THE UNIVERSITY of ADELAIDE

RISK MANAGEMENT FRAMEWORK

adelaide.edu.au

CONTENTS

PART A: Introduction 2

1. Scope and Purpose 2
2. What is Risk Management? 3
3. What are the benefits of risk management? 3
4. Risk management in the University 4

PART B: Risk Management Framework 5

5. Overview 5
6. Risk Management Standard 6
7. Risk Management Accountability 7
8. Risk Appetite 9
9. Risk Management Operating Model 11
10. Risk Assessment 12
11. Risk Categories 14

PART C: Methodology / Process 16

12. Overview 16
13. Step 1 - Establish the context 17
14. Step 2 - Identify the risk 19
15. Step 3 - Analyse the risk 20
16. Step 4 - Evaluate the risk 21
17. Step 5 - Treat the risk 22
18. Monitor and review 24
19. Communicate and consult 27

PART D: Appendix 28

20. Appendix 1: Glossary of Terms 29
21. Appendix 2: Risk Management Relevance in University Context 31
22. Appendix 3: University Risk Tolerance Statements 33
23. Appendix 4: University Risk Management Responsibilities 39
24. Appendix 5: University Risk Register 40
25. Appendix 6: University Risk Matrix (Likelihood & Consequence) 42

PART A: INTRODUCTION

1. Scope and Purpose

This document outlines the Risk Management Framework for the University of Adelaide and all its operations and entities. The framework defines the University's risk operating model, appetite, responsibilities, methodology, and monitoring and reporting obligations.

In this framework, the terms 'risk' and 'risk management' are defined as follows[1]:

- Risk is defined as the ***effect of uncertainty on objectives***. An effect is a deviation from the expected – positive and/or negative. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances or knowledge) and the associated likelihood of occurrence.
- Risk management is defined as the ***coordinated activities to direct and control an organisation with regard to risk.***

The University is committed to building a risk culture that encourages deliberate and pro-active risk management in a manner and at times or intervals commensurate with the University's strategic objectives.

The University[2] has a statutory obligation for risk management that is established within the *University of Adelaide Act 1971* (the Act). In addition, the University recognises that effective risk management is an integral part of good governance and best management practice, and that it assists the University meet its statutory objectives and deliver on its broader strategy and business plans.

The Council, the Audit Compliance and Risk Committee, and the Vice-Chancellor, have ultimate responsibility for risk within the University. From this highest level of governance and management, each of the Divisions, work with the Faculties, Schools and administrative areas so that risks are managed strategically and operationally. For the University's Controlled Entities, the Board and Senior Management of each entity takes responsibility for managing their risks.

While the principles of risk and the risk management processes are generic and applicable to all fields of risk, the reporting, management and monitoring of specific types of risk varies across the University. This means that various risks are managed by a number of areas, roles and committees at both governance and management levels spanning the vast range of activities of the University.

The University must also have regard to additional governance and management requirements and structures such as those imposed by government and regulatory authorities and agencies, funding bodies, insurers, ReturnToWorkSA, professional standards and accrediting bodies, ethics committees, and requirements of affiliates.

The Risk Management Framework connects the University's governance structure and the management structure so that the two work together to provide a joint commitment, set of expectations, and organisational and personal accountabilities and responsibilities. The purpose of the framework is to assist the University in integrating risk management into significant (i.e. critical / material) activities and functions.

[1] ISO 31000 Risk Management – Guidelines; and ISO Guide 73 – Vocabulary

[2] Throughout this document, any reference to "The University" means and includes the University itself, its student body, all academic and professional staff, titleholders and contractors, and staff and employees of controlled entities.

2. What is risk management?

Organisations of all kinds face challenging natural, political, socio-economic and cultural influences that make their operating environments uncertain. These influences may impact on the extent to which objectives can be met.

The effect this uncertainty has on the organisation's objectives is known as *risk*. Risk is the possibility of an event or activity preventing the University from achieving its outcomes or objectives.

Risk management encompasses the activities and actions taken to ensure that the University is conscious of the risk it faces, makes coordinated and informed decisions in managing those risks, and identifies potential opportunities.

Risk management can be *value enhancing* or *value protecting*, or both.

- The actions, processes and controls put into place to manage risks that affect the achievement of the University's strategy are *value enhancing*; that is, they increase the potential for achieving strategic outcomes that add value to the University.
- The actions, processes and controls put into place to manage risks that have a negative consequence are *value protecting*; that is, they protect the value of the University by preventing or minimising the impact of negative events.

There is some level of risk present in every aspect of the University's operations; therefore, it is critical that risks are understood and managed appropriately. In understanding the risks it faces, the University can make informed decisions that promote the achievement of strategic objectives / initiatives.

3. What are the benefits of risk management?

Effective risk management improves

- the ability to identify, evaluate, and manage threats and opportunities,
    - including the flexibility to respond to unexpected threats, and the
    - ability to take advantage of opportunities and gain a competitive advantage;
- the management of complex and shared risks;
- accountability and facilitates better governance;
- financial management;
- organisational performance and resilience; and the
- confidence to make difficult decisions.

Effective risk management decreases

- the potential for unacceptable or undesirable behaviours, such as fraud or harassment.

An effective risk management framework is essential for the ongoing sustainability and success of the University. It is also helps to assure the University Council, management and stakeholders that the risks of operating a university are understood, that adequate steps have been taken to minimise and mitigate risks, and that the University has in place systems to operate responsibly.

4. Risk management in the University

Risk management should be designed and executed so that the University can meet its statutory object and succeed in its broader strategic objectives as determined from time to time.

The University is influenced by internal drivers, such as the University's Strategic Plan and Enterprise Agreement, and external influences and challenges, such as:

- Political will, policy changes, funding cuts;
- Global economic instability, currency risks, financial sustainability, use of limited resources;
- Globalisation and the digital revolution: growing global business and political interdependence and the unending transformation of educational delivery;
- New choices and pressures for students and staff: increased student mobility and expectation in course content, delivery and environment; increasingly fierce competition for research funding and in attracting the most qualified staff and the brightest students;
- Rising equipment costs and escalating pressures on researchers from grant agencies and the international ranking environment;
- Space and infrastructure constraints which impact existing services and new initiatives;
- Environmental impacts: increasing pressures on the natural environment, and the need to manage the built and natural environment to ensure long term sustainability and survival;
- Threats of campus exposure to violence and pandemics with negative impacts for student and staff enrolment and retention; exposure to pandemic infections increasing with frequency and ease of travel;
- Increasing scrutiny and demands for diligence, transparency and accountability;
- Government regulation, monitoring and oversight;
- Regular audits from external agencies (e.g. Auditor General, Commonwealth & State Department of Education, ReturnToWorkSA) and a wide range of compliance obligations / requirements, both legislative / regulatory requirements and contractual obligations which scrutinise all aspects of the University's operations and demand compliance with best practice (e.g. NHMRC, TEQSA, ESOS & ERA, AQIS, the Ombudsman's Office, the Gene Technology Regulator).

A demonstrable risk management system incorporates

- *Risk appetite*
- *Risk profiles*
- *Risk assessments*
- *Treatment plans*
- *Results of monitoring & risk reviews*
- *Evidence of consultation & communication*
- *Good documentation / formal records*

In addition, Commonwealth and State funding bodies seek evidence of a *demonstrable* risk management system as part of their funding requirements and agreements.

Without a demonstrable system, relationships and funding associated with our learning, teaching and research opportunities, our commercial activities and our philanthropy and fundraising endeavours are potentially at risk.

For a University, brand and reputation are critical; damage to brand and reputation may be transient or long lasting and will almost certainly effect rankings, research funding, ratings, research partnerships, and public and political sentiment and support; it can adversely impact student enrolments, staff morale, and community engagement.

PART B: RISK MANAGEMENT FRAMEWORK

5. Overview

The Risk Management Framework is a set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. The foundations include the policy, objectives, mandate, and commitment to manage risk. The organisational arrangements include plans, relationships, accountabilities, resources, processes, and activities. The risk management framework is embedded within the organisation's overall strategic and operational policies and practices[3].

The University of Adelaide Risk Management Framework:

1. ***Connects*** the mandate with the process. The mandate comes from the University of Adelaide Act and the Council and is expressed through and overseen by various standing and management committees such as the Audit Compliance and Risk Committee, whose terms of references explicitly address risk management, and the University Risk Management Committee.
2. ***Recognises*** the influence and expectations of various external funders, regulators, auditors, and research collaborators, and through enterprise and operational risk and the internal audit program, connects those expectations and aspirations with what we do.
3. ***Influences*** the existing culture to better manage risk and opportunity, having regard for our economic, social, regulatory, political and competitive environment locally, regionally and internationally in alignment with our strategic objectives.
4. ***Defines*** the appropriate boundaries for risk-taking by setting organisational risk appetites and tolerance levels.

The **major elements** of the University Risk Management Framework include:

- Risk Management Policy – formally outlines the policy principles, procedures and institutional and individual responsibilities, requirements and structures. It recognises the legislative mandate and the role of the University Council. The policy affirms the University's strategic commitment to building a risk management culture in which risks and opportunities are identified and managed effectively.
- Risk Appetite Statement – articulates the University's appetite for risk, and associated tolerance levels.
- Risk Management Methodology – outlines the process to guide, direct and assist everyone to better understand and adopt consistent risk assessment processes.
- University Risk Register – principle repository for recording and tracking risks, including recommendations / agreed actions from auditors, regulators, insurers and relevant agencies.
- University Risk Centre – comprising the Director, Risk Services (Anne Hill) and General Counsel and Executive Director, Legal and Risk (Céline McInerney) in the Legal and Risk Branch, Division of University Operations, who have primary responsibility for facilitating and supporting University risk management.
- University Risk Management Committee – convened by the Chief Operating Officer and responsible for the overall coordination of risk management within the University, and reporting annually to management.
- Regular monitoring, review and reporting - confirmation that risk management is relevant, demonstrable, effective and supporting the objectives of the business.

[3] ISO 31000 Risk Management – Guidelines; and ISO Guide 73 – Vocabulary

6. Risk Management Standard

The University's Risk Management Framework and Policy are aligned to the International Standard ISO 31000: 2018 Risk Management – Guidelines (the Standard), which outlines the principles, framework and process for risk management.

Risk is defined by the Standard as the *effect of uncertainty on objectives*[4].

Risk management is defined as the *coordinated activities to direct and control an organisation with regard to risk.*

For those coordinating activities, making decisions, setting and achieving objectives and improving performance, managing risk:

- is iterative and assists organisations in setting strategy, achieving objectives and making informed decisions;
- is part of governance and leadership, and is fundamental to how the organisation is managed at all levels;
- is part of all activities associated with an organisation and includes interaction with stakeholders; and
- considers the external and internal context of the organisation, including human behaviour and cultural factors.

The University adopts the principles of risk management, as set out in the Standard, which provide guidance on the characteristics of effective and efficient risk management, communicating its value, and explaining its intention and purpose.

The principles are summarised as follows:

1. Framework and processes should be customised and proportionate to the level of risk faced by the organisation;
2. Appropriate and timely involvement of stakeholders is necessary;
3. A structured and comprehensive approach is required;
4. Risk management is an integral part of all organisational activities; risk management activities need to be aligned with other activities / objectives (strategy);
5. Risk management must be dynamic and anticipate, detect, acknowledge and respond to changes;
6. Risk management needs to use the best information available;
7. Human and cultural factors influence all aspects of risk management, and should be considered; and
8. Risk management is continually improved through learning and experience.

[4] ISO 31000:2018 Risk Management – Guidelines

7. Risk Management Accountability

The Council is the University's governing body and oversees and monitors the assessment and management of risk in accordance with its statutory obligations set out in the Act.

To assist in the discharge of its statutory mandate, Council has established Standing Committees to oversee and monitor academic, cultural, financial, property, audit, compliance and legal risks.

Management of risk (including planning, decision-making, reporting, and accountabilities) is determined by the Vice-Chancellor and Chief Operating Officer (COO).

From this highest level of management, each of the Divisions, led by the Vice-Presidents and COO, work with the Faculties, Schools and administrative areas so that management risks are managed strategically and operationally. For the University's Controlled Entities, the Board and senior management of each entity takes responsibility for managing their risks. Risk management is thus a *shared responsibility* across the governance committees, executive managers, local areas and staff. Appendix 4 provides further detail on roles and responsibilities.

To ensure the effectiveness of the Risk Management Framework, the Council and Senior Management need to rely on adequate monitoring and assurance functions within the University. The framework uses the ***Three Lines of Defence*** model (refer *Figure 1*) which is a simple way of explaining the relationship between these functions and acts as a guide to how responsibilities should be divided:

1. first line of defence – functions (people, process & technology) that own and manage risk;
2. second line of defence – management and oversight; functions that oversee and specialise in risk management and compliance; and
3. third line of defence – internal audit; functions that provided independent assurance.

The principles of risk and the risk management process are generic and applicable to all fields of risk, however the management and monitoring of specific types of risk varies across the University.

