





## 1. RISK

provide information to support University decision making  
provide a basis for effective resource allocation  
help the University meet compliance 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 of, and not separate from, the organizational purpose, governance, leadership and commitment, strategy, objectives and operations.

The 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 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

the depth

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





## **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



- c. Ensure all risks are being recorded in the enterprise risk register and that these risks are



### **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 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 six monthly 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 i 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*

<b>Risk Rating</b>	<b>Authority to Accept Risk</b>	<b>Notification/ communication Requirements</b>	<b>Formal recording / reporting</b>	<b>Inherent risk review and control requirements</b>
<b>High</b>	University Executive (through Risk Champions)	Council through Audit, Risk and Compliance Committee	Mandatory to Risk Register and Triennium Planning	Reviewed 6 monthly controls implemented to <b>reduce risk to medium or below</b> within 12 months with defined treatment plans
<b>Medium</b>	Dean/Directors/Head of Academic Group or Manager	Divisional Risk		

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 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 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 in August
Review RM Framework and Plan	Review the currency and effectiveness of 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 in August
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 Planning Package and identify new or emerging risks	Provost and all DVCs (Risk Champions to coordinate)	Every six months
Project Risk Register	Conduct risk assessments for all new projects and initiatives	Risk Owners	

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.
----------	--	--	---

## 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.	





4. Major	Between 5 & 10% recurrent reduction in operating fund revenue, one off loss of between \$20m & \$50m, Cash balance falls below 10 week safety margin	Loss of mandatory accreditation of single course, localised fraud or misconduct in academic activities including enrolments and examination processes, loss of multiple significant research projects	Significant negative publicity that could result in some loss of funding, staff and/or students	Unavailability of critical infrastructure, utilities between 1 and 2 weeks; Unavailability of ICT services during business day for 24-48 hours and major impact to critical business cycle; inability to deliver teaching for 24-48 hours; research productivity impact 8+ weeks; impact on JCU research standings	Recruitment to a business/academic critical role 12-24months, potentially impacting research rankings or loss of academic accreditations; Single high profile performance management case resulting in Fair Work Commission ruling against the University resulting in minor financial impact and causing reputational damage; Higher than desired staff turnover across a Division impacting performance; Morale issues impacting operational performance across some Divisions; Industrial action at Divisional level	One off serious successful prosecution or adverse findings, breach of significant contractual arrangement, statutory intervention due to breach of legislation; breach of university policy treated as misconduct resulting in formal action/investigation	Permanent disability; prosecution and penalty/fine between >\$200-500k; Smartraveller Alert Level 3 or combination of 3 and 4;	A number of significant University objectives can no longer be achieved	Medium-term (1-5 years) environmental damage, requiring >\$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.
3. Moderate	Between 1 & 5% recurrent reduction in operating fund								

2. Minor

One off, or recurring loss of between \$1m & \$5m

One off instances of minor misconduct dealt with according to normal procedures, loss of research project

One off negative local publicity that requires a minimal response from the University

Unavailability of critical infrastructure, utilities between 1 & 3 days; unavailability of ICT services during business day for 4-12

## Appendix C – Risk Rating Matrix

Table 5a: Risk Level Ratings

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

Table 5b: Risk Evaluation

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

## Appendix D – Control Effectiveness Ratings

*Table 6: Control Effectiveness Ratings*

**Rating   Effectiveness**

## Appendix E – Risk Management Glossary

*Adapted from AS/NZS ISO 31000:2018*

**communication and consultation** 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>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