Western Sydney University

Risk Management Guidelines

These guidelines should be read in conjunction with the University's Risk Management Policy

This guideline takes effect from 12/06/2019

Contents

1. Introduction

1.1 Purpose

The Risk Management Guidelines (RMG) supplements the University's Risk Management Policy (RMP). The policy and guidelines describe the University's approach to risk management. The guidelines provide the University's approach to risk management, risk management framework and key principles and processes to implement an effective risk management practice across the University.

These guidelines are based on the International Standard ISO 31000:2018 (Risk management – guidelines).

1.2 Using the Risk Management Guidelines

This guideline is the definitive reference for the University's risk management guidelines. The Risk Management Process Owner and anyone who is involved in managing risk can refer to this guideline.

2. Risk Management Approach

2.1 Background

The University maintains an enterprise-wide strategic risk management program, which is based on the methodology contained in the International Standard ISO 31000:2018 Risk Management – Guidelines . As part of the ongoing improvements to the risk management framework, Strategic and Operational Risk Registers should be maintained in the enterprise-wide risk management system (Protecht) for risk and compliance management.

This approach allows staff to access the on-line Registers from any location, at any time using a variety of desktop or portable devices. It also provides for more timely updates and assists with the identification of emerging risks or unwelcome trends. The system is secure and access to the Registers is securely managed.

2.2 Process Purpose

The purpose of the risk management process is to manage the lifecycle of all documented risks, ensuring that changes in our internal and external environment, which could impact the University's strategic goals and business unit objectives, are reflected in the Risk Register.

In doing so, the risk management process is likely to improve performance against the University's strategic and business unit objectives by contributing to:

- Fewer sudden shocks and unwelcome surprises
- More efficient use of resources
- Reduced waste
- Reduced fraud
- Better service delivery
- Improved innovation
- Increased likelihood of change initiatives being achieved
- More focus internally on doing the right things properly
- More focus externally to shape effective strategies

3. Risk Management Framework

3.1 General

The University's 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 Framework development encompasses integrating, designing, implementing, evaluating and improving risk management across the University. Figure 1 illustrates the components of a framework.

Figure 1 - Framework

The University should evaluate its existing risk management practices and processes, evaluate any gaps and address those gaps within the framework.

The components of the framework and the way in which they work together should be customised to the needs of the University.

3.2 Leadership and commitment

Top management, various committees and oversight or governance bodies, where applicable, should ensure that risk management is integrated into all of University's activities and should demonstrate leadership and commitment by:

- implementing all components of the framework;
- issuing a statement or policy that establishes a risk management approach, plan or course of action;
- ensuring that the necessary resources are allocated to managing risk;
- assigning authority, responsibility and accountability at appropriate levels within the University.

This will help the University to:

- align risk management with its objectives, strategy and culture;
- recognize and address all obligations, as well as its voluntary commitments;
- establish the amount and type of risk that may or may not be taken to guide the development of risk criteria, ensuring that they are communicated to the University and its stakeholders;
- communicate the value of risk management to the University and its stakeholders;
- promote systematic monitoring of risks;
- ensure that the risk management framework remains appropriate to the context of the University.

Top management is accountable for managing risk while oversight bodies are accountable for overseeing risk management. Oversight bodies are often expected or required to:

- ensure that risks are adequately considered when setting the University's objectives;
- understand the risks facing the University in pursuit of its objectives;
- ensure that systems to manage such risks are implemented and operating effectively;
- ensure that such risks are appropriate in the context of the University's objectives;
- ensure that information about such risks and their management is properly communicated.

3.3 Integration

Integrating risk management relies on an understanding of the University's structures and context. Structures differ depending on the University's purpose, goals and complexity. Risk is managed in every part of the University's structure. Everyone in the University has responsibility for managing risk.

Governance guides the course of the University, its external and internal relationships, and the rules, processes and practices needed to achieve its purpose. Management structures translate governance direction into the strategy and associated objectives required to achieve desired levels of sustainable performance and long-term viability. Determining risk management accountability and oversight roles within the University are integral parts of the University's governance.