- Academic Standards: The University has a statutory obligation for managing academic activities and standards. The Council, Academic Board and the Vice-Chancellor are responsible for management – including risk management - of academic standards. This includes the standards and requirements imposed by government and regulatory authorities, funding bodies, accreditors and professional standards committees.
- Workplace Health and Safety: The Council, the Audit Compliance and Risk Committee, the Vice-Chancellor, and the Executive Deans have overall responsibility for the University's Workplace Health and Safety Management System. Responsibilities for safety, injury management and well-being within the University are defined in the HSW Handbook and in the WHS systems of its Controlled Entities. Special consideration must also be given to the Return to Work SA Act and the "Code of Conduct for Self-Insured Employers".
- Research ethics, compliance and integrity: The Council, the Vice-Chancellor and the Deputy Vice-Chancellor (Research), have overall responsibility for risk management of all research activities. In addition special consideration must be given to National Codes, legal and regulatory compliance and statutory ethics committees.
- The University must also have regard to additional governance and management requirements and structures such as those imposed by government, regulatory authorities and agencies, underwriters and insurers, professional standards and affiliates.

Every person who engages in University activities is impacted in some way by risks, so every person has an active role in being '*risk aware'*. This involves identifying, assessing and managing risks and opportunities in day-to-day decision-making and business planning, understanding and adhering to the reporting process within the University's governance framework, and promoting a risk aware culture.

Certain people will be more active in the risk management process than others:

- all people who work for the University are encouraged to identify and report risks;
- senior staff and managers will help staff and students cooperate and comply with controls put into place by the University to mitigate certain risks;
- certain individuals / managers within the University, and within each of the Controlled Entities, will monitor and review or formally report on risks; and
- others will carry out tasks, often in collaboration, to ensure that risks are treated or controlled.

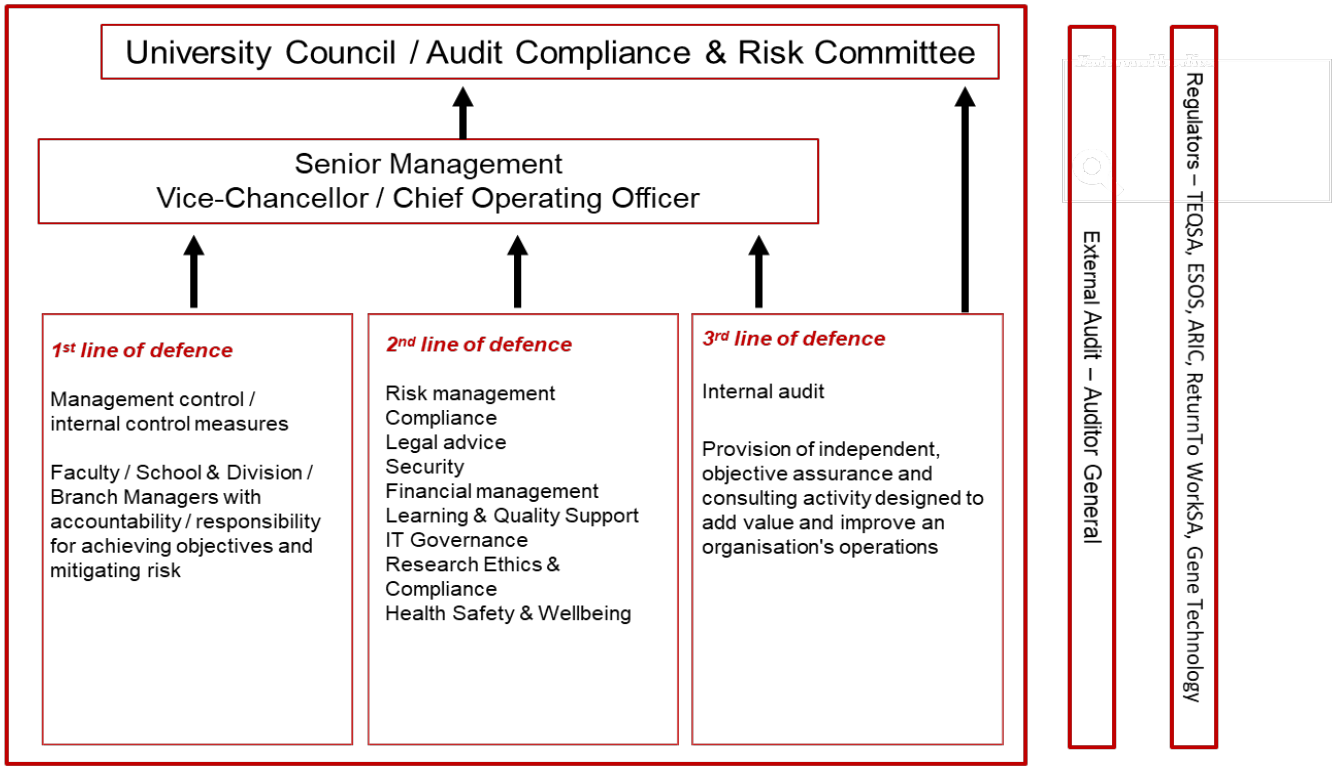
While ***hazard management*** and the control of safety risks are addressed through the University's Health, Safety and Wellbeing Framework, it is **everyone's** responsibility to ensure that all high or very high risks under the Hazard Management Framework are also reported in accordance with the University's Risk Management Policy.

Risk owners are accountable for the oversight and stewardship of risk management, from original concept through to execution and implementation, and where relevant, to the end of term of a proposal, project, plan or relationship. For research projects or activities, the risk owner is the Chief Investigator. For teaching projects or activities, the risk owner is the lead Academic managing or organising the activity.

The ***University Risk Centre*** (within the Legal and Risk Branch) will facilitate and support the University risk management framework.

Everyone is expected to work individually and collectively towards the active promotion of a positive risk management culture within and across the University, and its' Controlled Entities.

Three lines of defence*



Ref. The Institute of Internal Auditors Global

Figure 1: Three Lines of Defence

8. Risk Appetite

Risk is a necessary part of doing business. Not all risk can be treated or avoided, therefore, organisations have to accept some level of risk. An organisation's appetite for risk is central to the way it does business. Each level of the organisation needs clear guidance on the limits of risk they can take.

The University adopts the definitions for risk appetite and risk tolerance that are set out in the Standard - ISO 31000:2018 Risk Management - Guidelines.

- Risk appetite: *the **amount of risk** the University is willing to accept or retain in order to achieve its objectives.*
- Risk tolerance: *the **levels of risk taking** acceptable to achieve a specific objective or manage a category of risk.*

Risk appetite ***sets the tone*** for risk-taking in general; risk tolerance ***informs***

i. expectations for mitigating and pursuing specific types of risk;
ii. boundaries and thresholds for acceptable risk taking; and
iii. corrective actions to be taken when tolerances are reached or breached.

The University's appetite for risk is communicated primarily through the strategic planning process. In determining its appetite for risk, the University needs to strike a balance between a prudent and robust approach to risk mitigation, and to permit sufficient flexibility to foster the entrepreneurial spirit that has greatly contributed to the University's success.

Risk appetites and tolerances will be set, approved, monitored and reviewed at appropriate intervals by both governance and management noting that:

- Risk appetite is not a single, fixed concept.
- There will be a range of appetites for different risks which need to align and these appetites may vary over time: the temporal aspect of risk appetite is key to setting, monitoring, and adjusting risk appetite.
- Risk appetite must take into account differing views at a strategic, tactical and operational level.
- Although risk appetite is commonly thought of in strategic terms, risk appetite must be addressed throughout the breadth of the University's operations to be useful / effective.
- The propensity to take risk, and the propensity to exercise control, directly influence the setting and monitoring of risk appetite.
- It is important to determine what successful performance looks like in order to set risk appetite and tolerance.

Risk appetite is assessed as *conservative, balanced* or *entrepreneurial*, as follows:

Conservative: unless there is a compelling reason to do so, the University should not accept opportunities with risks attached that could result in significant exposure or loss, and should proceed with caution in pursuing these opportunities.

Balanced: there is some risk associated with the opportunity being pursued, however there are mitigating actions available to help reduce these risks to an acceptable level of exposure.

Entrepreneurial: there is some higher risk associated with the opportunity being pursued, but there are treatments available to mitigate the risk, and the opportunity is worth pursuing / too good to miss.

In broad terms the University's appetite for risk is shown in the table below.

Risk Category	Less willing to take risks								Greater willingness to take risks
	Conservative			**Balanced**			**Entrepreneurial**		
	1	2	3	4	5	6	7	8	9
1. Academic mission					■	■	■		
2. Strategic growth							■	■	■
3. Student experience					■	■	■		
4. Research						■	■	■	
5. Teaching					■	■	■		
6. Culture and values				■	■	■			
7. Financial viability				■	■	■			
8. Service disruption	■	■	■						
8. Safety and health	■	■	■						
10. Regulatory & compliance	■	■	■						
11. Environmental & social responsibility					■	■	■		

Figure 2: Risk appetite - broad categories of risk

Each risk category (listed above) will have a set of risk tolerance statements articulated. In most categories there will be a range of tolerances from the highest level of tolerance (10) to the lowest level (1) or zero tolerance (0). These tolerances are not exclusive; they are intended to help guide thinking around risk appetite.

Risk tolerance levels will be formatted as shown:

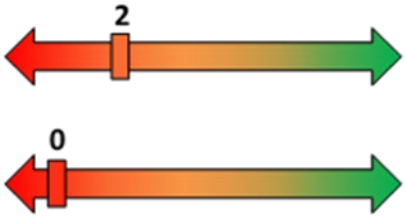
Risk Category	Level of Risk Tolerance	Risk Tolerance Statements
	Lowest to highest 0 = lowest tolerance 10 = highest tolerance	
Safety and health		The University is committed to providing a safe workplace for all employees, students, visitors and contractors. The University has a ***conservative*** appetite for risk towards safety and health. ***Low*** tolerance for lost time or injury in areas where there is inherent risk in the nature and location of some activities and environments. ***Zero*** tolerance for death or permanent disability due to departure from, or inadequate safety protocols, and for lost time or injury due to departure from prescribed safety protocols or standards.

Figure 3: Sample Risk Tolerance Statements

Refer to Appendix 3 for the full list of risk tolerance statements (note, these are subject to change as appetite changes).

9. Risk Management Operating Model

All risk management effort should be commensurate with both opportunity and exposure to risk, with a focus on the pursuit of opportunities rather than threat assessment, so that risk management is primarily a business enabler.

Risks are managed by a number of areas, roles and committees at both governance and management levels; therefore, in accordance with the University's enabling legislation:

- Academic risk is to be managed, monitored and overseen by Academic Board and the Vice-Chancellor.
- Research risk management is to be set, managed, monitored and overseen in accordance with the Relevant Laws and Codes. Research Risk is to be assessed by Risk Owners (i.e. Chief Investigators) using the University Risk Assessment and Reporting Tool. All projects rated High or Extreme risk must be logged in the University Risk Register.
- Workforce health and safety risk is to be set, managed, monitored and overseen in accordance with the Return to Work SA legislation and the University's self-insurance status under that legislation.
- The University's Controlled Entities must adopt University policy and procedures or demonstrate to the University's reasonable satisfaction that they have an equivalent policy and procedures.
- State and Federal regulators and agencies mandate Codes, laws or systems that apply to the University. They routinely prescribe, approve and oversee university policies, procedures and processes. Where this occurs, risk management effort does not need to be duplicated provided that there is demonstrable evidence of compliance with regulators' and agencies' requirements.

Subject to University policies, and State and Commonwealth laws that state otherwise, the University recognises that ***measured risk-taking*** is acceptable and appropriate: its aim is to calibrate risk management efforts relative to the exposure to risk and to emphasise opportunity wherever possible so that risk enables the achievement of the University's strategy.

Material Risks are those that may adversely affect the University's ability to deliver on its statutory objective or to deliver on its broader strategy and business plans. All material risks are to be identified, reviewed and reported to governance and management at appropriate intervals, having regard for the potential positive or negative impact on the University's pursuit and achievement of strategic, business and operational plans.

Sound risk management discipline must be evident ***throughout the lifecycle*** of current and proposed projects, activities, investments, relationships, business planning and decision-making, that commit the University to a relationship, undertaking, contract, agreement, obligation, the deployment of natural, built or technology resources or a financial liability.

Risk assessments should:

- be based on sound financial, commercial and business principles as well as the judgment and discernment of the relevant risk owner;
- demonstrably account for those influences and factors that provide the basis for stakeholders and management to make sound judgement about the things that matter, and to take actions that influence the University's direction and performance; and
- be formally documented in the University Risk Register, or approved alternative format, and available for governance or management scrutiny as required.

10. Risk Assessment

Risk assessment refers to the overall process of risk identification, analysis and evaluation; assessments should be tailored to the context. Documenting / recording the risk is important so that others can understand or appreciate the rationale for the decisions made and the treatment of the risk.

