EDITH COWAN UNIVERSITY

Strategic and Governance Services Centre

Integrated Risk Management Guidelines

Version	2.0
Relevance to	ECU Staff and Students
Responsible staff	Chief Risk Officer
Responsible Office	Strategic and Governance Services Centre
Date introduced	November 2007
Date(s) modified	September 2014, November 2015
	January 2016, February 2017, February 2021 July 2024
Next scheduled review date	July 2026
Related University documents	Policy rm001: Integrated Risk Management
	Policy hr081: Work, Health and Safety Work Health and Safety Hazard Identification and Risk Management Guideline Integrated Assurance Framework Risk Appetite Statement Framework
Related legislation and Standards	AS/NZ ISO 31000:2018 Risk management – guidelines

TABLE OF CONTENTS

1. PURPOSE AND SCOPE

The purpose of the University's Integrated Risk Management framework is to support the Council, University Executive, Schools, professional services and Controlled Entities to make effective decisions, based on a holistic understanding of the risks and opportunities; and ultimately support the achievement of the University's strategic objectives. As such, these guidelines apply to all members of the University community.

The University recognises that:

- risk is inherent in all academic, administrative and operational activities at the University;
- risk management is an integral part of good governance and management practice; and
- considered and structured risk-taking is required to achieve the University's strategic objectives.

2. RISK MANAGEMENT OVERVIEW

The University's risk management process, as outlined in these Guidelines, is consistent with the principles and standards of the International Standard on Risk Management, AS/NZ ISO31000:2018 ("the Standard").

The Standard defines risk as the effect of uncertainty on objectives, measured in terms of likelihood and consequence.

Risk management is the coordinated activities to direct and control the University with regard to risk. Risk management must be undertaken for all University activities. It does not need to be undertaken as a separate action and can be integrated into existing processes such as planning, project management, decision-making and reporting.

3. ACCOUNTABILITIES AND RESPONSIBILITIES

The following accountabilities and responsibilities apply with regards to risk management at ECU:

- The University Council has responsibility for oversight of risk management across the University and approves the University's risk governance framework and Risk Appetite Statement.
- The Quality, Audit and Risk Committee assists Council in fulfilling and discharging its responsibilities by providing independent and objective advice on the adequacy, integrity and/or effectiveness of the University's systems of risk management, internal control and compliance.
- The Vice-Chancellor is accountable for ensuring that a risk management framework is established, implemented and maintained in accordance with the Integrated Risk Management policy.
- The University Executive and Senior Management supports the Vice-Chancellor by assessing and managing the risks to the University and their portfolio's

objectives and strategies; leading the development of risk management plans; and allocating resources to enable effective risk management practices.

- The Risk and Incident Management Committee provides oversight of the Enterprise-wide Operational Risk Register. The objective of the RIMC is to reduce the overall risk associated with incidents and other adverse outcomes, by reducing the likelihood of reoccurrence and proactively managing enterprise-wide operational risks.
- The Chief Financial Officer is accountable for ensuring the University's compliance with section 57(2) of the Financial Management Act in relation to financial and foreign exchange risk management.
- The Director People and Culture is accountable for providing a work health and safety ('WHS') risk management framework to meet legislative compliance, including specialist WHS advice.
- The Chief Information Officer is accountable for risk management practices in relation to information technology, including information and cyber security. Cyber SMEs are included in relevant risk forums / workshops as required.
- The Strategic and Governance Services Centre (SGSC) provides specialist risk management advice and is responsible for ensuring that the risk management practices are implemented across the University and effective oversight is maintained through regular reporting on material risks.

4. RISK GOVERNANCE

The University's risk governance framework outlines the structures and processes required to oversee risk management activities and allows for escalation and reporting of risks depending on the identified risk rating.