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

3.4 Design

3.4.1 Understanding the University and its context

When designing the framework for managing risk, the University examines and understand its external and internal context.

Examining the University's external context may include, but is not limited to:

- the social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, whether international, national, regional or local;
- key drivers and trends affecting the objectives of the University;
- external stakeholders' relationships, perceptions, values, needs and expectations;
- contractual relationships and commitments;
- the complexity of networks and dependencies.

Examining the University's internal context may include, but is not limited to:

- vision, mission and values;
- governance, the University's structure, roles and accountabilities;
- strategy, objectives and policies;
- the University's culture;
- standards, guidelines and models adopted by the University;
- capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, intellectual property, processes, systems and technologies);
- data, information systems and information flows;
- relationships with internal stakeholders, taking into account their perceptions and values;
- contractual relationships and commitments;
- interdependencies and interconnections.

3.4.2 Articulating risk management commitment

Top management and oversight bodies, where applicable, should demonstrate and articulate their continual commitment to risk management through a policy, a statement or other forms that clearly convey the University's objectives and commitment to risk management. The commitment should include, but is not limited to:

- the University's purpose for managing risk and links to its objectives and other policies;
- reinforcing the need to integrate risk management into the overall culture of the University;
- leading the integration of risk management into core business activities and decision-making;
- authorities, responsibilities and accountabilities;
- making the necessary resources available;
- the way in which conflicting objectives are dealt with;
- measurement and reporting within the University's performance indicators;
- review and improvement.

The risk management commitment should be communicated within the University and to stakeholders, as appropriate.

3.4.3 Assigning University's roles, authorities, responsibilities and accountabilities

Top management and oversight bodies, where applicable, should ensure that the authorities, responsibilities and accountabilities for relevant roles with respect to risk management are assigned and communicated at all levels of the University, and should:

- emphasize that risk management is a core responsibility;
- identify individuals who have the accountability and authority to manage risk (risk owners).

3.4.4 Allocating resources

Top management and oversight bodies, where applicable, should ensure allocation of appropriate resources for risk management, which can include, but are not limited to:

- people, skills, experience and competence;
- the University's processes, methods and tools to be used for managing risk;
- documented processes and procedures;
- information and knowledge management systems;
- professional development and training needs.

The University should consider the capabilities of, and constraints on, existing resources.

3.4.5 Establishing communication and consultation

The University will establish an approved approach to communication and consultation in order to support the framework and facilitate the effective application of risk management. Communication involves sharing information with targeted audiences. Consultation also involves participants providing feedback with the expectation that it will contribute to and shape decisions or other activities. Communication and consultation methods and content should reflect the expectations of stakeholders, where relevant.

Communication and consultation should be timely and ensure that relevant information is collected, collated, synthesised and shared, as appropriate, and that feedback is provided and improvements are made.

3.5 Implementation

The University should implement the risk management framework by:

- developing an appropriate plan including time and resources;
- identifying where, when and how different types of decisions are made across the University, and by whom;
- modifying the applicable decision-making processes where necessary;
- ensuring that University's arrangements for managing risk are clearly understood and practised.

Successful implementation of the framework requires the engagement and awareness of stakeholders. This enables the University to explicitly address uncertainty in decision-making, while also ensuring that any new or subsequent uncertainty can be taken into account as it arises.

Properly designed and implemented, the risk management framework will ensure that the risk management process is a part of all activities throughout the University, including decision-making, and that changes in external and internal contexts will be adequately captured.

3.6 Evaluation

In order to evaluate the effectiveness of the risk management framework, the University should:

- periodically measure risk management framework performance against its purpose, implementation plans, indicators and expected behaviour;
- determine whether it remains suitable to support achieving the objectives of the University.

3.7 Improvement

3.7.1 Adapting

The University will continually monitor and adapt the risk management framework to address external and internal changes.

3.7.2 Continually improving

The University will continually improve the suitability, adequacy and effectiveness of the risk management framework and the way the risk management process is integrated.

