



JCU Risk Management Framework and Plan

Document Contact: Chief of Staff

Approved by Council (5/18) 07 September 2018

| | |
|---|----|
| 1. RISK MANAGEMENT FRAMEWORK..... | 3 |
| 1.1 General..... | 3 |
| 1.2 What is Risk?..... | 3 |
| 1.3 Why Should We Manage Risk?..... | 3 |
| 1.4 Objectives..... | 4 |
| 1.5 Risk Management Policy..... | 4 |
| 1.6 Risk Management Plan..... | 4 |
| 2. RISK MANAGEMENT PROCESS | 5 |
| 2.1 How Can We Manage Risk? | 5 |
| 2.2 Overview..... | 5 |
| 2.3 Communication and Consultation..... | 6 |
| 2.4 Establish context..... | 6 |
| 2.4.1 Parameters of risk..... | 6 |
| 2.5 Risk identification..... | 7 |
| 2.6 Risk Analysis | 8 |
| 2.7 Risk Evaluation..... | 9 |
| 2.8 Risk Treatment | 9 |
| 2.9 Monitoring and Review..... | 10 |
| 2.10 Recording | 10 |
| 3. RISK MANAGEMENT PLAN..... | 11 |
| 3.1 Risk Management Responsibilities..... | 11 |
| 3.2 Risk Management Framework Review | 13 |
| 3.3 Risk Register Establishment and Review | 14 |
| 3.4 Risk Management Plan Progress Reports..... | 14 |
| 3.5 University Plan and Annual report..... | 15 |
| 3.6 Training | 15 |
| 3.7 Summary of Key Risk Management Plan Activities | 16 |
| Appendix A – Likelihood Ratings..... | 18 |
| Appendix B – Consequence Ratings | 19 |
| Appendix C – Risk Rating Matrix..... | 19 |
| Appendix D – Control Effectiveness Ratings..... | 19 |
| Appendix E – Enterprise Risk Register Template for Riskware ERM | 20 |
| Appendix F- 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 WHS Officers. The WHS 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 JCU Singapore, which operates out of a different jurisdiction.

1.2 What is Risk?

The International Standard on Risk Management AS/NZS ISO 31000:2009 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.

The plan should ingrain a risk management consciousness into all levels of management.

1.5 Risk Management Policy

JCU has an adopted Risk Management Policy. This policy “sets the tone” for JCU's risk management approach 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?

The University already has rigorous planning processes which include University and Division Plans underpinned by an annual cycle of planning and accountability. Inherent within the various plans is consideration of the various risks facing the University and coordinated response(s) to these risks. However, to help ensure that important risks are not overlooked, a rigorous and systematic approach to identifying and adequately managing risks at strategic, operational and activity/project levels is essential.

Risk management is an ever-present management responsibility. However, this does not mean that it happens automatically. 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

The University's Risk Management process is compliant with AS/NZS ISO 31000:2009. Under this approach, there are five key stages to the risk management process.

1. Communicate and consult - with internal and external stakeholders
2. Establish context - the boundaries
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

Refer to figure 1 below for an illustration of the AS/NZS ISO 31000:2009 risk management approach.



Figure 1: JCU risk management approach using AS/NZS ISO 31000:2009 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 the foundation of good risk management and vital to successful implementation of the risk management process.

Context is established by the risk leadership team and involves setting boundaries around the depth and breadth of risk management efforts to help JCU stay focused and align the risk management framework to relevant matters required to achieve the strategic intent of the University.

Important considerations when determining context include:

- JCU's external environment – social factors, demographics, 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 attitude/tolerance, organisational structures, systems, processes, resources, key performance indicators and other drivers.

2.5 Parameters of risk

It is important that JCU understands its risk taking parameters and articulates its policies and procedures accordingly. Risk parameters are generally expressed in terms of risk capacity, risk tolerance and risk attitude. These factors will be consolidated in a University risk appetite statement and applied to the assessment of residual risk level across all risk areas (refer Section 2.5). Based on the results, the University may adjust activities to ensure decision making is consistent with its risk appetite.

