying the effectiveness of existing controls to inherent risk. The Risk Matrix tables in Appendix C-Table 5a Risk Level Ratings (see above) should also be used to determine the level of current risk.

Where controls either do not exist, or are considered ineffective to manage the risk down to risk appetite, risk treatment will be required. The level of risk remaining after risk treatment is the **residual risk**.

A Risk Treatment Plan should be developed for complex and significant risk items shown on the Risk Register (generally 'High' risk rating). The information provided in treatment plans should include:

- the reasons for selection of treatment options, including expected benefits to be gained;
- those who are accountable for approving the plan and those responsible for implementing the plan;
- proposed actions;
- resource requirements including contingencies;
- performance measures and constraints;
- reporting and monitoring requirements; and
- timing and schedule.

The treatment plans adopted will be documented and their implementation tracked through Riskware as part of the reporting process.



## 2.9 Monitoring and Review

Few risks remain static. Risks will be continuously monitored and reviewed; and the effectiveness of the controls in place and of the risk treatment plans will be assessed to ensure changing circumstances do not alter risk priorities. Feedback on the implementation and the effectiveness of the Risk Management Policy and Plan will be obtained from the risk reporting process, internal audits and other available information.

At minimum, the risk register will be reviewed every six months to the Vice Chancellor's Advisory Committee and to Audit, Risk and Compliance Committee of Council.

Key Risk Indicators (KRIs) have been developed within the Risk Appetite Statement and will be reported on a quarterly or annual basis as relevant to these Committees. Key Risk Indicators are designed to be predictive in nature and identify changes in emerging risks. They are linked to risk factors that may impact on the achievement of a particular strategy. Figure 2 below highlights how KRIs are linked back to organisational objectives, noting the terminology below is not necessarily reflective of the university sector.

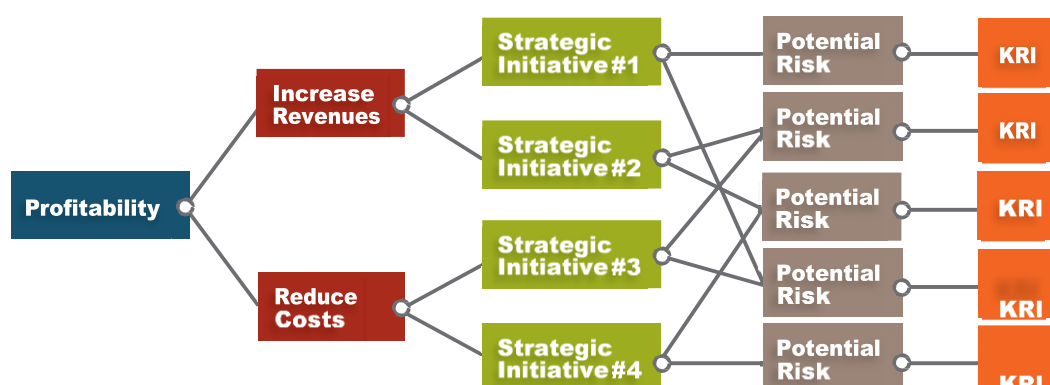


Figure 2: Linking Key Risk Indicators

From: Beasley, M. Branson, B. Hancock, B. "How Key Risk Indicators can Sharpen Focus on Emerging Risks", COSO Developing Key Risk Indicators to Strengthen Enterprise Risk Management, December 2010, 2

## 2.10 Recording and Reporting

Important risk management processes and activities throughout JCU will be recorded. Riskware ERM, JCU's web-based risk management software, will be used to record and update the enterprise risk registers for University and Divisional level as well as Work Health and Safety risk registers. Recording is important for the following reasons:

- it gives integrity to the process and is an important part of good corporate governance;
- it provides an audit trail and evidence of a structured approach to risk identification and analysis;
- it provides a record of decisions made which can be used and reviewed in the future; and
- it provides a record of risk profiles for JCU to continuously monitor.

Key records include:

- **Risk Management Policy** – Establishes commitment and provides a high level overview of risk management framework;
- **Risk Management Framework and Plan** – Details the risk management framework processes and activities;
- **Risk Register** – the key risks and controls for JCU's activities and processes will be recorded on Riskware ERM.
- **Risk Treatment Plans** – strategies to treat risk levels higher than acceptable risk attitude will be recorded on Riskware ERM.

Risk documentation including risk profiles, risk registers, written/formal risk assessments, risk/control audits, self-assessments will be maintained in JCU's official record keeping system. These records may be called upon in the management of ongoing treatments, as evidence in incident investigations, in dealing with insurance matters or during other inquiries, and for audit purposes.

Risk management records should be reviewed:

- On handover of responsibilities between managers
- On assuming responsibility for a project or program
- Regularly to match reporting requirements, and
- Whenever operating parameters are subject to major change.

### **3. RISK MANAGEMENT PLAN**

#### **3.1 Risk Management Responsibilities**

##### ***Council***

Council is ultimately responsible for approving, and committing to, the risk management policy and setting and articulating the University's appetite for risk. Responsibilities specific to the risk management framework include:

- a. reviewing and approving the Risk Management Policy;
- b. establishing and articulating the University's risk appetite statement;
- c. providing feedback to management on important risk management matters/issues raised by management;
- d. supporting management in communicating the importance and benefits of good risk management to stakeholders;
- e. fully considering risk management issues contained in Council reports.; and
- f. identifying and monitoring emerging University risks.