As relevant gaps or improvement opportunities are identified, the University should develop plans and tasks and assign them to those accountable for implementation. Once implemented, these improvements should contribute to the enhancement of risk management.

4. Risk Management Principles

The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of strategic and operational objectives.

The principles outlined in Figure 2 provide guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose.

The principles are the foundation for managing risk and should be considered when establishing the University's risk management framework and processes. These principles should enable Western Sydney University to manage the effects of uncertainty on its objectives.

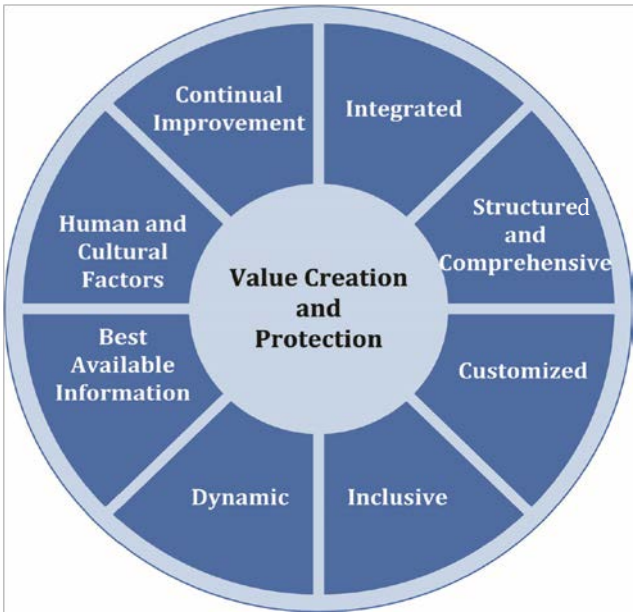

Figure 2 - Principles

Effective risk management requires the elements illustrated in Figure 2 and can be further explained as follows:

a. Integrated
   Risk management is an integral part of all the University's activities.

b. Structured and comprehensive
   A structured and comprehensive approach to risk management contributes to consistent and comparable results.

c. Customized
   The risk management framework and process are customized and proportionate to the University's external and internal context related to its objectives.

d. Inclusive
   Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.

e. Dynamic
   Risks can emerge, change or disappear as the University's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.

f. Best available information
The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.

g. Human and cultural factors
Human behaviour and culture significantly influence all aspects of risk management at each level and stage.

h. Continual improvement
Risk management is continually improved through learning and experience.

5. Risk Management Process

The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk. The risk management process adopted by Western Sydney University is illustrated in Figure 3.

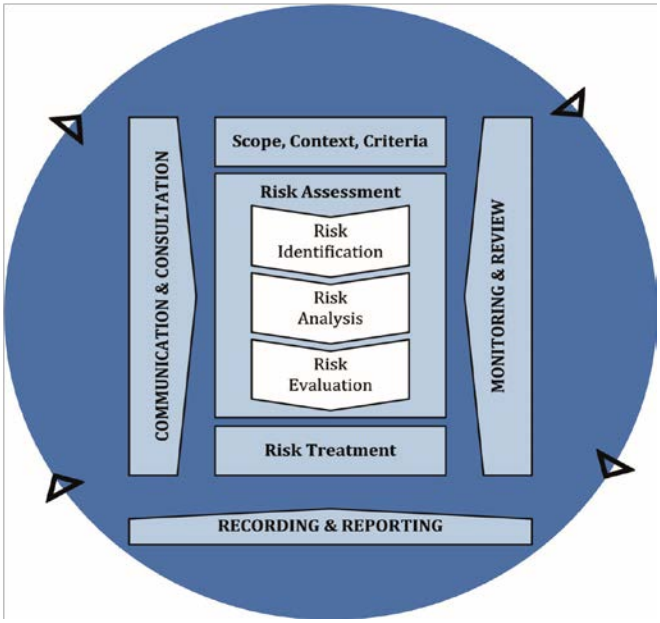

Figure 3 - Process

The risk management process should be an integral part of management and decision-making and integrated into the structure, operations and processes of the University. It can be applied at strategic, operational, programme or project levels.