The risk governance framework is provided in **Appendix 1** and outlined below:

Risk category	Definition	Relevant risk register and responsibility	SGSC (Enterprise Risk) review and reporting requirements
Strategic risks	Risks that may prevent the University from achieving its strategic objectives, as set out in the ECU Strategic Plan.	Strategic risk register, maintained in Riskware by Enterprise Risk.	Full review and update annually, reported to QARC and Council. Updates included in Strategic Risk Report twice per year to QARC and Council.
Enterprise-wide operational risks	Risks that impact the ability to achieve one or more operational objectives and have an impact on multiple processes, Schools or Centres.	Enterprise-wide operational risk register, maintained in Riskware by Enterprise Risk.	Full review and update annually, reported to RIMC. Updates included in Enterprise-wide Operational Risk Report four times per year to RIMC and twice per year to QARC.
Divisional operational risks	Risks which impact the ability of a School or Centre to achieve their operational objectives.	School and Centre operational risk registers, maintained in Riskware by Schools and Centres.	Full review and update annually. Updates included in Operational Risk Report three times per year to QARC.

Risk category	Definition	Relevant risk register and responsibility	SGSC (Enterprise Risk) review and reporting requirements
Functional risks: **Activity risks**	Risks associated with a specific activity, initiative or event, such as a research project; Work Integrated Learning placement; large scale event, etc.	Activity risks in Riskware, maintained by relevant risk owner.	Performed as required and reviewed in line with activity requirements. Reported as required to QARC.
Functional risks: **Project risks**	Risks associated with a specific project. Project risk registers are required for all significant projects under the remit of the University Project Management Office.	Project risk registers in Riskware, maintained by relevant project manager.	Performed as required for significant projects and reviewed in line with project requirements. Reported as required to QARC.
Work health and safety risks	Risks associated with health and safety hazards, which is anything that may result in injury to a person or harm to the health of a person.	Risk registers in the Work Health & Safety (WHS) module of Riskware, maintained as per the WHS Hazard Identification and Risk Management Guideline.	Reporting undertaken by People & Culture.

It is noted that there are often relationships between different levels of risks. As such, where possible, the linkage between risks at different levels (e.g. strategic and operational risks) will be highlighted as part of the capture of the risk.

5. RISK APPETITE

The University maintains a risk appetite statement which sets out the degree of risk the University is willing to accept in the pursuit of its strategic objectives.

The risk appetite statement is established by Council and is reviewed annually by the Vice-Chancellor and University Executive, endorsed by the Quality, Audit and Risk Committee ("QARC") and approved by Council.

Controlled Entities may maintain separate Council-approved Risk Appetite Statements which are aligned to their strategy and operations, and in accordance with the relevant Council-approved governance frameworks for Controlled Entities.

6. RISK ASSURANCE

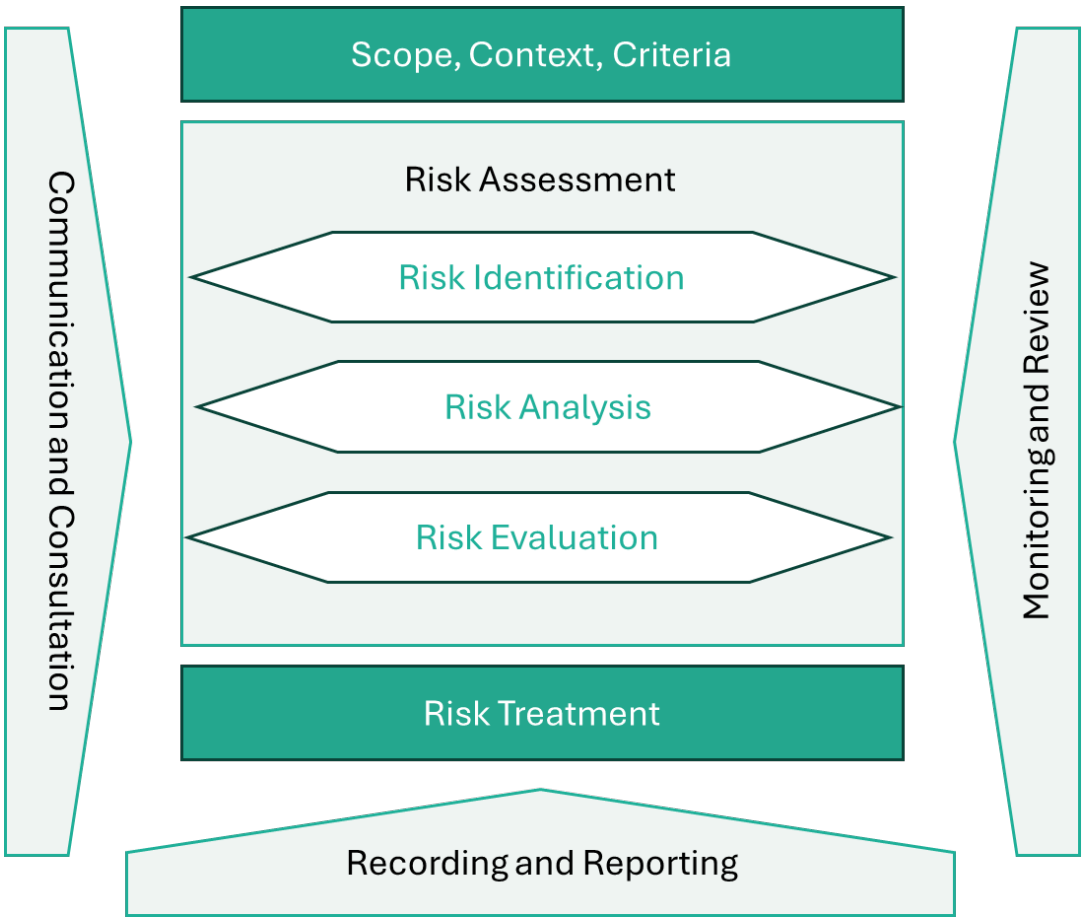
The University adopts a 'three lines of defence' model of risk assurance to support accountability in risk management through a layered defence approach.

