

# **Risk Management Procedures**

## 1. OVERVIEW

These procedures are designed to support the implementation of the University Risk Management Policy by ensuring that the University's risks, whether having a positive or negative consequence, are effectively identified and responded to; and defining how risk management will occur within the University.

The procedures describe the approach taken to risk management at AUT and explains how it is applied on different levels; the management of strategic, University-level risk, and risk management within Faculties and Professional Groups (Services), projects and programmes. The procedures provide guidance on the processes to be followed and outlines who is responsible for what parts of those processes.

## 2. INTRODUCTION

University activities may involve risks which could jeopardise the successful outcome of the University's objectives if not managed appropriately. The aim of risk management at AUT is to create and protect value. Therefore, risk management is about enabling the University to have a well-informed view of the key risks it faces and applying appropriate measures to manage those risks.

The balance between the costs of managing risk and the anticipated benefits needs to be considered. The goal is not to eliminate all risks, rather it is to manage the risks involved in University activities and to maximise our opportunities and minimise potential negative outcomes.

## 3. SCOPE

These procedures apply to all areas of the University and AUT controlled entities. It should be noted that certain risk domains (e.g. Health, Safety and Wellbeing - HSW) have additional risk management requirements documented that are consistent with this procedure.

## 4. RISK MANAGEMENT INTEGRATION

Risk management should be integrated into strategic/business planning and business as usual activities, projects within the University. The objective of carrying out the risk management process is to clearly identify what the risk is and how and to what extent it could impact on the activity or project being undertaken by the University.

There are points of overlap between Health, Safety and Wellbeing (HSW) and other University risks. The University has chosen to manage and report HSW and other risks separately. For more detailed information on methodology and application of HSW Risk Management please refer to HS9001 HSW Risk Management Framework Procedure.

## 5. RISK ASSESSMENT PROCESS

The risk assessment process is a continuous cycle designed to support the operation of processes and achievement of objectives. It should be remembered at all stages that the purpose of risk management processes is to stimulate thinking and consequent action, rather than to produce documents for their own sake. The key steps in this process are:

- A. Identification of potential events
- B. Risk evaluation
- C. Response
- D. Review and report

The risk assessment process should be applied:

- as part of the annual strategic planning process;
- as part of the annual faculty/group planning process;

- when selecting and implementing projects; and
- as part of a programme analysis process.

## A. Identification of potential events

This is the process of identifying, describing and categorising risk. The **purpose** of risk identification is to find, recognise and describe potential risks that make it more unlikely that the University will achieve its objectives. For each key strategic, business or project objectives, identify the risks by:

- **considering the question** - “what could occur”? Identify the risks that either, currently exist, or may arise that could impact on the achievement of objectives;
- **considering the internal and external environment and context** to prompt discussion about what the relevant risks might be. The external environment includes: political, legal, regulatory, financial and competitive environment. The internal environment includes: organisational structure, culture, goals and objectives as well as any pre-existing risk registers and operational information (complaints, breaches, fraud monitoring, errors and process failures etc.);
- **considering** the nature of any **contributing factors** and identify any **early warning signals** / performance indicators; and
- **considering if the risk identified is likely to** result in the objective not being achieved and whether the objective itself is essential to the success of the University.

A risk register (see template table in Appendix B) should be used to capture the risks, ratings and controls.

## B. Risk evaluation

This involves understanding the nature of risk and its characteristics. Risk evaluation involves a detailed consideration of the following:

- The likelihood of events, risk sources and consequences;
- The nature and magnitude of consequences;
- The effectiveness of existing controls; including sensitivity and confidence levels.

An event can have multiple causes and consequences and can affect multiple objectives. The likelihood and consequence of an **inherent** risk should be assessed using the ratings defined below on Appendix A. The numbers are indicative; assigning scores is not intended to be exact science. The purpose of the evaluation system is simply to help risk owners in the assessment and prioritisation of risks. It is advisable that risks are identified and scored with input from colleagues; a workshop is one useful way of doing this.

## C. Response

The next step is to decide on the optimal level of risk (risk threshold) that would better ensure the achievement of objectives. This involves comparing the results of risk analysis (step B) with the desired level of risk AUT is willing to take. For each risk scoring above the risk threshold, a practical and proportionate response should be identified. The ranks of responses may include:

- Tolerate – accept the risk and do not attempt to reduce it
- Transfer – transfer the risk to a third party (e.g. through insurance)
- Terminate – eliminate the risk (e.g. changing the objective or the approach being taken to achieve it, or by abandoning the objectives entirely)
- Treat – take action to reduce either the probability of the risk occurring or the severity of the impact were it to occur (or both). Such action is known as control.