##### ***Audit, Risk and Compliance Committee***

The Audit, Risk and Compliance Committee is responsible for approving and reviewing the University's Risk Management Framework and Plan and overseeing the risk management process of the University as a whole in accordance with the Committee's Charter, and recommends to Council an appropriate risk appetite or level of exposure for the University. The Audit, Risk and Compliance Committee is also responsible for reviewing and making recommendations to Council regarding the Risk Management Policy.

##### ***Other Council Committees***

Other Council Committees have responsibility for risk management relating to their governance area of responsibility (such as Work Health and Safety Committee and Finance and Infrastructure Committee).

##### ***Vice Chancellor***

The Vice Chancellor is responsible for leading the development of an enterprise risk management culture across the University through promoting and supporting the Risk Management Policy and Framework.

##### ***University Executive***

Members of the University Executive are responsible for ensuring that appropriate resources, systems and processes are in place to implement the Risk Management Framework across the organisation and that key University Level risks have been identified and are being managed appropriately. In particular University Executive will:

- a. Monitor the enterprise risk management process periodically by reviewing the University Level Risk Assessment;
- b. Examine the corporate risk profile and review of the operational risk management process results – based upon the risk information reported by the Divisions;

- c. Ensure all risks are being recorded in the enterprise risk register and that these risks are regularly reviewed;
- d. Implement enterprise risk management action plans; and
- e. Report to Council through the Vice-Chancellor.

### ***Chief of Staff (Risk Management Co-ordinator)***

The Risk Management Coordinator is responsible for ensuring that the Risk Management Framework and Policy are being effectively implemented across the organisation. Specific responsibilities include:

- a. Ensuring that the Risk Management Framework is reviewed in accordance with the policy review cycle and/or any change to the AS/NZS ISO 31000:2018 standard;
- b. Ensuring that the Risk Management Framework within JCU is assessed/audited by an independent third party every four years;
- c. Contributing to the risk management process and monitoring the management of the risk treatments for corporate risks;
- d. Submission of reports to the University Executive and Audit, Risk and Compliance Committee on the effectiveness of risk management activities;
- e. Provision of risk management advice to Risk Champions and where necessary, management and staff at all levels;
- f. Assisting with the facilitation of risk identification workshops when requested;
- g. Coordinating and facilitating enterprise risk management training across the University where appropriate;
- h. Assessing whether the processes for the identification and analysis of risks are being followed by Divisions (with assistance from Risk Champions)
- i. Compiling risk management reports and information for University Executive and Audit, Risk and Compliance Committee; and
- j. Monitoring the quality of the risk information.

### ***Risk and Compliance Officer***

The Risk and Compliance Officer supports the Chief of Staff in promoting and developing staff capability in risk assessment and management, and assists risk champions and staff with risk responsibilities within the Divisions. The Risk and Compliance Officer also oversees the requirements of the University's Compliance Framework, understanding legislative obligations relevant to the Higher Education Sector and the activities specific to JCU.

### ***Manager Internal Audit***

The Manager Internal Audit develops and implements the University's Internal Audit Strategy and risk based Internal Audit Annual Work Plan under the oversight of the Audit, Risk and Compliance Committee of Council and in consultation with Senior Management particularly the Chief of Staff; by assessing key business risks, identifying assurance gaps and emerging needs, and providing advice on how these might be addressed within the overall University assurance framework and the independent Internal Audit budget allocation.

### ***All Managers and Staff (Risk Owners)***

Managers and staff at all levels may be risk owners and are responsible for developing an understanding of and becoming competent in the implementation of risk management principles and practices in their work areas. Specific responsibilities include:

- a. establishing clear objectives and identifying and evaluating the significant risks that may influence the achievement of those objectives;
- b. designing, resourcing, operating and monitoring internal control systems;
- c. ensuring that a risk based approach to internal control is communicated to staff and embedded in operational processes;
- d. assessing and managing the risk of fraud and corruption, in line with the *Staff Code of Conduct* and the *Financial Management Practice Manual*;
- e. assigning accountability for managing risks within agreed boundaries; and
- f. providing an annual assurance to the University Executive regarding the extent of

compliance with the Risk Management Policy.

### ***Risk Champions***

Risk champions within each Division are responsible for coordination of risk management activities within that Division. Specific responsibilities include:

- a. provision of risk management advice to managers and staff within the relevant division when required;
- b. assisting with the facilitation of risk identification workshops when requested;
- c. coordinating the analysis and evaluation of identified risks in conjunction with the managers within the relevant division;
- d. ensuring that the processes for the identification and analysis of risks are being followed within their functional area;
- e. providing assistance to managers in the implementation of identified risk treatments; and
- f. ensuring that identified risks are documented in the Division risk register..

### **3.2 Risk Management Framework Review**

Documentation including policies, procedures, risk registers and systems relating to the risk management framework will be subject to periodic review.. The results of any review of the Risk Management Policy or Framework and Plan are to be reported to the University Executive, the Audit, Risk and Compliance Committee and ultimately the Council. n.

### **3.3 Risk Register Establishment and Review**

One of the key principles underpinning effective risk management is that it should be integrated into normal organisational processes especially those that set the objectives and strategies of the organisation. As the University has an established business planning process it is critical that risk management is integrated into the normal business planning cycle.

The risk management process described above will be applied at four levels within the University - these being University, Division, Project and Activity.