Risk capacity is the amount of risk an organisation can afford to take or sustain. As nearly all risks that cause a failure of some sort ultimately result in a financial impact, risk capacity is typically expressed in the organisation's access to capital or ability to raise capital, and its earnings stability or strength. This is arguably the maximum financial impact from risk (before insurance arrangements) that JCU can take without impeding its financial viability. Other factors in identifying this capacity include organisational risk culture, strategic positioning and competitive positioning.

Risk appetite is the amount and type of risk that the organisation is willing to take in order to meet their strategic objectives. Organisations will have different risk appetites depending on their sector, culture and objectives. A range of appetites exist for different risks and these may change over time. Understanding risk appetite is particularly relevant when JCU has to make choices that are inherently uncertain such as investment strategy, major projects and long term strategy formulation.

JCU's risk appetite statement covers a number of critical risk categories. The current risk appetite statement is:

James Cook University is a medium sized, research intensive, regionally based University operating across multiple campuses including internationally. To maintain and enhance JCU's standing and reputation within the sector the University must take business risks from time to time. These risks must meet the strategic and operational imperatives established through the annual planning cycle undertaken. 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 Strategic Intent 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 breaches and consequent penalty; 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.

Risk tolerance is the amount of risk an organisation is willing to bear in respect of a particular business line, function or risk category. Ideally, the tolerance is quantified, but in any event is expressed so that relevant management responsibilities are absolutely clear. Risk tolerance which cannot be expressed in financial terms is more difficult to articulate and needs to be closely assessed as risks are identified and analysed.

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 context of the risk management activity, procedure or process. The following categories of risk should typically be considered:

- Strategic risks;
- Operational risks;
- Financial risks;
- Reputational risks;
- Legal and Regulatory risks;
- Business disruption risks;
- People risks; and
- Academic risks

It is important to undertake a systematic and comprehensive identification of all risks including those not directly under the control of JCU because a risk that is not identified at this stage will not be included in further analysis. The key questions when identifying risks are:

- What can happen?
- Where can it happen?
- When can it happen?

- Why can it happen?
- How can it happen?
- What is the impact?
- Who is responsible for managing the risk?

JCU may utilise a number of methods to help identify risks that could materially impact the business. These include:

- Brainstorming
- Formal risk workshops and consultation with stakeholders
- Personal experiences
- Expert judgement
- Periodic working committee meetings
- Periodic reviews of the risk register
- Scenario analysis
- Business process reviews and work breakdowns
- Review of actual incidents and issues identified
- SWOT analysis

It is also important to consider the potential causes of a risk as it will help risk analysis - the next stage of the risk management process. Some causes of risk could include:

- commercial/legal relationships
- socio-economic factors
- political/legal influences
- personnel/human behaviour
- financial/market activities
- management activities and controls
- technology/technical issues
- the activity itself/operational issues
- business interruption
- natural events
- custody of information including the duty to provide and withhold access

2.6 Risk Analysis

Once risks have been identified, they are then analysed. Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. At this point, no consideration is given to existing controls. The following risk criteria should be used as a guide when analysing risks.

The likelihood of occurrence is the chance of a risk event occurring. When considering the likelihood of a risk, you need to consider both past history and estimate frequency of occurrence according to a designated timescale. JCU will utilise the likelihood ratings shown in Appendix A.

The consequence assessment is the effect or impact of the risk event. It is measured both financially (in terms of profit/loss or balance sheet impact) and operationally (human and physical). JCU will utilise the consequence criteria shown in Appendix B.

Inherent risk is the overall raw risk without controls in place. It is determined by combining the likelihood and consequence ratings. Ultimately, the level of inherent risk will determine how a risk is controlled. The Risk Matrix shown in Appendix C depicts the inherent risk levels that will be used by JCU. The risk matrix can also be used to determine residual risk level after existing or new controls are implemented and their effectiveness verified.