The three lines of defence are articulated in the Integrated Assurance Framework, which is a structured means of identifying and mapping the main sources and types of assurance occurring throughout the University and coordinating them in an effective and efficient manner.

The objective of the ECU Integrated Assurance Framework is to provide Council, QARC and the University Executive with a holistic view of assurance across the University's material business processes.

7. RISK MANAGEMENT PROCESS

The risk management process adopted by the University reflects the international standard on risk management, AS/NZ ISO31000:2018 *Risk management – principles and guidelines*, as set out in the figure below:



Further guidance on the enterprise risk management process is provided overleaf.

Step	1. Establishing the context	2. Risk assessment	3. Risk treatment	4. Recording and reporting	5. Monitoring and review	6. Communication and consultation
Objective	To set the scope, context and criteria of the risk assessment	To identify, analyse and evaluate the risk and assign a risk rating.	To determine what risk treatment is required to manage the risk.	To ensure risks are recorded and reported.	To identify, analyse and evaluate the risk and assign a risk rating.	To ensure appropriate stakeholders are involved in the risk management process.
Description	This step can be regarded as the planning phase of the risk assessment. The subject of the risk assessment is defined and placed into context and the level of effort is tailored appropriately. The risk owner identifies the primary affected business area, risk type and risk category.	The risk is described in terms of what could go wrong, in other words, the uncertainty of achieving the objectives. The risk identified must be relevant to the subject matter, appropriate given the context and useful for decision-making. Risk analysis involves determining the causes and consequences; as well as the existing controls that are in place to mitigate the risk. The risk is then evaluated by determining the likelihood of the risk occurring and the consequence if it does occur, by applying ECU's risk matrix. The result is a current risk rating.	There are two options for managing a risk: Accept the risk, based on the current risk rating and strength of existing controls. Reference should be made to the risk rating and ECU's risk acceptance criteria as well as ECU's risk appetite statement. Treat the risk, based on the view that further action is required to mitigate the risk to an acceptable level. Risk treatment plans should be developed which are specific, measurable, actionable, realistic and time specific. Once risk treatment plans have been developed, the risk must again be evaluated against ECU's risk matrix to	ECU uses Riskware's Enterprise Risk module as its enterprise risk management system. All risks should be recorded in Riskware to enable a holistic view of risk across the university. Various reports can be produced from Riskware and risk information is used to report to University Executive, QARC and Council. Work health and safety risks are recorded separately in the WHS module of Riskware, as per the Work Health and Safety Hazard Identification and Risk Management Guideline.	Monitoring and reviewing risks is an integral part of managing risks. The risk rating will determine how often a risk should be reviewed, in alignment of ECU's risk acceptance criteria. These parameters are built into Riskware which will provide notification to the risk owner when risk reviews are due. Risk treatment plans should also be reviewed regularly, and updates made to the completion progress.	During the initial planning process (refer step 1), attention must be given to the relevant stakeholders to involve in the risk management process. This will often be representatives from the relevant business area and may involve technical subject matter experts, such as Work Health and Safety; or external parties if relevant. Communication and consultation with stakeholders continues throughout the risk management process.