#### ***University Level***

As part of the University's annual business planning cycle, University Executive will conduct a University level risk assessment to identify, review and/or update key strategic risks facing the organisation that may impact on the University's ability to achieve its strategic intent. The outcomes of this assessment will be recorded in the University enterprise risk register and will be reported to the Audit, Risk and Compliance Committee and to the Council. Progress in implementing risk treatment plans emanating from the University Level Risk Assessment will be monitored on a regular basis by University Executive.

#### ***Division Level***

Each Division is required to identify and analyse key risks that may impact on achieving objectives specific to that Division. The outcome of this assessment will be recorded in a Divisional risk register.

#### ***Project Level***

All submissions regarding new projects or initiatives must be accompanied by a full risk assessment commensurate with the scale of the project or initiative. The risk assessment must be completed by the relevant Division using the process detailed above and must be recorded in an enterprise project risk register. The register is to be overseen by the Risk Management Champion.

#### ***Activity Level***

All Managers within the University are responsible for ensuring that risks arising from

the activities under their control have been properly assessed and are being adequately treated. To this end, the Risk Champions, in conjunction with relevant Managers and the University's Risk and Compliance Officer, shall develop an annual program of activity based risk assessments appropriate to the size, scale and risk profile of the department in question. The outcome of these risk assessments is to be recorded in an activity level risk register which is to be kept under ongoing review by the relevant Manager or Risk Owner.

### 3.4 Risk Management Plan Progress Reports

The Risk Management Coordinator is to coordinate the preparation of quarterly reports to University Executive and to the Audit, Risk and Compliance Committee regarding progress in implementing the Risk Management Plan. These reports will at least contain details of:

- any risk management initiatives undertaken during the previous quarter
- any major incidents that have occurred during the previous quarter
- heat maps showing the distribution of risks across the risk evaluation matrix
- the high residual risks facing the organisation and the controls in place to manage those risks (as per the table below)
- progress in implementing key risk treatment plans
- any other matters that may be of relevance to the Committee.

The following table identifies the communication, recording and control requirements for each risk rating.

*Table 1: Risk Notification and Control Table*

Risk Rating	Authority to Accept Risk	Notification/communication Requirements	Formal recording / reporting	Inherent risk review and control requirements
High	University Executive (through Risk Champions)	Council through Audit, Risk and Compliance Committee	Mandatory to Risk Register	Reviewed quarterly – controls implemented to <b>reduce risk to medium or below</b> within 12 months with defined treatment
Medium	Dean/Directors/Head of Academic Group or Manager	Divisional Risk Champion	Mandatory to Risk Register	Reviewed 6 monthly – include consideration of this risk in strategic and operational planning; controls to be identified and actions to reduce risk actively pursued
Low	Staff member one level removed from risk assessment	Nil	Included in Risk Register	Nil

### 3.5 Training

Risk owners and other key staff may require periodic training in how to implement the risk management process and their responsibilities and obligations under JCU's Risk Management Policy and Plan. General risk management training should be provided to all risk owners and other relevant staff every four years.

In addition, all new staff should be advised of JCU's commitment to risk management and their responsibilities and obligations when they commence working for JCU. This should generally be done through a short introduction at JCU's online induction session followed by a more detailed training session for risk owners within three months of commencing employment. The training may be delivered internally or externally or by a combination of the two. The Risk and Compliance Officer is responsible for coordinating and recording the provision of such training.

### 3.6 Summary of Key Risk Management Plan Activities

Table 2 summarises the key actions, reviews and reports required by JCU's Risk Management Plan. It details who is responsible for each activity and the required timing.

*Table 2: Summary of Key Activities*

Action	Description	Responsibility	Timing
Review RM Policy	Review the currency and effectiveness of JCU's Risk Management Policy	Council to approve on advice of University Executive and Audit, Risk and Compliance Committee (review to be coordinated by Chief of Staff)	Every five years
Review RM Framework and Plan	Review the currency and effectiveness of JCU's Risk Management Framework and Plan	Audit, Risk and Compliance Committee to approve on advice of University Executive (coordinated by Chief of Staff)	Every five years
University Risk Register	Review risks and controls contained in the University risk register and identify new or emerging risks	University Executive to initiate, Audit, Risk and Compliance Committee to review (coordinated by Chief of Staff)	Every six months
Division Risk Register	Review risks and controls contained in each register and identify new or emerging risks	All DVCs (Risk Champions to coordinate)	Every six months
Project Risk Register	Conduct risk assessments for all new projects and initiatives	Risk Owners (Risk Champions to assist)	Prior to deciding to proceed with new project/initiative
Activity Risk Registers	Conduct risk assessments for key activities and processes	Risk Owners (Risk Champions to assist)	As per annual plan to be developed within each Division where required
Risk Management Plan Progress Report	Review current status of key risks, Risk Treatment Plans, incidents and other relevant issues	University Executive and Audit, Risk and Compliance Committee (coordinated by Chief of Staff)	University Executive and Audit, Risk and Compliance Committee – quarterly
Training	Ensure risk owners and other staff are aware of the risk management process and their obligations.	Risk Management Coordinator (Risk Champions to assist)	Refresher for all Managers and Risk Champions as required. Introduction for all new staff at on-line induction with more detailed session for risk owners within three months of commencing.

## Administration

NOTE: Printed copies of this framework are uncontrolled, and currency can only be assured at the time of printing.