2.7 Risk Evaluation

Risk evaluation involves comparing the level of risk found during the analysis process against JCU's known priorities and requirements.

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.

Any risks accorded too high or too low a significance are adjusted and documented accordingly. 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). The benefits of the 3-tier risk matrix include:

- A more balanced approach to risk assessment without overly re-weighting risk to the low end.
- A singular High risk category providing uniform and greater visibility to University Council for assessment against risk appetite.
- Adopting Letters A-E for Likelihood enabling risk analysis (e.g. 5E = 15 or 1A = 11), to provide an alternate combination of likelihood and consequence. Differentiating between risks within the same tier is possible.
- Replacing risk level (high, medium, low) with a number scale to derive a risk profile and prioritise risk treatments and resources accordingly.
- Removing the double-up of terms used for consequence and risk level descriptors.
- More robust review of control implementation and effectiveness (existing/planned) in order to modify risk ratings. That is, changing residual risk within a tier or between tiers is better informed and more transparent.

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 modifying risks, 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. 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. Ultimately, the level of current risk will determine how a risk is treated.

Where controls exist and are considered effective to manage the risk down to medium/low and or within risk attitude, the current risk will be low and typically, no further work is required except for periodic monitoring.

Where controls either do not exist or are considered ineffective to manage the risk down to medium/low and or within risk attitude, the current risk could be high and risk treatment is

required. The level of risk remaining after risk treatment is the **residual risk**. Where JCU accepts the remaining current risk and no further risk treatment is planned, it is good practice to document the reason why.

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The options can include the following:

- a) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- b) taking or increasing the risk in order to pursue an opportunity;
- c) removing the risk source;
- d) changing the likelihood;
- e) changing the consequences;
- f) sharing the risk with another party or parties (including contracts, risk financing and insurance); and
- g) retaining the risk by informed decision.

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.

Risks will be monitored regularly in line with their significance. At minimum, the risk register will be reviewed every six months in line with the University planning cycle.

Key Risk Indicators (KRIs) will be developed to monitor risks on an ongoing basis. KRIs are operational in nature and should be determined by the risk owner once risks and their causes have been identified. An example of a KRI might be to monitor the number of student enrolments and determine a certain percentage reduction or change which would alert the accountable person that a potential risk to the University was forming.

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.

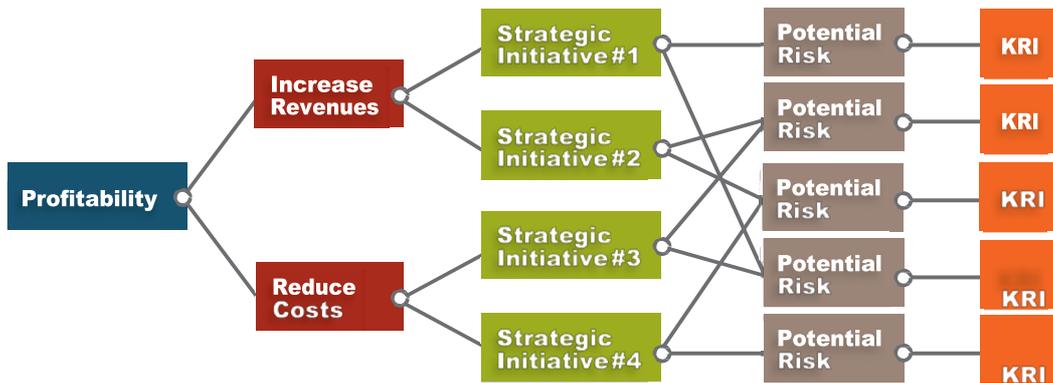


Figure 2: Linking Key Risk Indicators

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

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 will 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 and Risk Profiles** – 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.