5.1 Communication and Consultation

Communicating and consulting about risk underpins the successful management of risk. Effective communcation requires consultation with relevant stakeholders and the transparent, complete and timely flow of information between decision makers.

5.2 Establishing the Context

Prior to undertaking the risk assessment process, it is important to define the context against which risks will be assessed. This will help to:

a. clarify the scope and purpose of the risk assessment activity;
b. define the internal and external parameters to be considered when managing risk; and
c. identify the relevant stakeholders to communicate and consult with.

It is important to understand the internal and external environments that the University operates in which may influence or impact the function or process being assessed. The following are some aspects for consideration:

a. Internal context - the environment in which the University operating model is designed and based upon, including but not limited to:

i. understanding the University's Strategy, objectives, values and policies to identify areas of priority and alignment with operational business plans and drivers;
ii. considering the University's governance, structure, roles and accountabilities;
iii. considering available resources and capabilities; and
iv. understanding the University's Risk Appetite Statement (including risk tolerances).

b. External context - the environment in which the University operates and the impact of this on achievement of the University's objectives, including:

i. key legislations, rules and compliance standards requirements; and
ii. social, cultural, political, economic and market conditions.

5.3 Risk Assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

Risk assessment should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiry as necessary.

5.3.1 Risk Identification

The purpose of risk identification is to find, recognise and describe risks that might help or prevent the University achieiving its objectives. Relevant, appropriate and up-to-date information is important in identifying risks.

The University should identify risks, whether or not their sources are under its control. Consideration should be given that there may be more than one type of outcome, which may result in a variety of tangible or intangible consequences. An incomplete or not comprehensive list of risks may result in material risks not further analysed in the process.

Risks identified are documented in a risk register. The University has an approved Risk Register template which must be used when developing or revising a risk register. Risk register templates can also be downloaded from the University's Risk Management website.

When identifying and describing a risk, it should be comprehensive and include:

a. the source of risk;
b. the areas affected;
c. causes / potential triggers that may results in the risk event occurring;
d. potential consequences to the University should this risk event occur.

Note: potential consequences should be described in qualitative terms and not described as a process, a failure or lack of controls.

It is preferred that risk identification is conducted through a team-based approach with all members of the group having a good understanding of the tasks and objectives of the area being assessed. This will help reduce the chance of any risks being overlooked. Other techniques such as desktop risk assessments or management reviews can also be used.

It is important to identify the risk owner who will be responsible for the risk. This is critical to ensure that the risk is regularly monitored and appropriately addressed through mitigation strategies further down the risk management process.

Questions to ask when identifying potential risks might include:

a. What needs to go right to achieve a specific objective?
b. What are our top priorities?
c. What could go wrong that will derail us from achieving our objectives?
d. Where and how could this happen?
e. Where are our vulnerabilities?
f. How do we know if we are achieving our objective?
g. How do we know that we are making the right decisions?

5.3.2 Risk Analysis

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood of events and scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect mutliple objectives.

This stage is undertaken to better understand the risks identified in the previous step. This involves measuring the likelihood of the risk event occurring and extent of the consequences if the risk were to occur. The University's Risk Ratings Matrix and Likelihood Ratings Guide is attached at Appendix 3.

Measuring the likelihood and consequences of a risk event is not strictly a statistical or quantitative measure. It requires management's judgement which can be informed by previous experiences of a similar risk event, experience of other Universities or companies in similar scenarios, available University performance data or audit/independent review observations.

5.3.3 Risk Evaluation

Risk evaluation involves comparing the level of risk found during the risk analysis with the University’s risk appetite to determine whether the risk or its magnitude are acceptable or tolerable to the University. If the risk is not acceptable or tolerable, a risk treatment will need to be considered.

Evaluation of each identified risk may result in the following scenarios:

a. the residual risk rating is beyond an acceptable or tolerable level:
    i. further mitigation strategies or treatment are expected to be formulated to reduce the risk to acceptable levels; or
    ii. if no further treatment is identified, the acceptance of this risk will be made at the Senior Executive level.
b. the residual risk rating is below an acceptable or tolerable level:
    i. no further action is required; or
    ii. consider reducing the level of controls currently in place to reallocate resources to areas of greater need.