### Approval Details

Policy Domain	Corporate Governance
Policy Sub-domain	Risk, Assurance, Regulatory and Compliance
Policy Custodian	Vice Chancellor
Approval Authority	Council
Date for next Major Review	07/12/2028

### Revision History

Version no.	Approval date	Approved by	Implementation date	Details	Author
24-1	01/08/2024	Council	08/08/2024	Annual review – updated and clarified document as required.	Chief of Staff
23-1	07/12/2023	Council	14/12/2023	Major review.	Chief of Staff
20-1	30/07/2020	Council	03/09/2020	Annual review – updated and clarified document as required. No significant, material amendments	Chief of Staff
19-1	08/08/2017	Council	16/08/2019	Annual review – no amendments.	Chief of Staff
18-1	07/09/2018	Council	29/10/2018	Annual review - minor changes to policy, framework and plan as part of updating process and to reflect changes in position titles, changes to committees and grammatical corrections.	Chief of Staff
17-1	07/09/2017	Council	27/09/2017	Annual review.	Chief of Staff
16-1	01/09/2016	Council	06/10/2016		Chief of Staff

Keywords	Risk, risk assessment, risk analysis, risk appetite, consequence, likelihood
Contact person	Chief of Staff

## Appendix A – Likelihood Ratings

*Table 3: Likelihood Ratings*

Rating	Likelihood	Description	Quantification
1	Rare	The event may occur but only in exceptional circumstances and/or no past event history.	May occur within every 10-year period or more.
2	Unlikely	The event could occur in some circumstances. No past event history.	Could occur within a 5-to-10-year period.
3	Possible	The event may occur sometime. Some past warning signs or previous event history.	Could occur within a 1-to-5-year period.
4	Likely	The event will probably occur. Some recurring past event history.	Could occur within a 3-to-12-month period.
5	Almost Certain	The event is expected to occur in normal circumstances. There has been frequent past history.	Likely to occur within a 3-month period or during the performance of an actual task.