Risk assessments are ***required***:

1. Where there is ***potential*** *for one or more of the following consequences to materialise*:
   a) Sustained reduction in student satisfaction or enrolments
   b) Structural inability to meet teaching or research targets outlined in strategic plans
   c) Major organisational change leading to sustained industrial action
   d) Compromised safety for staff, students or volunteers
   e) Loss or extended interruption of critical business system or systems
   f) Sustained adverse media comment
   g) Significant financial costs / losses over time (>$1m)
   h) Legal or regulatory action leading to financial loss (>$1m) or pervasive reputational damage
   i) Material impact on access to or use of facilities and infrastructure
   j) Significant opportunity foregone (e.g. failing to capitalise on a major commercial opportunity)
2. When the University *is* ***asked*** *to, or* ***intends*** *to*:
   a. make a commitment (any binding agreement),
   b. incur a significant liability,
   c. apply resources, including in-kind contributions of time, effort or space,
   d. engage in a partnership, project or proposal that commits time, space and effort; or
   e. invest in or acquire assets in plant and equipment, technology or infrastructure ***and***
3. Where the ***financial value*** exceeds the thresholds or indicators shown in Figure 4.
4. Where an assessment is conducted in accordance with the Hazard Management chapter of the HSW Handbook and the *residual safety risk* (the risk after controls are applied) ***remains high or very high***.
5. When planning or prior to undertaking **any new research project**, and throughout the lifecycle of the project, using the University Risk Assessment and Reporting Tool.

Risk assessments are ***not required*** for University activities that are already subject to risk management frameworks or processes imposed internally, or externally by agencies, regulators or funding bodies. Where this is so, there is *no requirement to duplicate* that risk assessment exercise or process. These exceptions categories include risk systems and frameworks associated with:

i. Public funding provided through grants
ii. Risks and licences permitted under TEQSA
iii. The legislative requirements and standards for the quality assurance of courses offered to international students in Australian on a student visa (ESOS)
iv. Legislative requirements of the *WHS Act*, and the requirements of ReturnToWorkSA within the WHS Standards for self-insured employers where the residual risk (after controls are applied) is low or medium
v. Research that has been approved by recognised human and animal ethics committees
vi. Those activities regulated by the statutory office of the Gene Technology Regulator for the protection of the health and safety of people, and the environment
vii. Those activities regulated by the Commonwealth Department of Agriculture and Water Resources to safeguard Australia against animal and plant pests and diseases through audit and assurance
viii. Those activities regulated by the Department of Defence to safeguard national security
ix. Property projects (including capital works, maintenance, refurbishments and/or renovations) that are assessed in accordance with the Infrastructure Design Standards
x. Technology projects that are assessed in accordance with the Technology Governance Framework and Solutions Delivery Framework

The decision to accept that a formal risk assessment is not required is made by the business owner with delegation / authority, and / or the relevant Risk Owner.

Risk assessments must be available on request when required by the University, or by an internal or external auditor, agency or regulator, and must be escalated as required as per the Risk Management Policy.

Investment / commitment / University exposure - financial thresholds for mandatory risk assessment

$6m and above

Type of Risk Assessment: Aligning with Financial Investment Framework, any commitment / investment proposal intended for Council requires robust modelling, forecasts and investment rationale, to enable Council to make informed decisions

Investment / Commitment Approval: University Council (unless designated by Council as an Approved Project)

Documentation: Formal risk assessment incorporated in Detailed Business Case & Project(s) Risk Register; records retained in accordance with University Records Policy

$2m - $6m

Type of Risk Assessment: Aligning with Financial Investment Framework, requires Detailed Business Case, including a financial model

Investment / Commitment Approval: Vice-Chancellor; report to Council for noting

Documentation: Formal risk assessment incorporated in Detailed Business Case & Project(s) Risk Register; records retained in accordance with University Records Policy

$1m - $2m

Type of Risk Assessment: Aligning with Financial Investment Framework, requires Concept Business Case, including financial model for investments of between $1m-$2m or investments of >$1m for multiple years

Investment / Commitment Approval: Senior Executive as permitted by Delegation of Authority

Documentation: Formal risk assessment incorporated in Concept Business Case & Project Risk Register; records retained in accordance with University Records Policy

Below $1m

Type of Risk Assessment: Aligning with Financial Investment Framework, requires financial model for investments between $500k and <$1m in a year, or between $250k to <$1m p.a. over multiple years

Investment / Commitment Approval: As permitted by Delegation of Authority e.g. Faculty – Executive Dean or Head of School; Division – DVC / COO, or Branch Manager

Documentation: Formal risk assessment not mandated; records retained in accordance with University Records Policy

Exceptions categories = *no requirement to duplicate risk assessment*

The exceptions categories includes risk systems & frameworks associated with:

- Public funding provided through grants
- Risks & licenses permitted under *TEQSA*
- Legislative requirements & standards for the quality assurance of courses offered to international students in Australia on a student visa (*ESOS)*
- Legislative requirements of the WHS Act, and requirements of *ReturnToWorkSA* within the WHS standards for self-insured employers where the residual risk (after controls are applied) is low or medium
- Research that has been approved by recognised human & animal *Ethics Committees*
- Activities regulated by the statutory office of the *Gene Technology Regulator* for the protection of the health & safety of people & the environment
- Activities regulated by the Commonwealth *Department of Agriculture & Water Resources* to safeguard Australia against animal & plant pests & diseases through audit & assurance
- Activities regulated by the Department of Defence to safeguard *national security*
- *Property* projects (including capital works, maintenance, refurbishments, renovations) and *Technology* projects subject to formal project methodology

Figure 4: Requirements for mandatory risk assessment

11. Risk Categories

The University categorises risk in a number of ways: the primary differentiation is strategic and operational risk.

Strategic risks are captured within the University's Enterprise Risks. Not exclusively, strategic risks arise from the enabling legislation, the contemporary operating environment of a modern university, political uncertainty, the needs and demands of students, staff and stakeholders, the sector generally and our place locally and nationally, as a Go8 member, and as a globally competitive and ranked educational institution (geopolitical influence). The Enterprise Risks address risks and opportunities associated with:

1. advancing learning & teaching pedagogy;
2. attracting a high quality & diverse international student body;
3. driving strategic research objectives;
4. attracting, developing & retaining a high performing & agile workforce;
5. providing an environment that protects against virtual & physical threats;
6. managing financial performance & sustainability;
7. investing in physical & virtual environments, amenities & equipment;
8. maintaining pace & agility for dynamic transformation in technology;
9. overseeing & governing the University's strategic direction;
10. leveraging, fostering & sustaining engagement with business, industry, government & alumni;
11. preparing for & responding appropriately to a major disruption event;
12. complying with Australian & International legal & regulatory obligations; and
13. geopolitical risks.

Enterprise Risks must take account of the various strategic influencing factors in the University's mission of advancing learning and knowledge and the provision of university education, as well as the other activities of the University introduced through its governing legislation, such as commercial activities.

Operational Risks are specific, local and temporal. They come from internal activities as well as external influencers, such as funding sources, partnerships and alliances. They reflect part or all of the influencing factors in varying ways with variable impact across the University. Operational risks may be material.

Certain types of activities may give risk to major or extreme consequences for the University when they are not managed appropriately according to a risk management plan. While the list below is not exhaustive, consider the broader impact for the University when assessing risks associated with:

Domain	Activity
Relationships / engagements	• Engagements with foreign entities - that *have **not been** evaluated* by delegated authorities and deemed to be compliant to the Foreign Interference Transparency Scheme (FITS), Defence Trade Controls Act, International Sanctions and other foreign relations obligations that may be imposed by Government • Third parties where no contractual agreement exists or where insurance is limited
Academic & student engagement	• Engagements with foreign entities – *as above* • Compliance with regulators or funders – TEQSA, ESOS, HESA • Contract cheating / plagiarism • Third parties delivering University content • Availability / adequacy of student placements • Global mobility programs & travel
Research	• Engagements with foreign entities – *as above* • Research involving non-human primates, gene technology, biohazardous material, quarantine of goods, minors (children < 18 years of age), personal and sensitive data • Plant or seed research involving genetically modified organisms (GMOs) or tobacco products • Activities requiring handling or storing of chemical, biological, security sensitive or radiological agents • Cold storage of research material / samples

	• IP and commercialisation
Workplace health & safety	• Work involving chemical, biological, radiological, asbestos or animals • Contractors • Plant and equipment (including electrical, firearms, drones) • Field activities • Travel, including travel to high risk destinations
People	• Personnel, Titleholders, succession planning, skills shortages • Staff recruitment from overseas • Industrial relations • Discrimination and harassment
Financial	• Fraud • Budget over run • Taxation • Leases • Supply chain interruption • Currency fluctuations / global economic impacts
Governance	• University Policy, project management, business continuity, reputation • Decisions undocumented / due diligence not evident • Culture & behaviour • Complaints
Infrastructure / environment	• Physical assets & facilities • Sustainability & conservation • Environmental management or damage
Information technology	• Demand / future requirements • Pace & agility • System incompatibility • Loss or corruption of data • Hardware, software or server failure
Information	• Data protection / privacy • IP & Commercialisation • Knowledge management • Plagiarism • Management of information assets / records
Legal / contractual	• Breach of legislative requirements • Poor contract management • Ethics
Geopolitical	• Natural disasters • Pandemics • Political unrest / leadership vacuum

Project Risks are those activities, investments, relationships, partnerships, proposals, business planning and decision-making being planned, assessed, proposed, implemented or executed, that commit the University to a relationship, undertaking, contract, agreement, obligation, the deployment of natural, built or technology resources or a financial liability. Project risks should have a business case in accordance with Finance and Procurement Services *Investment Framework*. Refer to *Figure 6 Project / Activity Lifecycle* in Step 1: Establish the Context.

Formal documentation of risks is done in the ***University Risk Register***. The register should record the context of the risk, the risk assessment, and risk rating with reference to the University Risk Matrix. The risk matrix provides a standard approach to measuring risk within a single nomenclature and parameters.

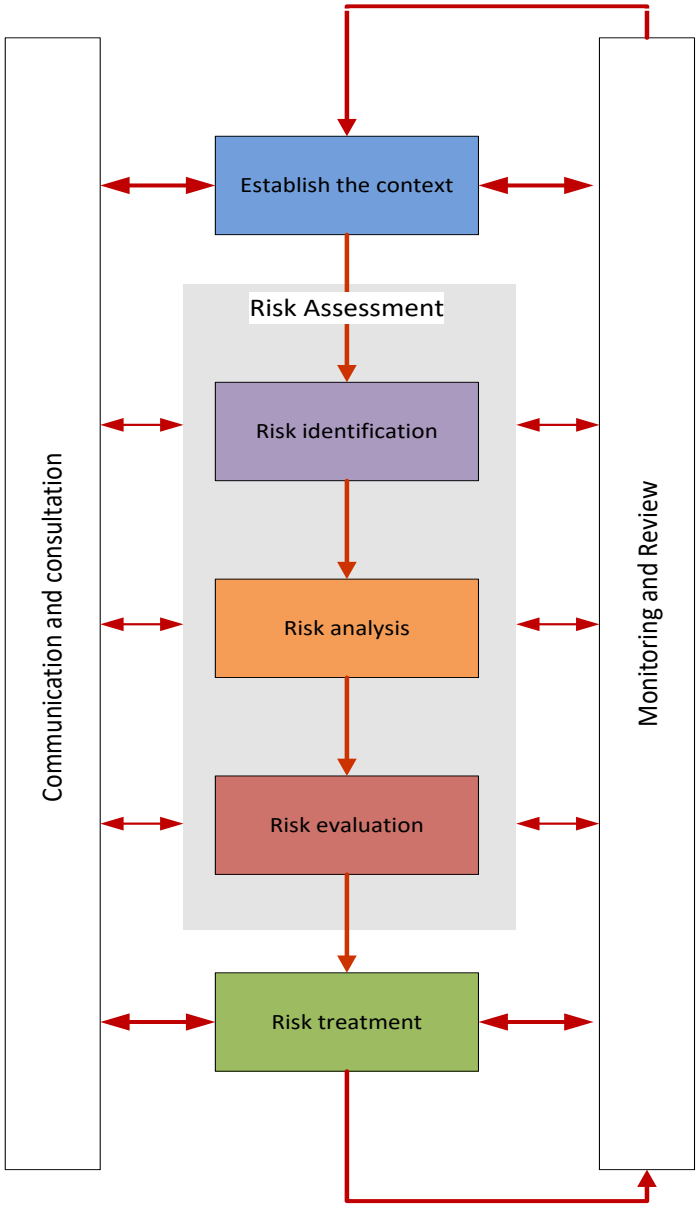
Refer to Step 3: *Analyse the Risk* and *Recording the Risk Management Process* for further information.

PART C: METHODOLOGY / PROCESS

12. Overview

Risk management is a necessary consideration each time a decision is made – whether to make an investment or binding commitment, start a new project, develop a new relationship, or invest in or acquire assets in plant, equipment, technology or infrastructure. Activities and decision-making must be aligned with objectives and outcomes that help the University reach its strategic goals or successfully execute operational plans. This is risk management. The process and steps described in this section are intended to help *manage risk*, taking into account the unique and special environments in which the University works.

The risk management steps include:



Step 1: Establish the context:
- Define the scope of enquiry/objectives: ie what activity, decision, project, program, issue requires analysis
- Identify relevant stakeholders/areas involved or impacted
- Internal and/or external environment/ factors

Step 2: Identify the risk:
Identify / assess
- What could happen?
- How and where it could happen?
- Why it could happen?
- What is the impact or potential impact?