Although many risks may be rated low or moderate from a University perspective, these may be unacceptable to the responsible manager and should be flagged as such. The risk register can in

this way identify risks that warrant priority attention both at a University level and/or an operational level.

Risks beyond the tolerable level may be accepted in some circumstances without further mitigation (i.e. other than maintaining existing controls) if, for example:

a. there is no appropriate risk treatment available;
b. the cost of the treatment outweighs the benefit;
c. the benefits and opportunities outweigh the potential consequences of the risk; or
d. the risk is being taken to pursue an opportunity in line with the University's strategy and objectives.

5.4 Risk Escalation and Treatment

If further risk treatment is required for a specific risk, the risk owner(s) is responsible for identifying and implementing appropriate measures to reduce the risk to an acceptable level.

Risk treatment strategies to reduce the risk level include:

a. avoiding the risk by discontinuing or not commencing the activity;
b. removing the source of the risk;
c. changing the likelihood of the risk;
d. changing the consequences of the risk; or
e. sharing the risk with another party (e.g. contracting or insurance).

The following principles should be considered when identifying risk treatments:

a. identify and assess a range of treatment options before selecting one or more of these options to be implemented;
b. a cost/benefit analysis may be useful in determining the most appropriate mitigation option; and
c. treating a risk may have implications elsewhere and impact on other activities. Consequential impacts, correlations and dependencies should also be considered to ensure that in managing one risk, an unacceptable situation is not created elsewhere.

Once a risk treatment plan is identified, it should outline the:

a. risk treatment to be implemented;
b. person responsible for implementation; and
c. timeframes for completion and resources required.

Examples of possible mitigation strategies include: re-designing or enhancing existing controls; introducing new controls; further monitoring of existing controls; or, in cases where a control has been assessed as ineffective, removing the existing control.

The management should take the following actions for each risk rating:

RISK RATING - MANAGEMENT ACTION REQUIRED
Catastrophic risk = immediate attention & response needed; requires a risk assessment & management plan prepared by relevant senior managers for Vice-Chancellor; risk oversight by the Executive Committee and the Board of Trustees, and any nominated Standing or Management Committee
High risk = risk to be given appropriate attention & demonstrably managed; reported to Vice-Chancellor, Executive Committee and other Senior Executives / Management Committees as necessary
Moderate 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 may be accepted by the Executive Committee.
Very low risk = acceptable with periodic review. Exposure to this level of risk is acceptable without additional risk treatments.

The University staff are required to complete risk mitigation plans or agreed management actions in accordance with dates proposed by management or the risk classification schedule as below:

Risk Rating	Risk Mitigation Timeframe
Critical	3 months
High	6 months
Moderate	9 months
Low	12 months or risk accepted
Very Low	Risk accepted

5.5 Monitoring and Review

The University will undertake continuous monitoring and review of the risk management process to:

- ensure controls are effective and efficient in both design and operation
- obtain further information to improve risk assessment
- analyse and learn lessons from events (including near-misses), changes, trends, successes and failures
- detect changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities, and
- identify emerging risks.

Risks are monitored and reviewed through a number of ways, including parties such as risk owners, the Audit and Risk Assessment Unit, the Senior Executive and various governance committees. However, the primary responsibility resides with the business unit risk owners.

5.6 Recording and Reporting

The risk management process and its outcomes should be documented and reported through appropriate mechanisms. Recording and reporting aims to:

- communicate risk management activities and outcomes across the University;
- provide information for decision-making;
- improve risk management activities;
- assist interaction with stakeholders, including those with responsibility; and accountability for risk management activities.

Reporting is an integral part of the University's governance and should enhance the quality of dialogue with stakeholders and support top management and oversight bodies in meeting their responsibilities.

Factors to consider for reporting include, but are not limited to:

- differing stakeholders and their specific information needs and requirements;
- cost, frequency and timeliness of reporting;
- method of reporting; and
- relevance of information to the University's objectives and decision-making.