See Annexure E for information required for the Enterprise Risk Register template on Riskware ERM and WHS Register.

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. It has a Health, Safety and Environment sub-committee.

Other Council Committees

Other Council Committees have responsibility for risk management relating to their governance area of responsibility (such as Finance 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 on an annual basis;

- 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 risk management training across the University;
- 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 *Statement on Integrity* 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 faculty/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 faculty/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 and planning package.

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. In particular the Risk Management Coordinator is to coordinate a review of the Risk Management Policy every two years (or earlier if there are any material changes in circumstances). The results of the review are to be reported to the University Executive, the Audit, Risk and Compliance Committee and ultimately the Council. The Risk Management Coordinator must also review the Risk Management Framework and Plan annually and submit the outcome and any recommended changes to University Executive and the Audit, Risk and Compliance Committee for adoption.

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

As part of the University's annual business planning cycle each Division is required to prepare a Planning Package detailing its objectives, strategies and targets. As part of the development of the planning package each Division shall identify and analyse key risks that may impact on achieving objectives. The outcome of this assessment will be recorded in a Divisional risk register and documented in the planning package. The risk register and progress in implementing risk treatment plans will be reviewed and reported at six monthly intervals in line with the review of the planning package.

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 Coordinator.

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 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 inherent and 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 and Triennium Planning | Reviewed 6 monthly – controls implemented to reduce risk to medium or below within 12 months with defined treatment plans |
| Medium | Dean/Directors/Head of Academic Group or Manager | Divisional Risk Champion | Mandatory to Risk Register and Triennium Planning | Reviewed 12 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 owner | Nil | Included in Risk Register | Nil |

3.5 University Plan and Annual report

JCU's University Plan must include a section on Risk Management that details proposed risk management activities for the coming year and discusses any key risk management issues.

JCU's Annual Report must include a section on Risk Management that details risk management activities undertaken during the previous year and any relevant risk management issues.

3.6 Training

All risk owners and other key staff 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.

3.7 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 two years in August |
| 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 year 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 as part of business planning cycle |
| 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 as part of business planning cycle |
| 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 |
| 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 – six monthly Audit, Risk and Compliance Committee – six monthly |

| | | | |
|-----------------|--|--|--|
| Annual Report | Detail risk management activities undertaken during the previous year and any relevant risk | Chief of Staff | Annual |
| University Plan | Detail proposed risk management activities for the coming year and discusses any key risk management issues. | Chief of Staff | Annual |
| 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 every two years. 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. | Likely to occur within a 3 month period or during the performance of an actual task. |

Appendix B – Consequence Ratings

Table 4: Consequence ratings

| Risk Level | Risk Area and Impact | | | | | | | |
|-----------------|--|--|---|--|---|---|--|--|
| | Financial | Academic | Reputation | Business Disruption | People | Compliance & Liability | Health, Safety & Environment | Strategic |
| 5. Catastrophic | >10% recurrent reduction in operating fund revenue, one off loss of > \$50m, Cash balance falls below 5 week forecast | Loss of accreditation of multiple courses, institutionalised and/or systemic fraud or misconduct in academic activities including enrolments and examination processes, loss of flagship research projects | Sustained negative national and international publicity that could result in significant loss of funding, staff and/or students | Unavailability of critical infrastructure, utilities > 2 weeks; unavailability of ICT services > 2 business days and catastrophic impact to critical business cycle; inability to deliver teaching > 2 days; impact to JCU research standings affecting top 2% achievement in Academic Ranking of World Universities | Recruitment to a business/academic critical role >24months resulting in serious damage to research reputation and league table standing; a significant number of resignations among high reputation researchers; Systemic failure to deal with grievances leading to multiple Fair Work Commission rulings against the University with moderate financial impact and reputational damage affecting student recruitment; Prolonged University-wide industrial action potentially resulting in business disruption, reputational damage and student recruitment | Successful class actions or serious prosecution, repeated breaches of significant contractual arrangements, significant statutory intervention due to serious breach of legislation and/or breach of university policy resulting in termination of employment | Fatality; prosecution and penalty/fine >\$500k; Smartraveller Alert Level 4; Long term environmental damage (5 years or longer), requiring >\$1M to remedy; Breaches results in prosecution by DEHP. | Most University objectives can no longer be achieved; complete revision of long term business model required |
| 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; Medium-term (1-5 years) environmental damage, requiring >\$500k to \$1M to study and/or remedy; Breaches result in an Enforceable Undertaking by DEHP | A number of significant University objectives can no longer be achieved |