Step 3: Analyse the risk:
- Identify the causes, contributing factors and actual or potential consequences
- Identify existing or current controls
- Assess the likelihood & impact/ consequence to determine the risk rating

Step 4: Evaluate the risk:
- Is the risk acceptable or unacceptable?
- Does the risk need treatment or further action?
- Do the opportunities outweigh the threats?

Step 5: Treat the risk:
- If existing controls are inadequate identify further treatment options
- Devise a treatment plan
- Seek endorsement & support for treatment
- Determine the residual risk rating once the risk is treated

Communicate & consult: at all stages of the process
- Ensure those responsible for managing risk, and those with vested interests, understand the basis on which decisions are made, why particular treatment options are selected or why risks are accepted/tolerated

Monitor & review: continually check
- Effectiveness of risk controls and/or treatments
- Changes in context or circumstances, and
- Document & report this activity accordingly

Figure 5: Risk Management Process

13. Step 1: Establish the context

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

The risk management process applies equally to risks that arise at an enterprise wide or strategic level, at an operational or day-to-day business level or for new projects, partnerships, and new initiatives.

Any proposed project, partnership, or initiative should actively consider risk and formally document the assessment ***throughout the lifecycle*** of the activity:

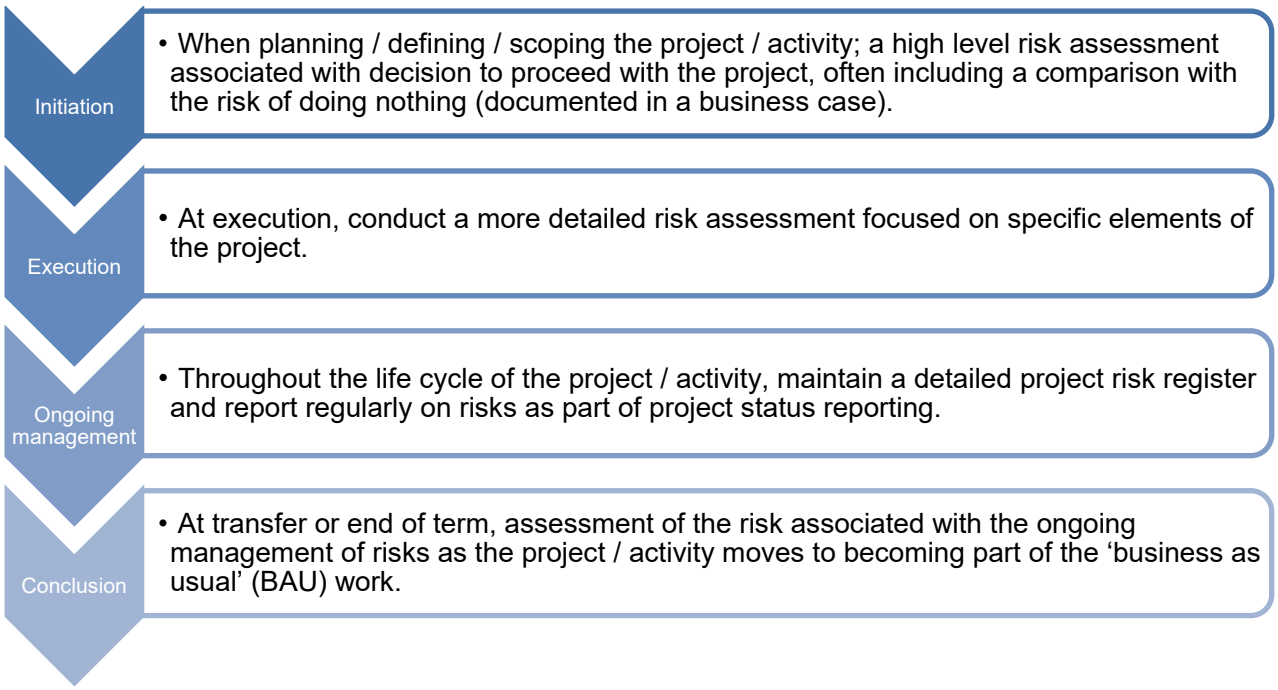


Figure 6: Project / Activity Lifecycle

It is recognised that individual and 'fit for purpose' processes may be established to assess and manage the specific risks of an individual project or initiative, but that further risk management work is required when the project moves to an operational level.

Identify the purpose and objectives right at the beginning; focus on this at the outset to avoid being overwhelmed by details and data.

The Process:

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

- **Define the broad objectives.** Identify *the reason* for the risk assessment – perhaps a change in law, a request from an external auditor or regulator, an operational change or review, or a mandatory assessment / requirement.

- **Identify the relevant stakeholders**. Aim for an appropriately inclusive process from the outset: be sure to identify any areas that are, or might be, impacted - and seek their input. Make sure that appropriate delegations are being exercised even at this early stage.

- **Gather background information.** Having proper information is important. Ask the right people and identify the information that is available. Sometimes it is useful to identify information that is not available (immediately) but may be necessary.

When gathering information, consider or refer to:

Strategic plans, investment plans, business plans	Audit reports, inspections, site visit reports
Research proposals	Previous contracts / agreements
Proposals for new or renewed engagements with foreign entities	Outcomes from previous foreign engagement compliance reviews
Personal experience (of staff, students, others)	Corporate knowledge or historical records
Previous event investigations or reports	Surveys, questionnaires and checklists
Insurance claim reports	Local or international experience
Expert judgment / industry advisory groups (internal University expertise &/or external expertise)	Structured interviews or focus group discussions

Where possible, consider both the strategic context and operational context, so that a complete picture is obtained.

Establishing the context

- sets the framework within which the risk assessment should be undertaken,
- ensures the reasons for carrying out the risk assessment are clearly known, and
- provides the backdrop of circumstances against which risks can be identified and assessed.

*The next three steps – Identify the risk, Analyse the risk and Evaluate the risk - form the **Risk Assessment** phase of the of the risk management process.*

14. Step 2: Identify the risk

Identify the risks that might have an impact on the objectives of the University, or relevant Faculty, School, Branch, area or entity.

Identify sources of the risk, areas of impact, events (including changes in circumstances) and their causes and potential consequences. Describe those factors that might create, enhance, prevent, degrade, accelerate or delay the achievement of your objectives.

Aim to also identify the issues associated with not pursuing an opportunity; that is, what is the risk of doing nothing and missing an opportunity?

Risk identification

Involves identifying sources of risk, areas of impact, events and their causes and consequences.

In identifying the risk, consider these kinds of questions:

- **What could happen:** what might go wrong, or what might prevent the achievement of the relevant goals or objectives? What events or occurrences could threaten the intended outcome(s)?

- **How could it happen:** is the risk likely to occur at all or happen again?
  If so, what could cause the risk event to recur or contribute to it happening again?

- **Where could it happen:** is the risk likely to occur anywhere or in any environment / place? Or is it a risk that is dependent on the location, physical area or activity?

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

- **What might be the impact:** if the risk were to eventuate, what impact or consequences would or might this have? Will the impact be felt locally or will it impact on the whole University?

  Areas of impact to consider include: education or research program / activity; human impact; service delivery; financial consequences; compromise to legal or contract compliance; and adverse impact on brand and reputation for failure to meet or achieve our strategic objectives.

- **Who does or can influence this partnership, program, project or event? How much is within the University's control or influence?** Make sure that those with delegations, control, influence, resources and budgets are at least informed if not actively involved. This becomes more important when considering the treatments for the risk (see Step 5: *Treat the Risk*).

Wherever possible, provide quantitative and/or qualitative data to assist in describing the risk or to support the risk rating. Sources of information may include past records, staff expertise, industry practice, literature and expert opinion.

15. Step 3: Analyse the risk

Develop a detailed understanding of the risk.

Once the risk has been identified and the context, causes, contributing factors and consequences have been described, look at the strengths and weaknesses of existing systems and processes designed to help control or mitigate the risk. Knowing what controls are already in place, and whether they are effective, helps to identify what - if any - further action is needed.

Process:

- **Identify the existing controls** – determine what controls are already in place to mitigate the impact of the risk. Controls may be strong or weak; they can be measureable and repeatable. Controls may include legislation, policies or procedures, staff training, segregation of duties, personal protective measures and equipment, and structural or physical barriers (e.g. setting up IT firewalls or guards around machinery).

- Once the controls have been identified, and their effectiveness analysed, an assessment is made of the likelihood of the risk occurring and the consequence if the risk were to occur. This produces an accurate, albeit subjective, assessment of the level of risk - or risk rating - and helps in the next step to determine whether risks are acceptable or need further treatment.

- **Assess the likelihood** – the likelihood of the risk occurring is described as *rare, unlikely*, *possible*, *likely*, or *almost certain* to occur.

- **Assess the consequence** – the consequences or potential impact if the risk event occurred are described as *insignificant*, *minor*, *moderate*, *major* or *extreme*.

- The assessment of likelihood and consequence is mostly subjective, but can be informed by data or information collected, audits, inspections, personal experience, corporate knowledge or institutional memory of previous events, insurance claims, surveys and a range of other available internal and external information.

Controls do not always require something special

Often, controls are already present as a natural part of the management of an issue or area, or can be embedded into normal management practices.

Example: Having a supervisor in a student lab session, having procedures in place and ensuring students have adequate instruction on safety issues, are all controls to minimise the risk associated with laboratory hazards.

- **Rate the level of risk:** use the University Risk Matrix (refer Appendix 6 or online at https://www.adelaide.edu.au/legalandrisk/self-service#risk-management) to assess the likelihood and consequence levels; the risk matrix then determines whether the risk rating is *low*, *medium*, *high* or *extreme*.

  The University Risk Matrix also specifies the management action required for the various risk ratings.

16. Step 4: Evaluate the risk

Decide whether the risk is acceptable or unacceptable. Use your understanding of the risk to make decisions about future actions.

Decisions about future actions may include:

- not to undertake or proceed with the event, activity, project or initiative
- actively treat the risk
- prioritising the actions needed, if the risk is complex and treatment is required
- accepting the risk

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

The *attitude, appetite* and *tolerance* for risk is likely to vary over time, across the University as a whole and for individual Faculties, Schools, Divisions, Branches and Controlled Entities.

A risk may be acceptable or tolerable in one or more of the following circumstances:

- No treatment is available
- Treatment costs are prohibitive (particularly relevant with lower rated risks)
- The level of risk is low and does not warrant using resources to treat it
- The opportunities involved significantly outweigh any threats

A risk is regarded as acceptable or tolerable if the decision has been made not to treat it (in accordance with the next step, Step 5: *Treat the risk*).

Accepting or tolerating a risk *does not mean* that the risk is insignificant. Risks that are considered acceptable or tolerable may still need to be monitored.

When conducting a risk assessment, there are generally lots of potential consequences identified. This is not necessarily a problem as a number of these can be addressed by the risk treatments, or they may not need any specific action.

Risk attitude

An organisation's approach to assess and eventually pursue, retain, take or turn away from risk

Risk appetite

The amount and type of risk that an organisation is willing to pursue or retain

Risk tolerance

An organisation's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives

The previous three steps described – *Identify the risk*, *Analyse the risk* and *Evaluate the risk* - form the **Risk Assessment** phase of the risk management process.

The **Risk Assessment** process is well suited to a structured and systematic approach. For complex or more widespread issues a facilitated workshop format involving participants with different perspectives is often helpful and using an experienced facilitator to lead the discussion can help provide another objective perspective.

Facilitated workshops can be requested by contacting the Legal and Risk Branch via helpdesklegal@adelaide.edu.au

17. Step 5: Treat the risk

Ensure that effective strategies are in place to minimise the frequency and severity of the identified risk. Develop actions and implement treatments that aim to control the risk.

Once the risk assessment phase is complete, identify the options for treatment - if there are any; otherwise tolerate the risk. Where options for treatment are available and appropriate, record those treatment options as part of the risk treatment plan.

Treatment options not applied to the source or root cause of a risk are likely to be ineffective and promote a false belief within the organisation that the risk is controlled.

Risk treatment

The process taken to modify the risk

Process:

- **Decide if specific treatment is necessary** or whether the risk can be adequately treated in the course of standard management procedures and activities; that is, embed the treatment into day-to-day practices or processes. In assessing what treatments could be implemented, it is useful to consider ways in which standard practices already serve as a control, or ways in which those standard practices could be modified to adequately control the risk.
- **Work out what kind of treatment is desirable for this risk –** determine what the goal is in treating this particular risk; is it to avoid it completely, reduce the likelihood or consequence, transfer the risk (to someone else such as an insurer or contractor) or accept the level of risk based on existing information? The type of risk treatment chosen will often depend on the nature of the risk and the tolerance for that risk.
- **Identify and design a preferred treatment option** once the goal of treatment is known.
    - If the goal is to ***reduce the likelihood or possibility*** of the risk, then you may need to adjust what is happening or might be planned: successfully altering the approach will depend on identifying the causes of the threat and the causal links between the threat and its impact – both of which should have been identified in the risk assessment phase.
    - If it is not possible to change the approach of the project or activity, then it may be possible to take some other intervening action to mitigate the event's occurrence or reduce the likelihood of the threat.
    - Understanding the nature of the risk event and how it occurs will make it easier to identify any possible intervening actions that would operate to reduce the risk.
    - If the goal is to ***reduce the consequence or impact*** of the risk, then contingency plans might be required to respond to a threatening event if it occurs. This planning may be undertaken in combination with other controls – that is, even if steps have been taken to minimise the likelihood of the risk, it may still be worthwhile to have a plan in place to reduce the consequences if the event actually occurs.
    - If the goal is to ***share the risk***, then involving another party, such as an insurer or contractor, may help. Risk can be shared contractually, by mutual agreement, and in a variety of ways that meet all parties' needs. Any such arrangement should be formally recorded – whether through a contract or agreement or by letter.