## Appendix B – Consequence Ratings

Table 4: Consequence ratings

Category	Risk Area and Impact									
	Strategic	Sustainability	Reputation	Legal and Regulatory (Compliance)	Work Health & Safety	Business Disruption	People	Technology	Academic (Education and Research)	Financial
5. Catastrophic	Most University objectives can no longer be achieved.  Complete revision of long term business model required.  Severe and sustained damage to mission and vision.  Complete failure to achieve critical strategic goals.  Loss of operational viability.  Total loss of stakeholder confidence.	Long term environmental damage (5 years or longer), requiring more than \$1M to remedy.  Breaches results in prosecution by DEHP.  Multiple Human Rights claims.  Serious breaches of the Voluntary Code of Best Practice for the Governance of AS Public Universities.  Serious ethical breaches with the potential for litigation, consistent failure to comply with regulatory mandatory reporting requirements.	Severe Negative Publicity: Sustained negative national and international media coverage causing significant loss of funding, staff, and students.  Long-term Trust Damage: Major incidents leading to a long-term loss of trust among key stakeholders including students, staff, partners, and the public.  Reputational Damage: Catastrophic impact on university rankings and reputation, resulting in severe competitive disadvantage.  High-profile Scandals: Involvement in high-profile scandals with severe legal, financial, and reputational repercussions.  Community and Stakeholder Backlash: Significant backlash from the community and stakeholders leading to prolonged reputational harm and operational challenges.	Severe Legal Breaches: Repeated and severe breaches of significant contractual or regulatory requirements leading to class actions or serious prosecutions.  Statutory Intervention: Significant statutory intervention due to serious breaches of legislation, resulting in major legal and operational repercussions.  Loss of Accreditation: Loss of accreditation for multiple courses, significantly affecting the university's reputation and operational capabilities.  Regulatory Sanctions: Severe sanctions from regulatory bodies, including large fines exceeding \$500,000 and restrictions on university operations.  Ethical Breaches: Serious ethical breaches with potential for litigation, significant loss of trust, harm, and long-term reputational damage.	Fatalities: Multiple fatalities as a result of a significant safety incident.  Severe Injuries: Multiple instances of permanent disability or life-altering injuries.  Regulatory Action: Prosecution with penalties exceeding \$500,000, resulting in severe legal and financial repercussions.  Operational Impact: Complete shutdown of a significant portion of university operations for an extended period due to a WHS incident.  Long-term Health Effects: Incident causing long-term health effects and/or psychological harm for a significant number of staff or students.	Complete shutdown of both physical and digital infrastructure for more than two weeks, rendering the university unable to conduct critical operations or deliver educational services.  inability to deliver teaching for more than 2 days.  Critical loss or impact to JCU research compromising standings affecting top 2% achievement in Academic Ranking of World Universities.	Key personnel loss: Loss of multiple key personnel or high-profile researchers leading to severe damage to university reputation and operational capacity.  Recruitment Challenges: Inability to recruit for business/academic critical roles for over 24 months, resulting in significant operational and reputational damage.  High Turnover: Systemic high turnover leading to an inability to deliver critical functions, loss of institutional knowledge and significant reputational damage.  Industrial Action: Prolonged university-wide industrial action causing major disruptions to operations and severe reputational damage.  Grievance Handling: Systemic failure to handle grievances, leading to multiple adverse rulings by Fair Work Commission and major financial and reputational impacts.  Payroll compliance: Non-payment or under-payment of staff leading to breach of employer-employee trust, risk of regulatory penalties and significant reputational damage.	Loss of Availability: Critical IT systems unavailable for more than 10 days, resulting in a severe impact on university operations and inability to deliver key services.  Loss of Integrity: Critical IT systems experience irretrievable loss of data, significantly impairing university functions and causing extensive operational and reputational damage.  Loss of Confidentiality: Large-scale release of sensitive and personal information, leading to significant harm to stakeholders and severe legal and regulatory consequences.  Cybersecurity Threats: Highly motivated and capable threat actors successfully breach systems, causing major disruptions and substantial financial loss.	Loss of accreditation of a flagship course or multiple courses severely impacting the university's reputation and ability to operate.  Institutionalised and/or systemic fraud or misconduct in academic activities including enrolments and examination processes.  Loss of flagship research projects that significantly affect the university's standing in global research rankings, or irretrievable loss of critical research data or long-term disruptions to major research initiatives.	Revenue Loss: More than 10% recurrent reduction in operating fund revenue, or a one-off loss exceeding \$50m.  Cash Flow Crisis: Cash balance falls below 5-week forecast leading to a severe liquidity crisis.  Fraud or Misconduct: Large-scale financial fraud or misconduct causing significant financial loss and reputational damage.  Sustainability Impact: Severe impact on the financial sustainability of the university, requiring major restructuring or external intervention.  Investment Loss: Loss of major investments causing long-term financial instability and inability to fund critical initiatives.
4. Major	A number of significant University objectives can no longer be achieved.  Major damage to mission and vision.  Major failure to achieve important strategic goals.  Significant operational disruptions.  Major loss of stakeholder confidence.	Medium-term (1-5 years) environmental damage, requiring more than \$500k to \$1M to study and/or remedy;  Breaches result in an Enforceable Undertaking by DEHP.  Sustained reputational damage as a result of significant loss of confidence in governance and management oversight of university activities.  Failure to comply with regulatory mandatory reporting requirements.	Significant Negative Publicity: Extended negative media coverage resulting in a notable loss of funding, staff, and students.  Loss of Stakeholder Confidence: Significant incidents causing a major loss of confidence among key stakeholders.  Reputational Damage: Major impact on university rankings and reputation, affecting competitiveness and attractiveness.  Ethical Violations: Involvement in significant ethical violations causing major reputational damage.  Community and Stakeholder Concerns: Serious concerns raised by the community and stakeholders leading to substantial reputational impact.	Legal Breaches: One-off serious legal breaches or adverse findings leading to major legal and financial consequences.  Regulatory Non-compliance: Significant non-compliance with regulatory requirements resulting in enforceable undertakings or substantial penalties between \$200,000 and \$500,000.  Accreditation Challenges: Risk of losing accreditation for key courses or programs, impacting the university's reputation and student enrolment.  Regulatory Sanctions: Significant sanctions from regulatory bodies affecting university operations and leading to reputational damage.  Ethical Issues: Major ethical issues requiring substantial management resources to address, causing harm or reputational damage.	Fatalities: Single fatality or multiple serious injuries resulting in permanent disability.  Severe Injuries: Serious injury requiring extensive medical treatment and rehabilitation.  Regulatory Action: Prosecution with penalties between \$200,000 and \$500,000.  Operational Impact: Partial shutdown of university operations for a significant period due to a WHS incident.  Health Effects: Incident causing long-term health effects and/or psychological harm for several staff or students..	Unavailability of critical infrastructure including utilities between 1 and 2 weeks severely affecting university operations and student services.  Inability to deliver teaching for 24-48 hours.  Research productivity impact 8+ weeks impacting JCU research standing.	Key Personnel Loss: Loss of key personnel or researchers causing noticeable but manageable operational impacts.  Recruitment Challenges: Difficulty recruiting for business/academic critical roles for 6-12 months, impacting short-term performance.  Turnover Rates: Higher-than-desired turnover rates in multiple disciplines, causing operational challenges.  Industrial Action: Localized industrial action causing moderate operational disruptions.  Grievance Handling: Performance management issues requiring significant HR intervention, with minor financial and reputational impacts.  Payroll Compliance: Significant payroll errors resulting in partial under-payment of staff for an extended period, leading to substantial employee dissatisfaction, potential legal action, and moderate reputational damage. This could also include the discovery of systemic payroll issues that require major corrective actions and result in regulatory scrutiny and penalties.	Loss of Availability: Critical IT systems unavailable for 24-48 hours during business days, causing major operational disruptions and delays in key university processes.  Loss of Integrity: Significant data integrity issues that disrupt operations and lead to major challenges in research and academic activities.  Loss of Confidentiality: Significant breach of sensitive data affecting a substantial number of stakeholders, resulting in considerable reputational damage and legal repercussions.  Cybersecurity: Motivated threat actors breach systems, resulting in significant operational and financial impacts.	Loss of mandatory accreditation of single course affecting student enrolment and university reputation.  Localised fraud or misconduct in academic activities including enrolments and examination processes.  Loss of multiple significant research projects or research data making a major negative impact on the university's research standings, affecting its competitive position.	Revenue Loss: Between 5% and 10% recurrent reduction in operating fund revenue or a one off loss of between \$20m and \$50m.  Cash Flow Issues: Cash balance falls below 10-week safety margin causing substantial liquidity concerns.  Fraud or Misconduct: Significant financial fraud or misconduct resulting in major financial loss and reputational damage.  Sustainability Impact: Major impact on financial sustainability, necessitating significant adjustments to budgets and operations.  Investment Loss: Significant loss of investments affecting the university's ability to fund important projects and initiatives.