| Risk Level | Financial | Academic | Reputation | Business Disruption | People | Compliance & Liability | Health, Safety and Environment | Strategic |
|------------------|--|--|---|---|---|---|--|--|
| 3. Moderate | Between 1 & 5% recurrent reduction in operating fund revenue, one off loss of between \$5m & \$20m | Loss of voluntary accreditation of single course, localised fraud or misconduct in academic activities, loss of significant research project | One off negative publicity of several days' duration requiring some management resources to deal with | Unavailability of critical infrastructure, utilities between 3 & 5 days; unavailability of ICT services during business day for 12-24 hours and/or moderate impact to critical business cycle; inability to deliver teaching for 12-24 hours; loss of raw un-reproducible data; research productivity impact 2-8 weeks; possible impact to JCU research standings | Recruitment to a business/academic critical role 6-12months from advertising; Escalation of performance management case(s) to Fair Work Commission; Inability to attract/retain key staff across multiple disciplines; Morale issues impacting operational performance across a Division | One off breach of legal or contractual arrangements requiring legal or regulatory intervention; repeated breaches of university policy with formal counselling of an employee | Lost time injury; penalty/fine between \$50-200k; Smartraveller Alert Level 2 or combination of 2 and 3; Short-term (less than 1 year) environmental damage, requiring >\$150k to \$500k to study and/or remedy; Administrative action taken by Env. Regulator | Some important University objectives can no longer be achieved |
| 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 hours and/or minor impact to critical business cycle; Inability to deliver teaching for 4-12 hours; Loss of research processing data, productivity impact (1-2 weeks) | Recruitment to a business/academic critical role within 3-6months from advertising; Performance management case(s) satisfactorily resolved by University requiring dedicated HR resources: Inability to attract/retain staff in a specialised area; Morale issues restricted to a Directorate/College impacting operational performance | Minor breach of regulations or standards; one off minor breach of university policy and no formal counselling of employee | Incident including medical treatment injuries, near miss; penalty/fine <=\$50k; Smartraveller Alert Level 1 or combination of 1 and 2; Environmental damage, requiring up to \$150,000 to study and/or remedy; Infringement notice may be issued by Env. Regulator | Reprioritisation of resources to enable achievement of key University objectives |
| 1. Insignificant | One off, or recurring loss of <\$1m | Minor academic indiscretions dealt with according to normal procedures | One off media enquiries or neutral press coverage | Unavailability of critical infrastructure, utilities < 1 day, unavailability of ICT services during business day for < 4 hours and/or very limited impact to critical business cycle; inability to deliver teaching for < 4 hours; Minor loss of research data, little to no productivity impact | Performance management cases resolved satisfactorily requiring minimal HR resources; Higher than desired staff turnover in non-critical areas; Localised morale issues with minimal impact on operational performance | Minor technical breach of standards | Incident including first aid; workplace hazard contained immediately and no ongoing safety risk; Smartraveller Alert Level 1; Negligible environmental impact, managed within operating budgets; Warning notice/letter may be issued by Env. Regulator | Little or no impact on University objectives |

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 | 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 - Enterprise Risk Register Template for Riskware ERM

CONTEXT

Step 1
Classify the Risk

Date Risk Identified: 29/04/2016
Risk Owner: Aaron Ginzburg

Select the primary affected Business Unit:
James Cook University (the Group)

Select the affected Business Function:
-- please select a business function --

Select the Risk Type:
-- please select a risk type --

Step 2
Select one or more impacted Risk Consequence Category

- Academic
- Compliance & Liability
- People
- WHS
- Business Disruption
- Financial
- Reputation

IDENTIFY

Step 3
Risk Description - Identify and describe the Risk

ANALYSE

Step 4
Risk Source/Causal Factor
What will/could cause the Risk to occur?