6. Status and Details

Status	Current
Revision History	Version 1
Revision Date	1 June 2021
Approval Authority	Board of Trustees
Approval Date	12 June 2019
Expired Date	Not Applicable
Unit Head	**Aman Chand** Director, Audit and Risk Assessment +61 2 45701517
Document Author	**Sharan Kaur** Business Risk Partner Office of Audit and Risk Assessment +61 2 45701193
Document Reviewer	**Aman Chand** Director, Audit and Risk Assessment +61 2 45701517 **Helen Fleming** University Secretary and General Counsel +61 2 96859895
Enquiries Contact	**Aman Chand** Director, Audit and Risk Assessment +61 2 45701517

Appendix 1 - Abbreviations Used

The following abbreviations are referenced within this document (note: definitions can be found at Appendix 2 below):

ITDS	Information Technology and Digital Services
ITSM	IT Service Management
RMG	Risk Management Guidelines
RMP	Risk Management Policy
WSU	Western Sydney University

Appendix 2 - Key Principles and Definitions

Common terminology used throughout the guideline is listed in the table below.

Term	Description
Assess and Estimate	The third step in the Risk Management framework. This step aims to prioritise each risk so that urgency of mitigation activities is clear. This is done by ranking the likelihood and impact of each risk occurring.
Assess and Evaluate	The fourth step in the Risk Management framework. This step aims to understand the risk exposure of the activity in comparison to other risks identified in the register. This is where activities or risks that have some sort of interrelationship are identified.
Identify Context	The first step in the Risk Management framework. This step identifies the activity objectives, scope, assumptions, constraints, stakeholders and how the activity fits with the University structure. Additionally, it confirms that the information is complete and accurate.
Identify Risks	The second step in the Risk Management framework. This step identifies the risks associated with the activity as threats or opportunities, preparing the risk register entry, any key performance indicators or early warning indicators and understanding the stakeholder viewpoint of the risk.
Impact	The result, or potential result, of a particular threat or opportunity actually occurring.
Implement	The sixth and final step in the Risk Management framework. In this step, the plan is implemented and monitored for effectiveness, and that corrective actions are put in place where the planned activities do not meet with the expected results.
Innovation	The process whereby ideas are generated and investigated for viability in the University environment.
Issue	Issue arises from lack of controls or lack of risk mitigation in place. A control is any measure or action that modifies or regulates risk.
Likelihood	An evaluation of a particular threat or opportunity actually happening, including a consideration of the frequency with which this may arise. Also called probability.
Opportunity	An uncertain event that would have a favourable impact on objectives or benefits if it occurred.
Plan	The fifth step in the Risk Management framework. In this step, a specific management plan to address the responses for each threat (minimise risk) or opportunity (maximise potential) is developed.
Probability	See likelihood.
Project Management	The PMO process by which projects are prepared, planned, approved and implemented in relation to its projects.
Residual Risk Rating	The score of a risk that defines its criticality. It is obtained by multiplying likelihood and impact.
Risk	Risk is the *effect of uncertainty* on the University's objectives and an effect is a positive or negative deviation from what is expected. Risk is measured in terms of consequence or outcome severity and likelihood
Threat	An uncertain event that could have a negative impact on objectives or benefits.

Appendix 3 - Western Sydney University Risk Rating Scale

Risk Rating Matrix (Impact * Likelihood)

Impact	Likelihood				
	Rare (1) (remote)	Unlikely (2) (uncommon)	Possible (3) (occasional)	Likely (4) (probable)	Almost Certain (5) (frequent)
Catastrophic (5)	Moderate	Moderate	High	Critical	Critical
Major (4)	Low	Moderate	High	High	Critical
Moderate (3)	Low	Moderate	Moderate	Moderate	High
Minor (2)	Very Low	Low	Moderate	Moderate	Moderate
Insignificant (1)	Very Low	Very Low	Low	Low	Low