Step	1. Establishing the context	2. Risk assessment	3. Risk treatment	4. Recording and reporting	5. Monitoring and review	6. Communication and consultation
			determine a residual risk rating. This rating will drive the frequency of future risk reviews. If the risk has been accepted, the current risk rating will be the same as the residual risk rating.			
Reference documents	Relevant internal and/or external documents such as strategies, policies, plans or analyses.	ECU Risk Matrix (**Appendix 2**)	Risk acceptance criteria (included in ECU Risk Matrix, **Appendix 2**)	n/a	Risk acceptance criteria (included in ECU Risk Matrix, **Appendix 2)**	n/a
Where to record Riskware	Step 1 – Classify the risk (basic risk information) Step 2 – Risk consequence category Step 3 – Detailed risk description (use this to add contextual commentary)	Step 4 – Risk description (title of the risk) Step 5 – Risk consequence Step 6 – Risk source/causal factor Step 7 – Existing controls Step 8 – Current risk rating	Step 9 – Risk treatment option Step 10 – Risk treatment plan Step 11 – Who is responsible and by when? Step 12 – Residual risk rating	Enterprise Risk module of Riskware	Step 11 – Who is responsible and when (for treatment plan reviews)	n/a
Riskware Quick Guide	*Riskware ERM – How to Create a New Risk*	*Riskware ERM – How to Create a New Risk*	*Riskware ERM – How to Create a New Risk*	*Riskware ERM – Generating Reports* *Riskware ERM – How to Filter*	*Riskware ERM – Actioning Emails*	n/a

Appendix 1

ECU RISK GOVERNANCE FRAMEWORK

Governance bodies/committees

University Council
Oversight of Risk Management across the University. Approve the Risk Framework and Risk Appetite Statement.

→

Vice-Chancellor
Responsible for ensuring that a Risk Management Framework is established, implemented and maintained.

→

Quality, Audit and Risk Committee
Assists Council in fulfilling and discharging its responsibilities by providing independent and objective advice.

→

University Executive & Senior Management
Supports VC by assessing and managing risks to the University and their portfolio's objectives and strategies.

→

Risk & Incident Management Committee
Provides oversight of the Enterprise-wide Operational Risk Register

Approve

Monitor

Risk categories	Reporting			Assurance	
Strategic risks	UE & SM SGSC checks in twice a year.	QARC Twice a year	UC Annually	Risk reviews (including periodic deep dives)	Internal Audit
Enterprise - wide operational risks	UE & SM SGSC checks in four times a year.	RIMC Four times a year	QARC Twice a year (in line with strategic risk updates)		
Divisional operational risks	UE & SM SGSC provides updated reports after annual workshops	QARC Three times a year			
Functional risks (Projects and Activity)	UE & SM SGSC provides updated reports after project workshops/ as required	QARC As required			

Exceptions: WHS risks: Managed and reported by P&C. City Campus Project: Separate Governance process.