Once a risk and the associated controls have been identified the risk should be assessed by rating the potential consequence and likelihood of the risk actually occurring. This is the determination of **residual** risk, which is the remaining level of risk after controls have been taken into consideration.

The following guidelines should be considered when assessing the consequences of risks:

- A risk may have consequences in a number of categories and where the indicative rating is different, the more severe rating should be used. For example, if a risk has a minor 'financial' consequence and a major 'health, safety and wellbeing' consequence, the consequence rating applied to the risk should be major.
- For the non-financial consequence categories, the criteria should be used as indicative guidance for ratings. Not all criteria need to be met in order for the rating to be applied and not all possible criteria have been described.

## D. Review and report

Risk owners should review their Business Unit Risk Registers at least on a quarterly basis and consider any changes in their areas. Residual risk ratings should be reported as per the escalation and reporting framework below and action plans should be developed to try and reduce the rating (likely by changing processes or introducing new controls). The ongoing effectiveness of key controls should be monitored to determine if the associated risk rating remains appropriate.

The Group Director Risk and Assurance will update the University Risk Register periodically. This information is reported to the Senior Leadership Team (SLT) and Council Finance and Audit Committee (CFAC), and is used in the Internal Audit programme planning process.

### *Escalation and reporting framework*

The table below outlines the reporting and escalation of risks based on the nature of the risk and the risk rating.

<b>Residual Risk Rating</b>		<b>Risk escalation and reporting</b>
<b>Very High</b>	<b>Immediate Action Required</b> Stop activity, process or task until actions are taken to minimise the risk.	<b>Report to:</b> Vice-Chancellor and Group Director (Risk & Assurance) immediately <b>Record in:</b> Business Unit Risk Register & University Risk Register  The Vice Chancellor will oversee the management of the risk and effectiveness of controls before activity or process can resume.
<b>High</b>	<b>Action Required</b> Action required to reduce the risk likelihood or consequence.	<b>Report to:</b> Senior Leadership Team (SLT) and Group Director Risk & Assurance monthly, and CFAC. <b>Record in:</b> Business Unit Risk Register & University Risk Register  The Vice-Chancellor will oversee the management of the risk.
<b>Medium</b>	<b>Monitor</b> Risks need to be continually managed by the Risk Owner.	<b>Report to:</b> Group Director (Risk & Assurance) quarterly <b>Record in:</b> Business Unit Risk Register and University Risk Register  The Group Director Risk & Assurance oversees effectiveness of controls.
<b>Low</b>	<b>Tolerate</b> Risk managed by the Risk Owner (within the business unit).	<b>Report to:</b> the Risk Owner who will oversee the management of the risk. <b>Record in:</b> Business Unit Risk Register

## 6. RISK REGISTERS

The risk register records the thought process used to identify and evaluate risks and the information

available at the time of the decision. It is also used as a tool to monitor and report risks to the relevant University member or Committee based on the escalation framework. A business risk register template is provided in Appendix B.

## 7. RESPONSIBILITY FOR MONITORING COMPLIANCE

Monitoring the compliance with Risk Management Procedures sits with Group Director Risk and Assurance.

## 8. POLICY BASE

- I. Risk Management Policy
- II. Australian / New Zealand Standards Risk Management – Principles and Guidelines ISO 31000:2018

## 9. ASSOCIATED DOCUMENTS

Document	Title
HS9001	HSW Risk Framework Procedure

## 10. DEFINITIONS

Document	Title
Policy	Means the Risk Management Policy.
Risk	Unplanned event which if occurs may impact the achievement of AUT objectives. Therefore, risk merely reflects the “uncertainty” inherent to AUT’s business environment. This uncertainty can present downside “threats” or upside “opportunities”.
Likelihood	The probability or frequency of the risk occurring.
Consequence	The outcome or impact of an event.
Inherent Risk	Risk in the absence of any mitigating or compensating controls
Control	A process, policy, practice or other action that acts to modify the level of risk.
Project Risk	Risk which is associated with a project
Residual Risk	Risk remaining after risk treatment (the implementation of controls)
Risk Management	The process of identifying, assessing and managing “uncertainty”. Risk Management is therefore seen as just good management – as such it is dynamic and integrated into day to day decision making processes.