      Sharing the risk does not remove our obligations and does not avoid us suffering consequential damage if something unexpected happens or something goes wrong.

Treatment options

- *Avoid the risk by not starting or continuing an activity*
- *Take or increase risk in order to pursue an opportunity*
- *Remove the risk source*
- *Change the likelihood*
- *Change the consequence*
- *Share the risk e.g. through Insurance, contracts, financing*
- *Retain the risk by informed decision*

- If the risk is so significant that the goal is to ***eliminate or avoid it altogether*** then the options are limited to changing the project materially, choosing alternative approaches or processes to render the risk irrelevant or abandoning the activity or partner or program. It is not often that a risk can be eliminated completely and balance is an important part of the risk assessment exercise (please note: this does not refer to safety type risks or hazards).
- Sometimes, a decision is made to ***accept or tolerate*** the risk, due to the low likelihood or minor consequences of the risk event, or the fact that the cost of effectively controlling the risk is unjustifiably high or that the opportunity outweighs the risk. The University acknowledges that in pursuing its strategic objectives *measured risk taking* is both acceptable and appropriate. However, in these instances the decision to accept risk should be carefully documented, so that a record is available for future reference (or evidence) if the risk does eventuate. Thought should also be given to contingency planning in order to deal with and reduce the consequences, should they arise.

- **Evaluate treatment options** and assess their feasibility relative to the tolerance for risk. Do the controls selected appear to have the desired treatment effect (that is, will they stop or reduce what they are meant to stop or reduce)?
  - Will the controls trigger any other risks*? For example, a sprinkler system installed to counter fire risk may cause water damage, presenting a different risk requiring consideration or management.*
  - Are the controls beneficial or cost efficient? Does the cost of implementing the control outweigh the cost that would flow from the event occurring without the control in place? Overall, is the cost of implementing the control reasonable for this risk?

  The cyclical process of treating a risk, deciding whether residual risk levels are tolerable and assessing the effectiveness of that treatment are all case-by-case assessments that depend on a good understanding of the risk and a focus on the end objective of the activity being assessed.

- **Document the risk treatment plan.** Once the treatment options have been identified, a risk treatment plan should be prepared (NB. These can be easily generated through the University risk register once a risk is recorded). Treatment plans should identify responsibilities for action, time frames for implementation, budget requirements or resource implications, performance measures and review process where appropriate. The review process should monitor the progress of treatments against critical implementation milestones.

- **Implement agreed treatments**. Once any options requiring authorisation for resourcing, funding or other actions have been approved, treatments should be implemented by those identified as having the responsibility to do so. The person assigned with the primary responsibility for the risk is ultimately accountable for the treatment of the risk.

- **Once the risk has been treated, assess the level of residual risk.** Even when a risk has been treated and the controls are in place the risk may not be completely eliminated. The level of *residual risk* refers to the likelihood and consequence of the risk occurring after the risk has been treated. Once implemented, treatments provide or modify the controls. If the controls are effective, the residual risk rating should be lower than the original risk rating.

  The residual risk should be documented, monitored and reviewed. Where appropriate, further treatment might be prudent. Having a good awareness of residual risk is important in monitoring and reviewing risk on an ongoing basis.

18. Monitor and review

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

To ensure structured reviews and regular reporting occurs, each local area is encouraged to identify a process that allows key risks within their area to be monitored.

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

Monitoring & review is a planned part of the risk management process

The University's changing and evolving environment means the source and context of risks, risk tolerance and risk controls may change over time.

Process:

- **Continuous monitoring:** once risks have been identified, recorded, analysed, and the agreed treatments have been implemented, an appropriate monitoring and reporting regime needs to be established to provide assurance that the treatment has been effective and now helps to control the risk. Some risk treatments will of course become embedded into daily practices and methods of work.

  The frequency of review will depend on the risk rating, the strength of controls and the ability to effectively treat the risk. Each of us has a role to play in continually monitoring known or emerging risks and regularly checking or ensuring that controls are in place and are being used.

- **Faculty/School, Division/Branch or Controlled Entity Management review:** managers need to ensure there is a process for reviewing risk profiles and activities in their area of responsibility. Wherever possible, risk management should become an agenda item on management meetings or committees and avoid the need for separate processes.

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

- **Internal audit:** the University's internal audit program provides for a review of systems, policies and process assurance and compliance. The auditors apply a risk-based approach to the audit program and help bring a measure of independence and external perspective to the University Risk Management Framework.

- **External audit:** the University is audited annually by the South Australian Auditor General. That external audit covers financial, governance, contracting, IT and risk management systems and processes. Management and staff may be required to respond to the risk management activities involved with these audits. Other audits occur from time to time and are imposed through contracts, compacts, and Federal and State legislation.

- **Local Coordinators or Risk Facilitators:** for staff active in the monitoring and review of risks, being able to access and use the University Risk Register (URR) may be required. To apply for access to the URR please contact the Director Risk Services for training and support.

  (*Refer to the contact details in the* Appendix*).*

Formal Risk Reporting

Formal risk reporting is an important part of being able to demonstrate the effectiveness of the risk management program. The University is required to report to various internal and external bodies and stakeholders. To achieve this the University needs to be informed about risks in a timely manner and to be able to access - and reproduce - those risk assessments easily.

Therefore, the Risk Management Policy requires Material Risks to be identified, reviewed and reported to governance and management at appropriate intervals, having regard for the potential positive or negative impact on the University's pursuit and achievement of strategic, business and operational plans.

The Policy also requires extreme and high risks (assessed by reference to the University Risk Matrix) to be reported to the relevant Risk Owners for appropriate escalation and treatment.

This formal reporting process assists / enables:

- Executive Deans and Senior Managers (Vice-Presidents and Chief Operating Officer) to report annually on extreme and high risks to the University Risk Management Committee; and
- Board Directors / Chief Executives / General Managers of Controlled Entities to report annually on the entities risk management profile to the nominated Standing Committee of Council.

Formal risk reporting is encouraged through the University Risk Register, or other appropriate format. Formal reports should identify new risks, detail the progress with treating existing risks and report outcomes from the monitoring and review process.

Annual risk reporting should confirm that all risks relevant to the area of responsibility are being adequately and appropriately managed. In addition, any risk verified as an extreme risk will require a risk assessment and management plan to be prepared by the Risk Owner for the Vice-Chancellor.

Extreme and high risks are overseen by the University Risk Management Committee (URMC). Responsive and appropriate action will be agreed between the person with primary responsibility for the risk (Risk Owner) and the appropriate Senior Manager (or Controlled Entity where relevant). Medium and low risks need to be managed by the local area and monitored and reviewed locally as necessary.

Having a formal structured reporting process enables the University to confirm that:

- the risk management framework is effective;
- individuals are doing what should be done to assess and manage risks; and
- those accountable for risks are answerable for managing the risks.

Risk management records should be traceable

In the risk management process, records provide the foundation for improvement in methods and tools, as well as in the overall process.

Recording the Risk Management Process

To ensure that risk management is effective, and to provide evidence of a *demonstrable* risk management system, it is important to have a documented formal record of the risk assessment and outcomes. The tool for recording risks in the University, and across its Controlled Entities, is the **University Risk Register**. A risk register is simply a documented record of the identified risks, their significance or rating, and how they are managed or treated. The University's risk register is an electronic web based tool that enables the recording of risks and facilitates the printing of risk reports and summaries.

All areas of the University, and each of the Controlled Entities, are encouraged to formally record and document their risks within the risk register. In this way, a *risk profile* or description of the types and significance of risks will evolve. Risk profiles will vary greatly by Faculty, School, Branch, Division or Controlled Entity and will evolve over time.

A risk profile *is a description of any set of risks. Over time the types and significance of risks will evolve.*

There is value in each local area having, or compiling, a formal and consolidated risk profile, as it helps to determine how much time and effort should be put into risk management and how frequently monitoring and reviews should be conducted. Even for areas in the University that might consider themselves to be '*low risk*', the risk management process can contribute significantly to business planning, improving the responsiveness of the area to crises or threats and responding to opportunities in an informed and measured manner.

With all areas gradually contributing to and using the risk register, an invaluable body of institutional knowledge will evolve, further strengthening the University's demonstrable risk management processes and maximising the University's efforts and strategies.

Project risks

The specific risks associated with an individual project or initiative, should be captured locally ***throughout the lifecycle*** of the activity as per Establish the Context section on page 17. These risks should be recorded locally in an Excel spreadsheet or similar product (e.g. SmartSheet); an overarching, generic risk in the University's risk register should be considered.

What to record

When documenting a risk assessment record the following information within the register:

- A description of the risk (setting the context)
- Causes or contributing factors
- Consequences (impacts) of the risk – actual or potential
- Current controls in place that help manage the risk
- An assessment of the likelihood and consequence based on current or existing controls, to rate each risk
- Further actions or treatments needed to address the risk
- Any progress updates as the treatments are implemented
- Results from monitoring and review, including effectiveness of controls

By formally recording risks we

- *commit to continuous learning;*
- *obtain benefits for re-using information for management purposes;*
- *minimise costs & efforts of creating & maintaining records;*
- *maximise access & retrieval of information; and*
- *comply with retention periods; and recognise the sensitivity of the information.*

Printing risk records: the University Risk Register can automatically generate Risk Summary Reports. These reports, which reflect the risk profile for the area, can be used for local area reporting and to supplement formal/annual reports. The University Risk Register can also generate Risk Management Reports and Risk Treatment Plans for individual risks. More information about the University Risk Register is available in Appendix 5 and on the Legal & Risk website.

19. Communicate and Consult

Effective communication and consultation is essential to ensure that those responsible for implementing risk management, and those with a vested interest, understand the basis on which decisions are made and the reasons why particular treatment options are selected.

Communicate and consult with internal and external stakeholders during any and all stages of the risk management process, particularly when plans are being first considered and when significant decisions need to be made.

Risk management is enhanced through effective communication and consultation when all parties understand each other's perspectives and, where appropriate, are actively involved in decision-making.

Methods of communication and consultation may include:

- meetings;
- distribution of minutes;
- reports;
- online communication systems and learning packages;
- induction packages;
- newsletters;
- circulation lists;
- flow charts; and
- staff awareness and education sessions / staff training.

Communicate and consult

Use a variety of methods to ensure that those responsible for implementing risk management are kept properly informed.

A collaborative and consultative team approach - through co-creation - is more likely to:

- Help establish the context appropriately;
- Ensure the interests of all stakeholders are understood and considered;
- Ensure that risks are adequately identified;
- Bring together different areas of expertise when assessing or analysing risks;
- Ensure that different, and sometimes opposing, views are appropriately considered when defining risk criteria and in evaluating risks;
- Help secure endorsement and support for a treatment plan; and
- Enhance any change management processes associated with the risk.

PART D: APPENDIX

In this section additional information is provided to assist staff with risk management, and to encourage a consistent and comprehensive language and approach to managing risk across the whole University.

The information includes:

- Glossary of key risk management terms
- Risk management relevance in University context
- University Risk Management Responsibilities
- University Risk Register: a basic introduction to reporting a risk
- University Risk Matrix: with the consequence and likelihood tables

Other tools and resources can be found on the University website:
https://www.adelaide.edu.au/legalandrisk/risk-management

For more information on risk management in your local area, contact your Head of School or Branch, or your line manager or supervisor.