3. Moderate	<p>Some important University objectives can no longer be achieved.</p> <p>Noticeable damage to mission and vision.</p> <p>Moderate failure to achieve some strategic goals.</p> <p>Moderate operational disruptions.</p> <p>Moderate loss of stakeholder confidence.</p>	<p>Short-term (less than 1 year) environmental damage, requiring more than \$150k to \$500k to study and/or remedy.</p> <p>Administrative action taken by Environmental Regulator.</p> <p>Allegations of mismanagement and lack of governance oversight on university activities; breaches in conduct at the senior management or governance level. Warning/notice letter from Regulator on governance practices.</p>	<p>Negative Publicity: One-off negative media coverage requiring substantial management resources to address.</p> <p>Stakeholder Trust Issues: Incidents causing moderate loss of trust among stakeholders.</p> <p>Reputational Impact: Moderate impact on university rankings and reputation, requiring corrective actions.</p> <p>Ethical Issues: Noticeable ethical issues causing reputational concerns.</p> <p>Community and Stakeholder Feedback: Moderate concerns raised by the community and stakeholders, impacting reputation.</p>	<p>Legal Breaches: Repeated breaches of university policy requiring legal or regulatory intervention and penalties between \$50,000 and \$200,000.</p> <p>Regulatory Non-compliance: Moderate non-compliance issues resulting in warning notices or minor penalties.</p> <p>Accreditation Risk: Potential loss of voluntary accreditation for single courses or programs, requiring corrective actions.</p> <p>Regulatory Actions: Moderate actions from regulatory bodies requiring changes to university practices.</p> <p>Ethical Concerns: Noticeable ethical concerns impacting university reputation or harm to individuals and requiring management intervention.</p>	<p>Serious Injuries: Injuries resulting in lost time and requiring significant medical treatment.</p> <p>Regulatory Action: Penalties between \$50,000 and \$200,000, possibly including regulatory intervention.</p> <p>Operational Impact: Temporary disruption to university operations due to a WHS incident.</p> <p>Health Effects: Incident causing moderate health effects and/or psychological harm for a number of staff or students.</p>	<p>Unavailability of critical infrastructure, utilities between 3 &amp; 5 days moderately affecting university operations and student services.:</p> <p>Inability to deliver teaching for 12-24 hours.</p> <p>Loss of raw un-reproducible data.</p> <p>Research productivity impact 2-8 weeks with possible impact to JCU research standings.</p>	<p>Key Personnel Loss: Loss of key personnel or researchers causing noticeable but manageable operational impacts.</p> <p>Recruitment Challenges: Difficulty recruiting for business/academic critical roles for 6-12 months, impacting short-term performance.</p> <p>Turnover Rates: Higher-than-desired turnover rates in multiple disciplines, causing operational challenges.</p> <p>Industrial Action: Localized industrial action causing moderate operational disruptions.</p> <p>Grievance Handling: Performance management issues requiring significant HR intervention, with minor financial and reputational impacts.</p> <p>Payroll Compliance: Frequent payroll errors affecting a moderate number of staff over a noticeable period, leading to employee dissatisfaction and requiring considerable administrative effort to resolve. This may involve repeated corrections and minor regulatory scrutiny with some impact on employee trust and minor reputational damage.</p>	<p>Loss of Availability: Critical IT systems unavailable for 12-24 hours during business days, causing moderate disruptions to operations and delays in service delivery.</p> <p>Loss of Integrity: Moderate data integrity issues that disrupt some operations and impact short-term research activities.</p> <p>Loss of Confidentiality: Breach of sensitive data affecting a moderate number of stakeholders, causing reputational damage and potential legal challenges.</p> <p>Cybersecurity: Threat actors breach systems, causing moderate operational disruptions and financial impacts.</p>	<p>Loss of voluntary accreditation of a course requiring corrective actions to maintain standards.</p> <p>Localised fraud or misconduct in academic activities requiring investigation and remedial actions.</p> <p>Loss of significant research project with a moderate impact on the university's research standings, requiring efforts to regain position.</p>	<p>Revenue Loss: Between 1% and 5% recurrent reduction in operating fund revenue and a one off loss of between \$5m and \$20m.</p> <p>Cash Flow Concerns: Temporary cash flow issues requiring adjustments to financial planning and budgeting.</p> <p>Fraud or Misconduct: Moderate financial fraud or misconduct causing noticeable financial loss and requiring management intervention.</p> <p>Sustainability Impact: Noticeable impact on financial sustainability, requiring moderate budget adjustments and cost-saving measures.</p> <p>Investment Loss: Moderate loss of investments impacting the funding of some projects and initiatives.</p>
	<p>Reprioritisation of resources to enable achievement of key University objectives.</p> <p>Minor impact on mission and vision.</p> <p>Minor failure to achieve a few strategic goals.</p> <p>Minor operational disruptions.</p> <p>Minor loss of stakeholder confidence.</p>	<p>Environmental damage, requiring up to \$150,000 to study and/or remedy.</p> <p>Infringement notice may be issued by Environmental Regulator.</p> <p>Failure to comply with voluntary reporting requirements.</p>	<p>Localized Negative Publicity: One-off negative local media coverage requiring minimal response.</p> <p>Minor Stakeholder Trust Issues: Incidents causing minor loss of trust among some stakeholders.</p> <p>Reputational Impact: Minor impact on university reputation, easily manageable.</p> <p>Ethical Concerns: Minor ethical concerns addressed through standard procedures.</p> <p>Community and Stakeholder Comments: Minor negative feedback from the community and stakeholders with limited impact.</p>	<p>Legal Breaches: Minor breaches of regulations or standards with limited legal consequences.</p> <p>Regulatory Non-compliance: Minor non-compliance issues resulting in warning letters or notices.</p> <p>Accreditation Issues: Minor issues with accreditation requiring minimal corrective actions.</p> <p>Regulatory Notices: Receipt of minor notices from regulatory bodies requiring minimal adjustments.</p> <p>Ethical Issues: Minor ethical issues addressed through standard procedures with limited reputational impact.</p>	<p>Moderate Injuries: Injuries requiring medical treatment but not resulting in significant lost time.</p> <p>Regulatory Action: Penalties up to \$50,000.</p> <p>Operational Impact: Minor disruptions to university operations due to a WHS incident.</p> <p>Health Effects: Incident causing minor health effects or psychological harm for some staff or students.</p>	<p>Unavailability of critical infrastructure including utilities between 1 &amp; 3 days with minimal impact on university operations and student services.:</p> <p>Inability to deliver teaching for 4-12 hours.</p> <p>Loss of research processing data, productivity impact (1-2 weeks).</p>	<p>Key Personnel Loss: Loss of a few key personnel causing minor operational disruptions.</p> <p>Recruitment Challenges: Difficulty recruiting for business/academic critical roles within 3-6 months, causing minor operational impact.</p> <p>Turnover Rates: Higher-than-desired turnover rates in non-critical areas, causing localized operational issues.</p> <p>Industrial Action: Minor industrial action causing minimal operational disruption.</p> <p>Grievance Handling: Minor performance management issues resolved with minimal HR intervention.</p> <p>Payroll Compliance: Minor payroll discrepancies affecting a small number of staff for a short duration, leading to temporary employee dissatisfaction and requiring minor administrative corrections. This could include occasional payroll processing errors that are quickly identified and resolved with minimal impact on employee trust and no regulatory penalties.</p>	<p>Loss of Availability: Critical IT systems unavailable for 4-12 hours during business days, causing minor operational disruptions.</p> <p>Loss of Integrity: Minor data integrity issues with limited operational impact.</p> <p>Loss of Confidentiality: Breach of sensitive data affecting a small number of stakeholders, causing minimal reputational damage.</p> <p>Cybersecurity: Attempted breaches by threat actors with minor operational impacts.</p>	<p>Minor issues with accreditation requiring minimal corrective actions.</p> <p>Minor instances of academic misconduct managed according to normal procedures.</p> <p>Loss of research project with limited effect on overall position or minor loss of research data with limited impact on project outcomes.</p>	<p>Revenue Loss: One off, or recurring loss of between \$1m and \$5m.</p> <p>Cash Flow Impact: Minor cash flow issues managed within existing financial processes.</p> <p>Fraud or Misconduct: Minor financial fraud or misconduct with limited financial loss and minimal reputational impact.</p> <p>Sustainability Impact: Minor impact on financial sustainability, manageable within current budgets.</p> <p>Investment Loss: Minor loss of investments with limited impact on project funding.</p>