University Risk Impact and Likelihood Assessment Table

Impact Score	Generic Impact Description	Area of Impact – Description of Consequence					
		Education & Research	Health and Safety	Service Delivery	Brand & Reputation	Financial	Legal/ Compliance
(5) Catastrophic	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 School • 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 University status / international rankings • Widespread / persistent / sustained negative media attention	• Huge financial loss (greater than $25m) • 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 (greater than $10m) • 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 / wellbeing • 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 (greater than $5m) • 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

Impact Score	Generic Impact Description	Area of Impact – Description of Consequence					
		Education & Research	**Health and Safety**	**Service Delivery**	**Brand & Reputation**	**Financial**	**Legal/ Compliance**
(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 / wellbeing • 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 (greater than $2m) • 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 / wellbeing • 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 (less than $2m) • Impact can be absorbed by daily business running costs	• Unlikely to result in adverse regulatory response or action

Likelihood Score	Definition of Likelihood
(5) Almost Certain	Highly likely to happen, possibly frequently or already happened
(4) Likely	Will probably happen, but not a persistent issue
(3) Possible	May happen occasionally
(2) Unlikely	Not expected to happen, but is a possibility
(1) Rare	Very unlikely this will ever happen

Appendix 4 - Risk Categories

Academic – Curriculum Quality	Quality and standard of academic program or course contents, planning strategy for course offerings, approvals and monitoring process for courses and units,educational and teaching operations (distance, on-campus, online, etc.)
Academic – Research	Research income, research load, research work and staff, research capacity, intellectual property, patents, ethical conduct in research etc.
Behaviour	Staff attitudes to risk, risk culture, staff reckless (disasters), staff conservative (opportunities lost), staff uptake of policies. Student demonstrations, terrorism, fraud, corrupt conduct, activists seeking to damage the University.
Commercial Activities	Engaging in commercial activities that are not part of the core operations of the University that could have significant financial exposures and risks
Environmental	Water, soil, air contamination, asbestos, waste management, incidents causing injury/ death, environmentally triggered emergencies, natural hazards and radiation.
Financial	Reductions in income, change of funding model or policy, liquidity, financial loss, insurances, debt, budget overruns, tenders, market risk, credit risk, operational risk, financial decisions are poorly made or executed.
Infrastructure	The physical fabric of the University, buildings, roads, pathways, utilities (electricity, water), IT infrastructure.
International	Overseas ventures/ reputation/ programs, relationships with overseas universities.
Legal	Contracts and agreements, high profile litigation - financial and reputational impact.
Legislation or Regulatory Compliance	Breach, financial penalty/ impact on reputation, laws, regulations, codes, statutory obligations affecting the University.
Market Competition and Society Changes	New Universities entering into the Western region, online learning and teaching competition, changes in expectations from employers, government, communities and society.
Organisation	Strength of policies and procedures, planning, staffing, morale, training, ethical culture, leadership and management.
Political	Ability to respond to major changes in education policies, level of government consultation, change of government.
Projects	Significant transformation projects including key IT projects that are not well managed, run over time, over budget and scope and do not deliver on the expected outcomes and benefits. Risk of change is not managed.
Reputation	Damaging media reports, employability of graduates, research links, regional involvement. The reputation of the organisation could be damaged from all sources of risk categories.
Third Party	Potential risk associated with supplier, distributors and partners.
Work Health & Safety (WHS) or Safety or People risk	Includes human resource management practices, recruitment, induction, training & development, OH&S (occupational health and safety), hazard management, industrial actions, health, rehabilitation, EEO (equal employment opportunities), fraud, corruption & crime
Technology	It is related to the complete change in technology or introduction of a new technology. For ITDS risk registers, see breakdown of this category.
Technology	Strategic direction of IT, reliance on vWSU, blended learning, ecommerce/ email/ internet, student records system, library.
Disaster Recovery	the defined process and plan for restoring IT resources
Hardware	servers, devices, desktops, printers, fax equipment, phones, cameras
Networking	switches, routers, cabling, wireless access points
Applications	any corporate, desktop, teaching, research or standalone application
Customer Support	anything related to customer service and support
IT Security	anything related to the security of our IT systems
Resources	staff, contractors, expertise, knowledge, availability