For assistance in applying risk management practices, for training and access to the University Risk Register, or for clarification on any content in this document, please contact: helpdesklegal@adelaide.edu.au

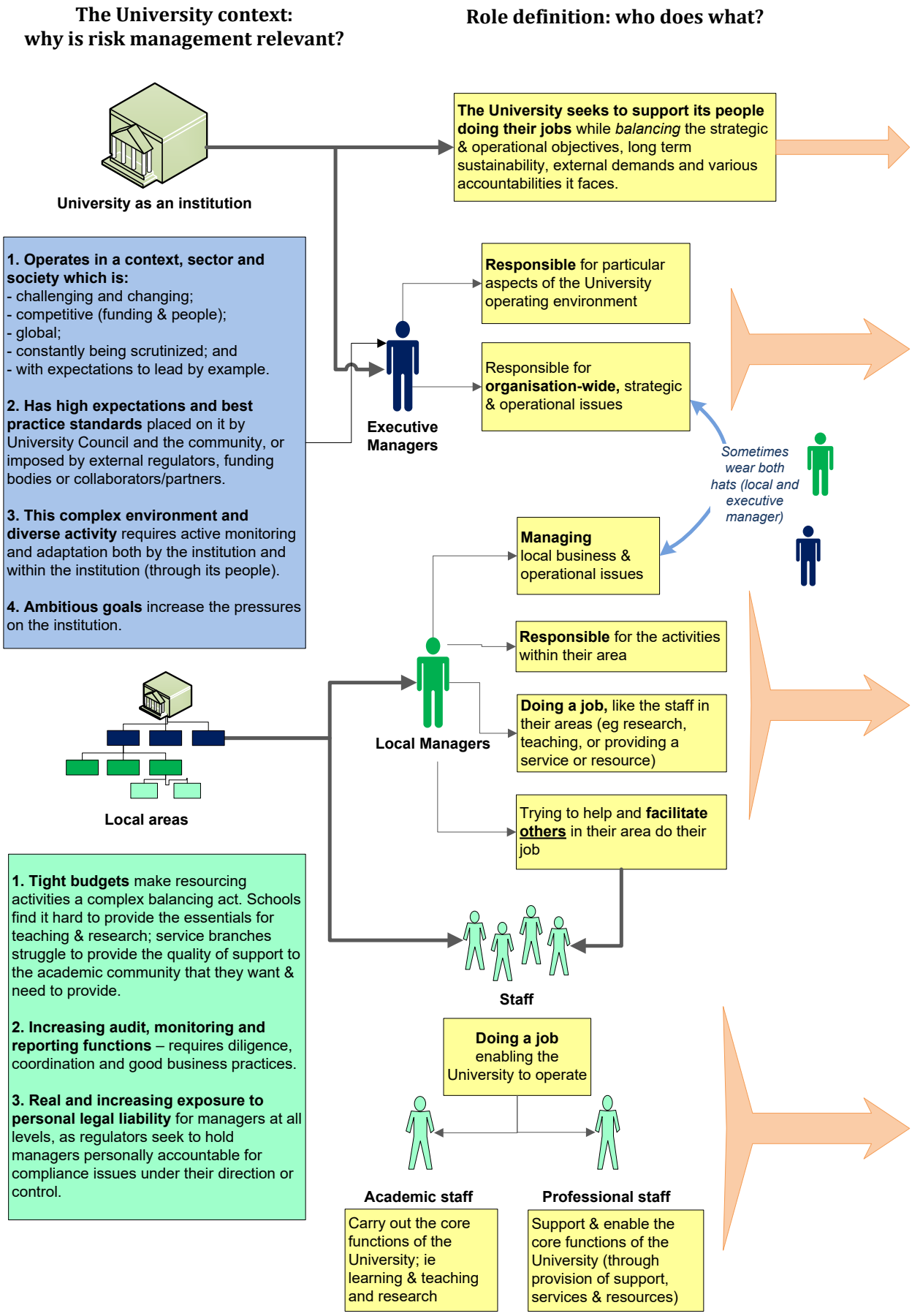
20. Appendix 1: Glossary of Terms

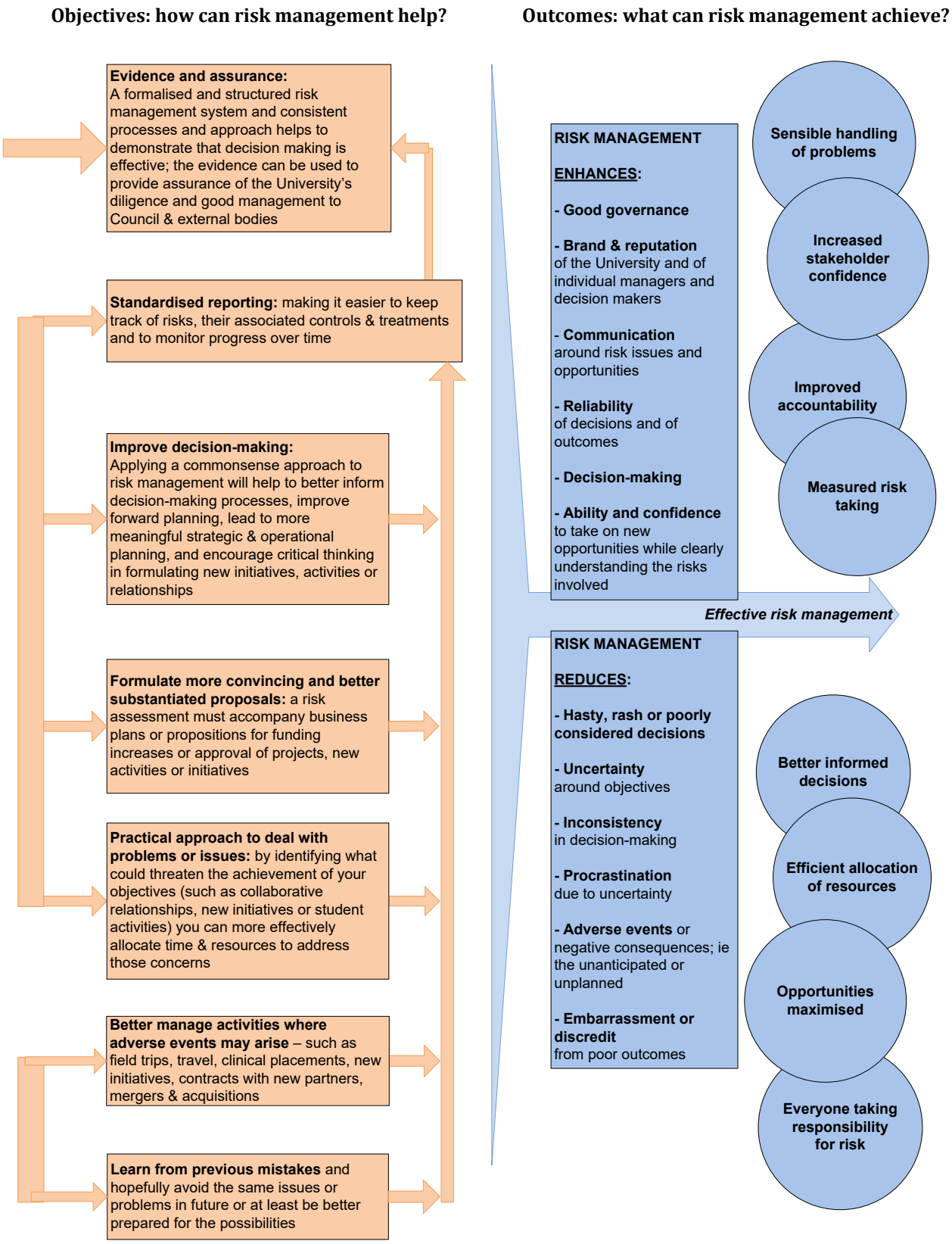
Risk	Effect of uncertainty on objectives • *An effect is a deviation from the expected; positive or negative;* • *Objectives may have different aspects and can apply at different levels;* • *Often characterised by reference to potential events and consequences or a combination of these;* • *Often expressed in terms of a combination of an event and the associated likelihood of occurrence;* • *Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence or likelihood.*
Material risks	Are those that may adversely affect the University's ability to deliver on its statutory objective or to deliver on its broader strategy and business plans
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 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 risks
Stakeholder	Person or organisation that can affect, be affected by or perceive themselves to be affected by a decision or activity, or persons having power or influence over the decision or activity.
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
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation
Risk identification	Process of finding, recognising and describing risks
Risk description	Structured statement of risk usually containing four elements: sources, events, causes and consequences
Risk source	Element which alone or in combination has the intrinsic potential to give rise to risk
Event	Occurrence or change of a particular set of circumstances. An event: • *can consist of one or more occurrences, and can have several causes;* • *can consist of something not happening;* • *can sometimes be referred to as an 'incident' or 'accident'; and* • *where there are no consequences, can also be referred to as a 'near miss', 'incident', or 'close call'.*
Risk owner	Person or entity with the accountability and authority to manage a risk
Risk analysis	Process to comprehend the nature of risk and to determine the level of risk: • *Provides the basis for risk evaluation and decisions about risk treatment;* • *Includes risk estimation.*
Likelihood	Chance of something happening In risk management terminology, likelihood is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as probability or a frequency over a given time period)

Consequence	Outcome of an event affecting objectives, which can lead to a range of consequences. The consequences can • *be certain or uncertain;* • *have positive or negatives effects on objectives;* • *be expressed qualitatively or quantitatively;* and • *escalate through knock-on effects.*
Risk matrix	Tool for ranking and displaying risks by defining ranges for consequence and likelihood
Level of risk	Magnitude of a risk or combination of risks expressed in terms of their consequences and their likelihood. Also known as the risk rating.
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 attitude	Organisation's approach to assess and eventually pursue, retain, take or turn away from risk
Risk appetite	Amount and type of risk that an organisation is willing to pursue or retain
Risk tolerance	Organisation's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives
Risk acceptance	Informed decision to take a particular risk • *Acceptance can occur without risk treatment or during the process of treatment* • *Accepted risks are subject to monitoring and review*
Risk treatment	Process to modify risk. Risk treatment may include one or more of the following options: • *avoiding the risk by deciding not to start or continue with an activity that gives rise to the risk;* • *taking or increasing risk in order to pursue an opportunity;* • *removing the risk source;* • *changing the likelihood;* • *changing the consequence;* • *sharing the risk with another party or parties (including contracts and risk financing); and / or* • *retaining the risk by informed decision*
Control	Measure put in place to modify the risk. Controls: • *include any process, policy, device, practice, or other actions which modify risk; and* • *may not always exert the intended or assumed modifying effect.*
Residual risk	Risk remaining after risk treatment. Residual risk: • *can contain unidentified risk; and* • *is also known as 'retained risk'.*
Resilience	Adaptive capacity of an organisation in a complex and changing environment
Monitoring	Continual checking, supervising, critically observing or determining the status in order to identify any deviation from the required or expected performance level
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives
Risk reporting	Form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management
Risk register	Record of information about identified risks
Risk profile	Description of any set of risks

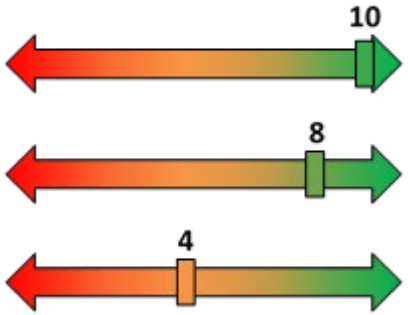
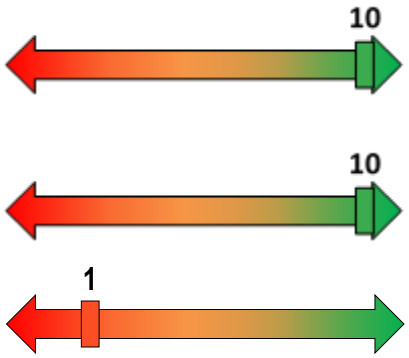
Key source: ISO Guide 73: 2009 Risk Management – Vocabulary

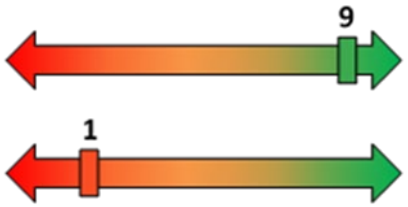
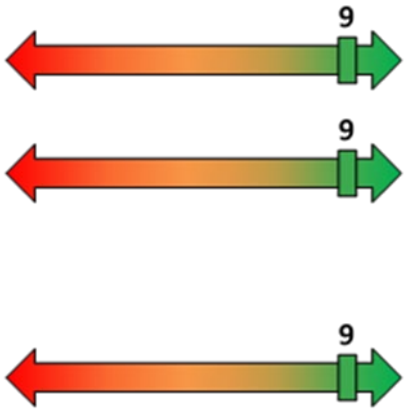
21. Appendix 2: Risk Management Relevance in University Context



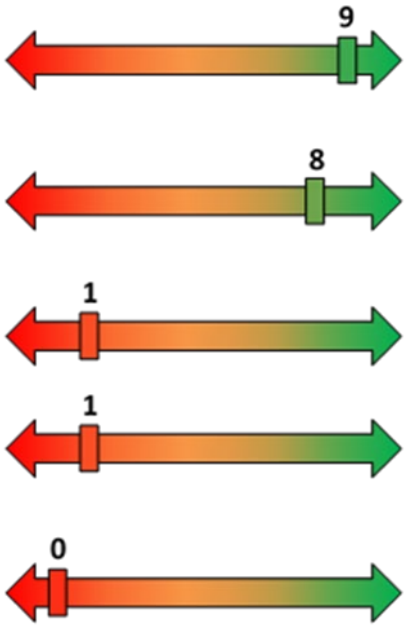


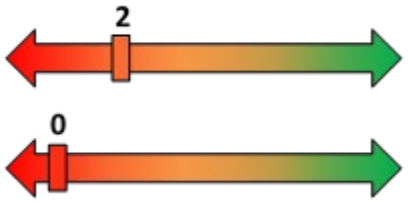
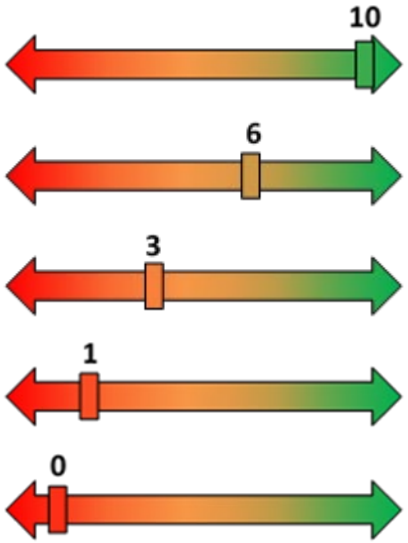
22. Appendix 3: University Risk Tolerance Statements