## 11. IMPLEMENTATION

These procedures will be implemented once they appear on the Policies and Procedures webpage.

## Appendix A

### Risk Matrix (Likelihood x Consequence)

			Consequence					
Likelihood			1	2	3	4	5	
			Insignificant	Minor	Moderate	Major	Extreme	
	5	Almost Certain	Highly likely to happen, possibly frequently	Low	Medium	High	Very High	Very High
	4	Likely	Will probably happen, but not a persistent issue	Low	Medium	High	High	Very High
	3	Possible	May happen occasionally	Low	Medium	Medium	High	High
	2	Unlikely	Not expected to happen, but is a possibility	Low	Medium	Medium	Medium	High
	1	Rare	Very unlikely to occur	Low	Low	Low	Medium	High
			Insignificant	Minor	Moderate	Major	Extreme	
	<b>Financial</b> – compared against: <ul style="list-style-type: none"><li>Budget vs. actuals</li><li>Revenue loss</li><li>Increased costs</li></ul>		•Unlikely to impact on budget or funded activities	•Requires monitoring & possible corrective action within existing resources	•Impact may be reduced by reallocating resources	•Requires significant adjustment or cancellation to approved / funded projects / programmes	•Significant budget impact (revenue shortfall or expense over-run) with no capacity to adjust within existing budget / resources	
	<b>Infrastructure</b>		•Minor impact on delivery of service or operational activities with no impact to strategic goals •Negligible damage to property and equipment	•Loss / interruption / compromise of critical business systems or teaching / research systems for a tolerable period but at an inconvenient time •Problems with delivery of services or programmes. •Partial loss or damage to property and equipment with minor impact to service delivery interruption.	•Loss / interruption / compromise of critical business systems or teaching / research systems for a protracted period of time •Service delivery targets are compromised •Loss or damage to property and equipment resulting in moderate service delivery interruption.	•Cessation of major critical business systems or teaching / research systems for an unacceptable period and / or at a critical time in the University calendar. •Major service delivery targets cannot be met. •Loss or damage to key property and equipment resulting in major service delivery interruption.	•Cessation of major critical business systems or teaching / research systems for an intolerable period and/or at a critical time in the University calendar •Failure of a major infrastructural asset (building or campus) incapable of being used for the delivery of University outputs resulting in significant impact of and disruption to strategic goals	