EVALUATE

Step 5
Existing Control(s)
Describe the Control and its effectiveness

Step 6
Current Risk Rating
Level of Risk with existing Control(s)

TREAT

Step 7
Risk Treatment Option
Select your Treatment Option to mitigate/manage this risk

Step 8
Risk Treatment Plan
Describe your Treatment Plan to mitigate/manage the Risk

Step 9
Who is responsible and by when?
Select the person and due date

Step 10
Target Risk Rating
Level of Risk after Treatment

powered by **riskware** Copyright Disclaimer Privacy Contact Us About Us

Appendix F- Risk Management Glossary

Adapted from AS/NZS ISO 31000:2009

| | |
|---------------------------------------|---|
| 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 |
| consequence | outcome of an event affecting objectives |
| control | measure that is modifying risk |
| establishing the context | 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 |
| external context | external environment in which the organisation seeks to achieve its objectives |
| internal context | internal environment in which the organisation seeks to achieve its objectives |
| level of risk | magnitude of a risk , expressed in terms of the combination of consequences and their likelihood |
| likelihood | chance of something happening |
| monitoring | continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected |
| residual risk | risk remaining after risk treatment |
| review | activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives |
| risk | effect of uncertainty on objectives |
| risk analysis | process to comprehend the nature of risk and to determine the level of risk |
| risk appetite | the amount and type of risk an organisation is prepared to accept in the pursuit of its organisational objectives |
| risk assessment | overall process of risk identification , risk analysis and risk evaluation |

| | |
|----------------------------------|---|
| risk criteria | terms of reference against which the significance of a risk is evaluated |
| risk evaluation | process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable |
| risk identification | process of finding, recognizing and describing risks |
| risk limit | 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 |
| risk management | coordinated activities to direct and control an organisation with regard to risk |
| risk management framework | set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring , reviewing and continually improving risk management throughout the organisation |
| risk management plan | scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk |
| risk management policy | statement of the overall intentions and direction of an organisation related to risk management |
| risk management process | 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 |
| risk owner | person or entity with the accountability and authority to manage the risk |
| risk profile | description of any set of risks |
| risk source | element which alone or in combination has the intrinsic potential to give rise to risk event |
| risk tolerance | the specific maximum risk that an organisation is willing to take regarding each relevant risk (sub-) category, often in quantitative terms |
| risk treatment | process to modify risk |

Administration

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

Approval Details

| | |
|----------------------|-----------------|
| Policy Sponsor | Vice Chancellor |
| Approval Authority | Council |
| Date for next review | August 2019 |

Revision History

| Version | Approval date | Implementation date | Details | Author |
|---------|---------------|---------------------|--|----------------|
| 18-1 | 07/09/2018 | 08/09/2018 | Annual review of framework and plan – approved by Council (5/18) refer to Council Minutes 07/09/2018 | Chief of Staff |
| 17-1 | 07/09/2017 | 27/09/2017 | Annual review of framework and plan – approved by Council (5/17) refer to Council Minutes 07/09/17 | Chief of Staff |
| 16-1 | 01/09/2016 | 06/10/2016 | Revised framework and plan – refer to Council minutes (7/16) 1 September 2016. | Chief of Staff |

| | |
|-----------------|---|
| Contact person: | Chief of Staff |
| Keywords | Compliance, standards of compliance, compliance framework |