Risk Category / key indicator	Level of Risk Tolerance	Risk Tolerance Statements
	Lowest to highest **0 = lowest tolerance** **10 = highest tolerance**	
Pursuit of academic mission		The University recognises that creative and enterprising people will thrive in a culture that encourages ambition, facilitates participation, and celebrates success. We aspire to a culture founded in excellence, respect, intellectual curiosity and collegial decision-making. The University has a ***balanced to entrepreneurial*** appetite for risk in pursuing the advancement of learning and knowledge, including the provision of university education (statutory objective / academic mission). ***Highest*** tolerance for Academic Freedom, recognising that the expression of Academic Freedom must always be respectful. ***High*** tolerance for our institutional autonomy, and the decisions made to enhance our strategic mission or protect our reputation. ***Lower*** tolerance for decisions made without appropriate information and evidence, or without broad consultation.
Strategic growth		The University's growth and development is set out in the Strategic Plan, *Future Making*. The 5 key pillars align global connectivity, research scholarship and human potential with the social, intellectual and economic needs of young leaders locally, nationally and internationally. The University has an ***entrepreneurial*** appetite for risk towards strategic growth. ***Highest*** tolerance for engaging in proposals, projects and partnerships th*at will* result in highly prepared graduates able to engage globally and become citizens of tomorrow, and/or enhanced learning and teaching and research outputs / income. ***Highest*** tolerance for promoting and supporting start-ups and early capital investment in prospecting and market testing, to deliver the desired markets and products. ***Lowest*** tolerance for engaging in projects, proposals and partnerships without due diligence and appropriate project management and contract stewardship.

Risk Category / key indicator	Level of Risk Tolerance	Risk Tolerance Statements
	Lowest to highest **0 = lowest tolerance** **10 = highest tolerance**	
Student experience		The University is committed to providing a high quality academic and research experience for its students. That commitment extends to the pastoral and cultural aspects of the students experience (including student safety, mental wellness and wellbeing), to ensure that support is available, accessible and appropriate, and that the students are satisfied, and stay engaged and connected with the University and their studies (future alumni). The University has a ***balanced to entrepreneurial*** appetite for risk towards student experience. ***Higher*** tolerance for pursuing activities and projects that result in student engagement, and improve student satisfaction levels and retention rates. ***Lowest*** tolerance for compromises to the agreed minimum standard for an acceptable student learning experience and acceptable research experience.
Research		The University is committed to expanding and diversifying its research programs and industry engagement, the recruitment of high calibre students and staff, while maintaining the student experience and our reputation. At all times, our initiatives must remain ethical and must be appropriately considered in terms of the feasibility of success and the investment required. The University has a ***balanced to entrepreneurial*** appetite for risk towards research. ***Higher*** tolerance for pursuing research opportunities, partnerships and high performing staff that contribute to the translation of research, our reputation of excellence, and enhance our rankings. ***Higher*** tolerance for responding to and accommodating the industry specific (Industry Engagement Partners) appetites for investment in development (R**&D**). ***Higher*** tolerance for systems, philosophy and spaces that activate the maximum benefit of R&D outcomes (utilisation, management of conflict of interest).

Risk Category / key indicator	Level of Risk Tolerance	Risk Tolerance Statements
	Lowest to highest **0 = lowest tolerance** **10 = highest tolerance**	
		***Lowest*** tolerance for engagement with organisations who don't share our values, or from whose association with us will cause unacceptable risk to our reputation and brand, and damage our overall engagement with community.
		***Lowest*** tolerance for compromising the quality of research.
		***Zero*** tolerance for research misconduct, breach of relevant National Codes, fraudulent research, or false publication of research data or material.
Teaching		The University is committed to ensuring a high quality educational program (the product) to meet the future needs of students, employers, industry and the broader community (the people), and to employing high calibre teaching professionals to deliver the programs in a transformative and innovative manner, complying at all times with prescribed Standards and aligned with the expectations of the University's *Academic Performance Expectations* (the how). The University has a ***balanced to entrepreneurial*** appetite for risk towards teaching.
		***Higher*** tolerance for pursuing transformative and innovative teaching programs, (process techniques, recruitment).
		***High*** tolerance for a blended profile of experience or qualifications in the academic / teaching workforce (including people from a non-academic background).
		***High*** tolerance for growing the student cohort (domestic and international) *coupled with a*
		***Low*** tolerance for growing student cohort at expense of students' opportunity to thrive or succeed, and low tolerance for compromising the University internal standards (entry requirements/English language) and compromising the student experience.
		***Lowest*** tolerance to any compromise to academic integrity (permit mistakes).

Risk Category / key indicator	Level of Risk Tolerance	Risk Tolerance Statements
	Lowest to highest **0 = lowest tolerance** **10 = highest tolerance**	
Culture and values		The University values a culture of scholarship, discovery, sustainability, engagement, social justice and integrity and is cognisant of society and community expectations. In balancing competing priorities, the University may need to accept some degree of risk; subject always to ensuring that the potential benefits and risks are fully understood before initiatives are authorised, and that sensible measure to mitigate unacceptable risk are established. The University has a ***balanced*** appetite for risk towards culture and values. ***Higher*** tolerance for meaningful and innovative engagement within the University, and with business, industry and government (BIG), the higher education sector, and the broader community. ***High*** tolerance for transparency and consultation in our communications. ***Lowest*** tolerance for failure to declare conflicts and / or manage conflicts of interest. ***Lowest*** tolerance for inappropriate behaviour or performance that falls short of the University Code of Conduct and agreed values and behaviours, and for poor behaviour or conduct that compromises academic integrity and/or impacts the University and beyond (reputational impact/damage). ***Zero*** tolerance for unethical or unlawful behaviour, or for behaviour / conduct that puts people at risk, or threatens their safety or wellbeing, including threatening, harassing or violent behaviour.
Financial viability		Over and above our willingness to achieve our efficiency targets, we also require a stable financial position to be preserved as outlined in our financial statements / reserves / investments. As we have so many stakeholders relying on us, and we are entrusted with public funds, we must have a strong focus on performance measurement and management. The University has a ***balanced*** appetite for risk towards financial viability. ***Higher*** tolerance for exploring innovative methods for financing our strategic growth objectives.

Risk Category / key indicator	Level of Risk Tolerance	Risk Tolerance Statements
	Lowest to highest **0 = lowest tolerance** **10 = highest tolerance**	
		***Low*** tolerance for non-compliance with accounting standards & Treasurers Instructions, (government financial orders). ***Zero*** tolerance for internal fraud; and the risk may only be accepted where all legislative fraud control requirements are in place and the risk has been reduced to the point where additional controls have negative cost / benefit.
Service disruption		University activities and services operate throughout the calendar year, and at all times of the day. It is important that these activities are high quality, and that the services operate efficiently and effectively when needed. The University has a ***conservative*** appetite for risk towards service disruption. ***Highest*** tolerance for quality services (best available - associated with property, technology, or people). ***Moderate*** tolerance towards manual systems and outages of non-critical internal systems, accepting that some inefficiency may exist and non-critical errors may occur, provided they do not result in a breach of regulation, privacy and/or result in litigation. ***Low*** tolerance towards widespread or sustained industrial action by staff, resulting in service interruption. ***Lowest*** tolerance for service interruption to critical systems, or to systems at critical times; or for service disruption that will impact the safety and wellbeing of students, staff and University community. ***Zero*** tolerance for deliberate misuse or inappropriate use of systems that results in outages to critical systems, or to systems at critical times.
Safety and health		The University is committed to providing a safe workplace for all employees, students, visitors and contractors. The University has a ***conservative*** appetite for risk towards safety and health. ***Low*** tolerance for lost time or injury in areas where there is inherent risk in the nature and location of some activities and environments.

Risk Category / key indicator	Level of Risk Tolerance	Risk Tolerance Statements
	Lowest to highest **0 = lowest tolerance** **10 = highest tolerance**	
		***Zero*** tolerance for death or permanent disability due to departure from, or inadequate safety protocols, and for lost time or injury due to departure from prescribed safety protocols or standards.
Regulatory and compliance		Our reputation for integrity and competence should not be compromised with our key stakeholders, funders, regulators, Government industry partners and community. The University has a ***conservative*** appetite for risk towards regulation and compliance. ***Zero*** tolerance for legal and compliance breaches. While minor breaches may occur from time to time, due to the complexities of business and the environments we operate in, there should be no excuse for careless or intentional departure from regulations or standing operating procedures.
Environmental and social responsibility	 	The University is committed to ensuring sustainable campuses and creating strong platforms for engaging with the community on collective action to protect the environment (and address climate change). The University has a ***balanced to entrepreneurial*** appetite for risk towards environmental and social responsibility. ***Higher*** tolerance for activities and initiatives that prioritise sustainability and diversity, and involve and engage with relevant communities. ***Lowest*** tolerance for adverse environmental impacts or breaches from our activities.

23. Appendix 4: University Risk Management Responsibilities

The responsibility for risk management across the University is as follows:

All University Personnel	• Apply Risk Management principles and processes to both anticipate, and respond to, changing circumstances and events; • Report extreme and high risks (assessed by reference to the University Risk Matrix) to the relevant Risk Owners for appropriate escalation and treatment; and • Contribute to Risk Management activities as directed by University Personnel whose primary responsibility includes managing certain risks.

Risk Owners (both academic and administrative) and where relevant, Controlled Entities (Board and Chief Executive or General Manager)	• Foster and encourage an environment where managing Risk is accepted as a shared responsibility.
	• Ensure that the principles and practices of Risk Management are communicated and embedded into strategic and operational practices, and planning processes.
	• Before approval is given to proceed with a proposal, project, plan or relationship, satisfy themselves that a Risk Assessment has been completed, is sufficient, and will be the subject of ongoing review.
	• Ensure risks rated as extreme or high (assessed in accordance with the University Risk Matrix) are referred to the Director Risk Services for recording in the University Risk Register.
	• Notify new risks considered to be extreme or high risk to the appropriate authority / manager, and the Director, Risk Services.
	• Monitor and manage their risks so that:
	  ○ it is clear who is responsible for actions and treatments;
	  ○ risk controls and treatments are current and effective;
	  ○ extreme and high risks are given appropriate attention and are escalated prudently.
	• For Controlled Entities, report annually to the Director, Risk Services in a time and manner prescribed, for reporting to the relevant University Standing Committee.

Director, Risk Services (within Legal and Risk Branch, Division of University Operations)	• Co-ordinate the University's Risk Management activities in accordance with best practice, this Policy and the Risk Management Framework. • Manage the University Risk Register. • Facilitate the risk reporting process for internal and external bodies / stakeholders.
University Risk Management Committee	• Oversee the University's enterprise and operational Risk Management activities. • Advise on risk strategy, policy, management and escalation. • Report to the Vice-Chancellor, relevant Standing Committees and external agencies and stakeholders as required.
Vice-Chancellor	• As the principal academic and chief executive officer of the University, the Vice-Chancellor and President is responsible for the academic standards, management and administration of the University.
University Council	• Council has a statutory responsibility for overseeing and monitoring the assessment and management of risk across the University including commercial undertakings; and in academic activities, significant commercial activities and Controlled Entities.

24. Appendix 5: University Risk Register

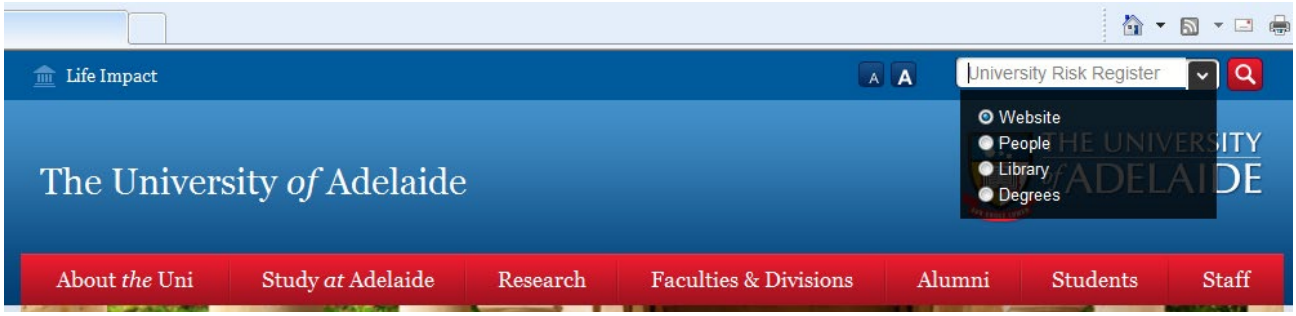
The University Risk Register (register) has been designed to capture risks and facilitate the organisation-wide management and reporting of risks.