1. Insignificant	<p>Little or no impact on University objectives.</p> <p>Negligible impact on mission and vision.</p> <p>Insignificant failure to achieve strategic goals.</p> <p>Negligible operational disruptions.</p> <p>Stable stakeholder confidence.</p>	<p>Negligible environmental impact, managed within operating budgets.</p> <p>Warning notice/letter may be issued by Environmental Regulator.</p> <p>Lack of awareness of social responsibilities, ethics and integrity principles</p>	<p>Neutral Publicity: Occasional media enquiries or neutral press coverage with no significant impact.</p> <p>Stable Stakeholder Trust: No significant loss of trust among stakeholders.</p> <p>Reputational Impact: Negligible impact on university reputation.</p> <p>Ethical Issues: Insignificant ethical issues managed within normal operational processes.</p> <p>Community and Stakeholder Feedback: Routine feedback from the community and stakeholders with no significant impact.</p>	<p>Legal Breaches: Insignificant breaches of standards with no legal consequences.</p> <p>Regulatory Compliance: Full compliance with regulatory requirements, with occasional minor advisory notices.</p> <p>Accreditation: No significant issues with accreditation.</p> <p>Regulatory Impact: Negligible impact from regulatory bodies.</p> <p>Ethical Issues: Insignificant ethical issues managed within normal operational processes.</p>	<p>Minor Injuries: Injuries requiring first aid with no significant lost time.</p> <p>Regulatory Action: No significant penalties, only minor regulatory warnings.</p> <p>Operational Impact: Negligible disruption to university operations due to a WHS incident.</p> <p>Health Effects: Incident causing negligible health effects.</p>	<p>Unavailability of critical infrastructure including utilities for less than 1 day with no significant impact on university operations and student services.</p> <p>Inability to deliver teaching for more than 4 hours.</p> <p>Minor loss of research data with little to no productivity impact.</p>	<p>Key Personnel Loss: Loss of individual key personnel with no significant impact on operations.</p> <p>Recruitment Challenges: Recruitment challenges resolved within 3 months with negligible operational impact.</p> <p>Turnover Rates: Normal turnover rates causing no significant operational issues.</p> <p>Industrial Action: No significant industrial action.</p> <p>Grievance Handling: Routine performance management issues handled within normal processes with negligible impact.</p> <p>Payroll Compliance: Very minor and infrequent payroll errors affecting a very small number of staff, easily resolved with no significant impact on employee satisfaction, trust, or operational processes. These errors are typically identified and corrected in the next payroll cycle with no risk of regulatory penalties or reputational damage.</p>	<p>Loss of Availability: Critical IT systems unavailable for less than four hours during business days, causing negligible operational disruptions.</p> <p>Loss of Integrity: Insignificant data integrity issues with no meaningful impact on operations.</p> <p>Loss of Confidentiality: Insignificant breach of sensitive data with minimal impact.</p> <p>Cybersecurity: Low-level attempts by threat actors with no significant operational impacts.</p>	<p>No significant issues with course accreditation.</p> <p>Insignificant incidents of academic misconduct managed with according to normal procedures.</p> <p>Research projects progress as planned with minor delays.</p>	<p>Revenue Loss: One off, or recurring loss of less than \$1m.</p> <p>Cash Flow Stability: Stable cash flow with no significant issues.</p> <p>Fraud or Misconduct: Negligible financial fraud or misconduct with no meaningful financial or reputational impact.</p> <p>Sustainability Impact: No significant impact on financial sustainability.</p> <p>Investment Loss: Insignificant loss of investments with no impact on funding.</p>
------------------	--	---	---	---	--	--	--	---	--	---