Appendix 2

RISK CONSEQUENCE RATING

		Minor	Moderate	Substantial	Major	Catastrophic
		1	2	3	4	5
Service Delivery & Performance		Negligible impact on the delivery of services. No impact on performance targets.	Isolated disruption to teaching, research or professional activities affecting service delivery and performance targets for a short-term period.	Interruption to teaching, research or professional activities for protracted period. One or more areas at significant risk of performing under target.	Sustained disruption to teaching, research or professional activities. Inability to meet one or more performance targets.	Cessation of teaching, research, or professional activities. Risk of total failure to meet performance targets.
Operations & Infrastructure		Minor disruption to systems, operations or infrastructure which does not affect the delivery of services.	Disruption to systems, operations or infrastructure affecting isolated group of stakeholders.	Significant disruption or loss of systems, operations or infrastructure which causes widespread disruption.	Disruption or loss of critical systems, operations or infrastructure affecting a large part of the University.	Failure or loss of critical systems, operations or infrastructure affecting viability of the University.
Financial	Overall	Minor impact on budget or funded activities.	Financial loss requiring corrective action within existing resources.	Substantial financial loss requiring reallocation of resources.	Major financial loss requiring adjustment or cancellation of funded projects.	Significant financial loss threatening viability.
	School / Centre	< $10k, or 0.5%	$10k to $100k, or 0.5% -1% of budget	$100k-$1m, or 1-5% of budget	$1m to $5m, or 5-10% of budget	> $5m, or 10% of budget
	ECU-wide	< $0.5m	$0.5m to $2.5m	$2.5m to $10m	$10m - $20m	> $20m
Brand, Reputation & Engagement		Isolated media attention. Little to no broader stakeholder interest.	Minor adverse media attention, but no impact to reputation or lasting concern to stakeholders.	Substantial short-term damage to reputation of a section of the University. Short-term adverse media attention. Impact on key partnerships.	Major negative publicity and damage to University reputation. Major adverse media attention. Breakdown or termination on operational partnerships.	Reputation and standing of the University affected. Long-term adverse media attention. Breakdown, or termination of strategic partnerships.
Governance & Compliance		Minor breaches of policies, rules or regulations with negligible impact.	Breaches of policies, rules or regulations that are isolated, with limited legal or regulatory impact.	Breaches of policies, rules, regulations or legislation that are systemic, or may result in legal or regulatory action.	Breaches of policies, rules, regulations or legislation that will result in legal or regulatory action including investigations and/or significant penalties.	Breaches of policies, rules, regulations and laws that will result in significant penalties and/or loss of critical approvals, accreditations or registrations.
Work Health & Safety		No injury or illness sustained or minor first aid or non-medical treatment required only, e.g. band-aid, icepack or non-prescription medication.	Medical treatment by a health professional and/or restricted work duties/hours, e.g. stitches or issuing of prescription medication. No time off work.	Injury or illness that would typically result in lost time and multiple medical treatments.	Serious injury or illness typically resulting in extensive lost time and/or requiring WorkSafe notification, e.g. hospital in-patient treatment; serious head or eye injury.	Single or multiple fatality.

RISK ACCEPTANCE CRITERIA

Level of risk	Delegation	Acceptance criteria	Review period
Low	Supervisor / Team Leader	**Acceptable with periodic review.** Exposure to this level of risk is acceptable without additional risk treatments.	Review period should not exceed 12 months.
Moderate	Manager / Associate Dean	**Acceptable with periodic review.** Exposure to this level of risk is acceptable, provided an appropriate assessment has been conducted. Consideration should be given if whether any treatments are required.	Review period should not exceed 12 months.
Substantial	Executive Dean / Dean / Director	**Acceptable with ongoing review.** Exposure to this level of risk may only continue with effective mitigating controls or an appropriate treatment plan.	Review period should not exceed 6 months.
High	Deputy Vice-Chancellor / University Executive	**Unacceptable without effective mitigating controls or treatment.** Exposure to this level of risk may only continue with effective mitigating controls (rated moderately effective and above) and/or an appropriate treatment plan to reduce the risk/manage the risk exposure.	Review period should not exceed 3 months.
Extreme	Vice-Chancellor / University Council	**Unacceptable.** Exposure to this level of risk should be immediately discontinued except in extreme circumstances. In extreme circumstances, it requires urgent attention and treatment plans to support the implementation of effective controls should be designed and implemented as a priority	Review period should not exceed 1 month.

RISK RATING SCALE

Level of risk	Minor (1)	Moderate (2)	Substantial (3)	Major (4)	Catastrophic (5)	
	Moderate (5)	Substantial (10)	High (15)	Extreme (20)	Extreme (25)	5
	Low (4)	Moderate (8)	Substantial (12)	High (16)	Extreme (20)	4
	Low (3)	Moderate (6)	Moderate (9)	Substantial (12)	High (15)	3
	Low (2)	Low (4)	Moderate (6)	Moderate (8)	Substantial (10)	2
	Low (1)	Low (2)	Low (3)	Low (4)	Moderate (5)	1

RISK LIKELIHOOD RATING

Rating	Probability	Description
Almost certain	> 80%	Event is expected to occur.
Likely	51 – 80%	Event will probably occur.
Possible	26 – 50%	Event may occur occasionally.
Unlikely	10 – 25%	Event is unlikely to occur but is a possibility.
Rare	< 10%	Event is conceivable, but very unlikely to occur.