The register enables a risk to be logged (recorded), an assessment of risk to be documented, allows for the monitoring and review of risks, and generates risk reports based on standardised templates. In using the register individual areas will, over time, be able to build and maintain their risk profile. The University, as an organisation, is also able to generate reports for those internal committees, auditors and external stakeholders seeking assurance that risks are being managed.

Risk Register

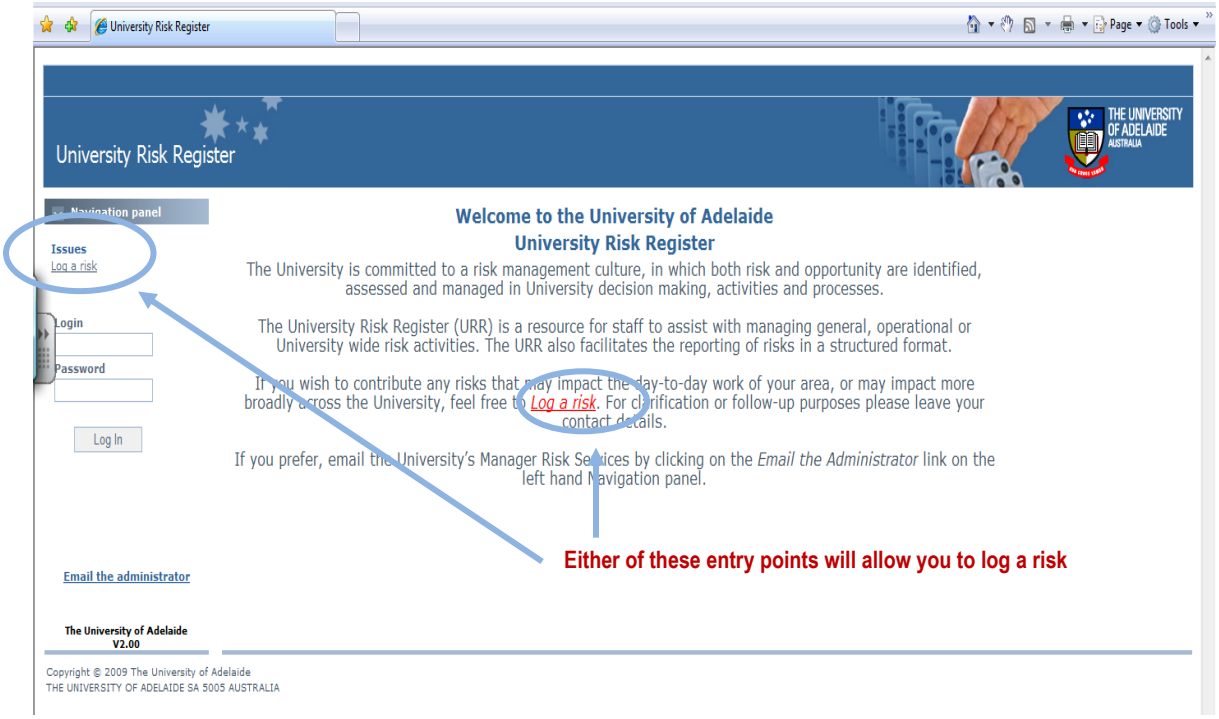
A record of information about identified risks

The register is accessible from the University website at https://www.adelaide.edu.au/legalandrisk/risk-management/university-risk-register.

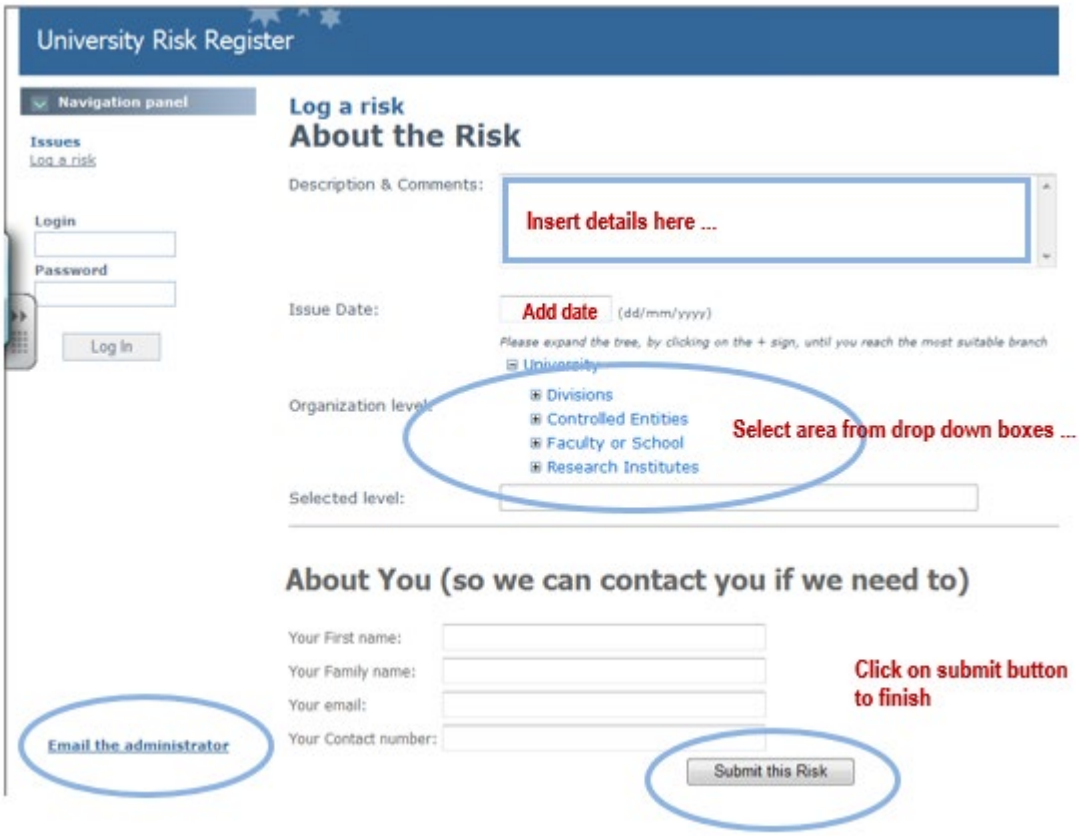


Please note: ***Workplace hazards or safety issues are reported separately***. They are assessed and managed in accordance with the Health Safety and Wellbeing (HSW) Policy and Handbook and under the responsibility of the HSW Team in Human Resources (HR). HSW related risks will be reported through the University Risk Register by HR where and when it is appropriate to do so.

Any staff member can ***Log a Risk*** (i.e. no special login is required) – see below:



When logging a risk you are asked to describe the risk and identify where the risk has been detected or where it sits within the University or Controlled Entity organisational structure:



The 'Description & Comments' field only accepts a limited number of characters or words. If there is too much detail the risk will not be saved.

If you have more information than will fit into the Description & Comments field Email the administrator (see left hand side of screen).

The University encourages the use of the register.

Access to the system is tailored to suit individual business needs. Local areas are encouraged to identify key staff requiring user access. Training and support is available from the Legal & Risk Branch.

Further information is available from http://www.adelaide.edu.au/legalandrisk/risk-management/

25. Appendix 6: University Risk Matrix (Likelihood & Consequence)

Score	Description of likelihood
a Almost Certain	Highly likely to happen, possibly frequently
b Likely	Will probably happen, but not a persistent issue
c Possible	May happen occasionally
d Unlikely	Not expected to happen, but is a possibility
e Rare	Very unlikely this will ever happen

RISK RATING - MANAGEMENT ACTION REQUIRED
• **Extreme risk** = immediate attention & response needed; requires a risk assessment & management plan prepared by relevant senior managers for Vice-Chancellor; risk oversight by Council or nominated Standing Committee or Management Committee
• **High risk** = risk to be given appropriate attention & demonstrably managed; reported to Vice-Chancellor or other senior Executives / Management Committees as necessary
• **Medium risk** = assess the risk; determine whether current controls are adequate or if further action or treatment is needed; monitor & review locally, e.g. through regular business practices or local area meetings
• **Low risk** = manage by routine procedures; report to local managers; monitor & review locally as necessary

RISK MATRIX					
CONSEQUENCE **LIKELIHOOD**	**1** **Insignificant**	**2** **Minor**	**3** **Moderate**	**4** **Major**	**5** **Extreme**
***a* - Almost certain (frequent)**	**M**	**M**	**H**	**E**	**E**
***b* - Likely (probable)**	**L**	**M**	**H**	**H**	**E**
***c* - Possible (occasional)**	**L**	**M**	**M**	**H**	**H**
***d* - Unlikely (uncommon)**	**L**	**L**	**M**	**M**	**H**
***e* - Rare (remote)**	**L**	**L**	**L**	**L**	**M**

Score	Generic impact description	Area of impact - description of consequence					
		Education & Research	Human	Service delivery	Brand & reputation	Finance	Legal / Compliance
5 Extreme	Event or circumstance with potentially disastrous impact on business or significant material adverse impact on a key area	• Unsustainable loss / reduction in student enrolment / retention • Loss of a Faculty • Serious / sustained reduction in research activity / output • Serious / sustained problems reaching a number of student, teaching or research targets • Irreparable impact on relationship with partners / collaborators	• Death or permanent disability • Loss of critical number of key staff impacting on skills, knowledge & expertise • Widespread / sustained staff industrial action • Sustained student protest / violence	• Cessation of major critical business systems or Education / Research programs for an intolerable period and at a critical time in the University calendar	• Irreparable damage to or loss of brand / image reputation • Serious / long term damage to Go8 status / international rankings • Widespread / persistent / sustained negative media attention	• Huge financial loss • Significant budget impact (revenue shortfall or expense over-run) with no capacity to adjust within existing budget / resources • May attract material adverse findings from external regulators or auditors	• Serious breach of legislation / contract with significant prosecution / fines likely • Future funding / approvals / registration / licensing in jeopardy • Potential for litigation including class actions • Criminal or civil proceedings initiated
4 Major	Critical event or circumstance that can be endured with proper management	• Major loss / reduction in student enrolment / retention • Loss of a key School • Major impact on research activity over a sustained period • Major problems meeting teaching or research targets • Major long term damage to partnership / collaboration	• Serious injury / harm, including sexual assault / rape • Dangerous near miss • Long term loss of some key staff resulting in skills / knowledge / expertise deficits • Threat / staff industrial action • Threat / student protests	• Cessation of major critical business systems or Education / Research programs for an unacceptable period and / or at a critical time in the University calendar	• Sustained damage to brand / image / reputation nationally / internationally • Long term national or local negative media coverage	• Major financial loss • Requires significant adjustment or cancellation to approved / funded projects / programs	• Major breach of contract / Act / regulations / consent conditions • Expected to attract regulatory attention • Investigation, prosecution and / or major fines possible • Allegations of criminal / unlawful conduct
3 Moderate	Significant event or circumstance that can be managed under normal circumstances	• Significant loss / reduction of number of students in a course • Loss of a key academic course • Significant impact on research activity over a sustained period • Significant problem meeting teaching or research targets • Significant but short term damage to partnership	• Adverse impact on person's health / welfare • Lost time or penalty notice due to unsafe act / plant / equipment • Short term loss of skills / knowledge / expertise • Severe staff morale / increase in workforce absentee rate • Student dissatisfaction	• Loss / interruption / compromise of critical business systems or Education / Research program for a protracted period of time • Major service delivery targets cannot be met	• Significant but short term damage to brand / reputation • Student / stakeholder and / or community concern • Prominent local negative media coverage	• Significant financial loss • Impact may be reduced by reallocating resources	• Breach of contract, Act, regulation or consent conditions Potential for regulatory action • Potential for allegations of criminal / unlawful conduct
2 Minor	Event with consequences that can be readily absorbed but requires management effort to minimise the impact	• Short term reduction in student enrolment / retention • Minor impact on research activity • Temporary problems meeting some teaching / research targets	• Potential adverse impact on person's health / welfare • Inappropriate behaviour • Work place safety compromised • Some loss of staff with tolerable loss / deficit in skills • Dialogue required with industrial groups or student body	• Loss / interruption / compromise of critical business systems or Education / Research program for tolerable period but at an inconvenient time • Problems with delivery of local services or localised programs	• Some short term negative media coverage • Concern raised by students / stakeholders	• Some financial loss • Requires monitoring & possible corrective action within existing resources	• Minor non compliances or breaches of contract, Act, regulations, consent conditions • May result in infringement notice
1 Insignificant	Some loss but not material; existing controls and procedures should cope with event or circumstance	• Minor downturn in student enrolments / retention • Negligible impact on research activity or achievement of teaching / research targets	• Minimal or no adverse impact on person's health / welfare • Negligible skills or knowledge loss	• Negligible impact on delivery of service	• Minor / localised damage to brand, image or reputation	• Unlikely to impact on budget or funded activities	• Unlikely to result in adverse regulatory response or action

FOR FURTHER ENQUIRIES

The University of Adelaide SA 5005 Australia

Mitchell Building,
North Terrace,
Adelaide SA 5005

ENQUIRIES helpdesklegal@adelaide.edu.au

TELEPHONE +61 8 8313 4539

adelaide.edu.au

SOUTH AUSTRALIA