## Appendix C – Risk Rating Matrix

Table 5a: Risk Level Ratings

Consequence	Likelihood				
	Rare (E)	Unlikely (D)	Possible (C)	Likely (B)	Almost Certain (A)
<b>5 Catastrophic</b>	Medium	High	High	High	High
<b>4 Major</b>	Medium	Medium	High	High	High
<b>3 Moderate</b>	Low	Medium	Medium	High	High
<b>2 Minor</b>	Low	Low	Medium	Medium	Medium
<b>1 Insignificant</b>	Low	Low	Low	Low	Medium

Table 5b: Risk Evaluation

Consequence	Likelihood				
	Rare (E)	Unlikely (D)	Possible (C)	Likely (B)	Almost Certain (A)
<b>5 Catastrophic</b>	15	19	22	24	25
<b>4 Major</b>	10	14	18	21	23
<b>3 Moderate</b>	6	9	13	17	20
<b>2 Minor</b>	3	5	8	12	16
<b>1 Insignificant</b>	1	2	4	7	11

## Appendix D – Control Effectiveness Ratings

*Table 6: Control Effectiveness Ratings*

Rating	Effectiveness	Description
1	Not Effective	Control(s) does not address risk or no controls identified or controls identified and address risk, but not implemented.
2	Somewhat Effective	Control(s) exists, but not very effective as control design can be improved, better communicated and implemented.
3	Reasonably Effective	Control(s) mostly reliable and effective. Documentation exists but can be better communicated, testing and monitoring of controls needs to be improved
4	Highly Effective	Control(s) fully verified and tested as reliable and effective. Fully documented process and well communicated

## Appendix E – Risk Management Glossary

*Adapted from AS/NZS ISO 31000:2018*

<b>communication and consultation</b>	continual and iterative processes that an organisation conducts to provide, share or obtain information and to engage in dialogue with stakeholders and others regarding the management of risk stakeholder person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity
<b>consequence</b>	outcome of an event affecting objectives
<b>control</b>	measure that maintains and/or modifies risk
<b>establishing the context</b>	defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy
<b>external context</b>	external environment in which the organisation seeks to achieve its objectives
<b>internal context</b>	internal environment in which the organisation seeks to achieve its objectives
<b>level of risk</b>	magnitude of a risk, expressed in terms of the combination of consequences and their likelihood
<b>likelihood</b>	chance of something happening
<b>monitoring</b>	continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected
<b>residual risk</b>	risk remaining after risk treatment
<b>review</b>	activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives
<b>risk</b>	effect of uncertainty on objectives
<b>risk analysis</b>	process to comprehend the nature of risk and to determine the level of risk
<b>risk appetite</b>	the amount and type of risk an organisation is prepared to accept in the pursuit of its organisational objectives
<b>risk assessment</b>	overall process of risk identification, risk analysis and risk evaluation

<b>risk criteria</b>	terms of reference against which the significance of a risk is evaluated
<b>risk evaluation</b>	process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable
<b>risk identification</b>	process of finding, recognizing and describing risks
<b>risk limit</b>	threshold to monitor that actual risk exposure does not deviate too much from the desired optimum; breaching risk limits will typically act as a trigger for corrective action at the process level
<b>risk management</b>	coordinated activities to direct and control an organisation with regard to risk
<b>risk management framework</b>	set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation
<b>risk management plan</b>	scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk
<b>risk management policy</b>	statement of the overall intentions and direction of an organisation related to risk management
<b>risk management process</b>	systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk
<b>risk owner</b>	person or entity with the accountability and authority to manage the risk
<b>risk profile</b>	description of any set of risks
<b>risk source</b>	element which alone or in combination has the intrinsic potential to give rise to risk event
<b>risk tolerance</b>	the specific maximum risk that an organisation is willing to take regarding each relevant risk (sub-) category, often in quantitative terms
<b>risk treatment</b>	process to modify risk