<b>Teaching/Learning and Research</b>	<ul style="list-style-type: none"> <li>• Minor downturn in student enrolments/retentions.</li> <li>• Negligible impact on research activity or achievement of teaching/research KPIs.</li> </ul>	<ul style="list-style-type: none"> <li>• Short term reduction in student enrolment /retention.</li> <li>• Minor impact on research activity.</li> <li>• Temporary problems meeting some teaching/research -KPIs</li> </ul>	<ul style="list-style-type: none"> <li>• Significant loss/reduction of number of students in a course</li> <li>• Loss of a key academic course.</li> <li>• Significant impact on research activity over a sustained period.</li> <li>• Significant problem meeting teaching or research KPIs</li> <li>• Significant but short-term damage to partnership.</li> </ul>	<ul style="list-style-type: none"> <li>• Major loss/reduction in student enrolment/retention.</li> <li>• Loss of a key school.</li> <li>• Major impact on research activity over a sustained period.</li> <li>• Major problems meeting teaching or research KPIs</li> <li>• Major long-term damage to partnerships /collaboration.</li> </ul>	<ul style="list-style-type: none"> <li>• Unsustainable loss/reduction in student enrolment/retentions.</li> <li>• Loss of faculty.</li> <li>• Serious / sustained reduction in research activity / output.</li> <li>• Serious / sustained problems reaching a number of students, teaching or research -KPIs.</li> <li>• Irreparable impact on relationship with partners / collaborators.</li> </ul>
<b>Legal and regulatory compliance</b>	<ul style="list-style-type: none"> <li>• Unlikely to result in adverse regulatory response or action</li> </ul>	<ul style="list-style-type: none"> <li>• Minor non compliances or breaches of contract, Act, regulations, consent conditions</li> <li>• May result in infringement notice</li> </ul>	<ul style="list-style-type: none"> <li>• Breach of contract, Act, regulation or consent conditions</li> <li>• Potential for regulatory action</li> <li>• Potential for allegations of criminal / unlawful conduct</li> </ul>	<ul style="list-style-type: none"> <li>• Major breach of contract / Act / regulations / consent conditions</li> <li>• Expected to attract regulatory attention</li> <li>• Investigation, prosecution and / or major fines possible</li> <li>• Allegations of criminal / unlawful conduct</li> </ul>	<ul style="list-style-type: none"> <li>• Serious breach of legislation / contract with significant prosecution / fines likely</li> <li>• Future funding / approvals / registration / licensing in jeopardy</li> <li>• Potential for litigation including class actions</li> <li>• Criminal or civil proceedings initiated</li> </ul>
<b>Brand and Reputation</b>	<ul style="list-style-type: none"> <li>• Minor damage to brand, image or reputation</li> <li>• No stakeholder concerns</li> </ul>	<ul style="list-style-type: none"> <li>• Some short-term negative media coverage</li> <li>• Minor concern raised by students / stakeholders</li> </ul>	<ul style="list-style-type: none"> <li>• Significant but short-term damage to brand / reputation</li> <li>• Student / stakeholder and / or community concern</li> <li>• Prominent local negative media</li> </ul>	<ul style="list-style-type: none"> <li>• Sustained damage to brand / image / reputation nationally / internationally</li> <li>• Long term national or local negative media coverage</li> </ul>	<ul style="list-style-type: none"> <li>• Irreparable damage to or loss of brand / image reputation</li> <li>• Serious / long term damage to university status / international rankings</li> <li>• Widespread / persistent / sustained negative media attention</li> </ul>
<b>Health and Safety</b>	PLEASE REFER TO THE HSW RISK ASSESSMENT FRAMEWORK (HS9001)				
<b>Project performance (excludes major capital building projects)</b>	<ul style="list-style-type: none"> <li>• Cost and budget overruns &lt;2%</li> <li>• Negligible impact on quality and resources required</li> <li>• No key delivery dates or milestones missed</li> </ul>	<ul style="list-style-type: none"> <li>• Costs and budget overruns between 3%-5%</li> <li>• Minor impact to quality of the output remedied within approved resources</li> <li>• Minor schedule slip, no critical activities late</li> </ul>	<ul style="list-style-type: none"> <li>• Cost and budget overruns between 6-15%.</li> <li>• Quality and performance below goal and moderate changes required to achieve intended benefits</li> <li>• Moderate schedule slip</li> </ul>	<ul style="list-style-type: none"> <li>• Cost and budget overruns between 16-30%.</li> <li>• Significant changes required to meet a threshold requirement.</li> <li>• Significant project benefits not realised.</li> <li>• Major schedule slip</li> </ul>	<ul style="list-style-type: none"> <li>• Cost and budget overruns of &gt;30%.</li> <li>• Product or service doesn't deliver the key intended outcomes for the business.</li> <li>• No benefit realised from the project.</li> <li>• Severe impact to approved resourced</li> <li>• Key delivery dates and milestones have been missed</li> </ul>

**APPENDIX B  
EXAMPLE OF A RISK  
REGISTER**

**GROUP/ FACULTY/PROJECT:**

**PREPARED BY:**

**DATE OF REVISION:**

<i><b>Risk</b></i>				<i><b>Assessment of Risk &amp; Controls</b></i>			<i><b>Risk treatment and Evaluation</b></i>				<i><b>Status</b></i>
Risk Ref	Risk Category	Risk Description	Consequence(s)	Inherent Risk Rating (Likelihood x Consequence)	Mitigating Controls	Residual Likelihood Rating (Likelihood x Consequence)	Risk Owner	Action(s) Required	Action(s) Owner(s)	Action(s) Due Date	Open vs Closed?
Enter a reference for the Risk.	Select the Consequence Area(s) this risk relates to.	Enter a description for the Risk.	Stipulate what the forecasted consequence of this risk is.	Score the risk (likelihood x consequence) before mitigating controls.	Reference any compensating controls in place to mitigate the risk.	Score the risk (likelihood x consequence) before mitigating controls.	Reference who is accountable for managing this risk.	State the actions required to mitigate the risk (i.e. controls)	Reference who is responsible for delivering this action (i.e. Control owner)	Enter the due date for the action.	Stipulate the status of the risk (Open vs Closed).

Score the risk (likelihood x consequence) after considering any mitigating controls.