Enterprise Risk Management

1. PREAMBLE

1.1 Charles Darwin University (the University) is committed to the management of risk and fostering a culture of risk management. The University recognises that risk at the heart of everything it does and to be successful, the University must take risks knowingly and manage risk to an acceptable level.

1.2 Enterprise risk management (ERM) is the process of identifying and addressing the potential events that represent risks to the achievement of strategic goals, or to opportunities to gain competitive advantage. ERM is an integral and inseparable part of good governance, management practice, performance culture and processes that are the core of University business.

1.3 The University is committed to embedding enterprise risk management within its learning and teaching, research, operations and commercial activities.

2. PURPOSE

2.1 The Enterprise Risk Policy (policy) communicates the University's commitment to managing enterprise-wide risks and establishes clear expectations to ensure the CDU community are aware of their responsibilities for managing risk

3. SCOPE

3.1 The Enterprise Risk Management Policy (policy) applies to:

a. all members of the University community, including Council members, Board and Committee members, staff, students, contractors and adjuncts of the University; and

b. all activities under the control of the University.

4. POLICY PRINCIPLES

Risk Management Principles

4.1 In line with the International Standard *ISO 31000:2018 Risk management - Guidelines*, the University's risk management principles are:

a. **Integrated**: Risk management is an integral part of all University activities;

b. **Structured and Comprehensive**: A structured and comprehensive approach to risk management contributes to consistent and comparable results;

c. **Customised**: The risk management system and processes are customized and proportionate to the University's external and internal context related to its strategic goals;

d. **Inclusive**: The 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; and

h. **Continual Improvement**: Risk management is continually improved through learning and experience.

Enterprise Risk Management Framework

4.2 The key components of the University's Enterprise Risk Management Framework are:

a. the Enterprise Risk Plan;

b. this policy;

c. the risk management methodology and processes, as set out in the Risk Management Procedures (to be developed 2022);

d. the risk appetite statement and KRI's (to be developed 2022);

e. the Strategic Risk Register;

f. the Corporate Risk Register;

g. the Emerging Risk Register;

h. the Risk Assessment Criteria and Risk Matrix;

i. the Risk Management Training Program (to be developed 2022);

j. the Risk Management Communications Plan (to be developed 2022);

k. the Risk Management Governance Structure – Council and relevant Boards and Committees;

l. the Compliance Management Policy;

m. the Internal Audit Plan;

n. Compliance Plan

o. Insurance arrangements;

p. Other University policies and procedures relating to specific areas of risk, including as health, safety and environment; emergency planning and business continuity; incident management; fraud and corruption; conflicts of interest; privacy and cyber / information security; and

q. External Audit.

5. Risk Management Roles and Responsibilities

5.1 The key risk management roles and responsibilities are:

a. **Council**: Ultimately responsible for overseeing risk management across the University and articulating its willingness to take risk through the approval of risk appetite statements. Council is supported in the discharge of its risk management responsibilities by the Audit, Risk and Compliance Committee.

b. **Audit, Risk and Compliance Committee (ARCC)**: Responsible for ensuring that an appropriate Risk Management Framework is in place across the University that is fit for purpose, operating as intended and that key risks to the achievement of the strategic goals are managed within risk appetite. ARCC are supported in the discharge of their risk management responsibilities by the Finance and Infrastructure Development Committee and Academic Board.

Once printed, this Policy is considered an uncontrolled document. Only documents in the online Library are considered the most current version.

Page 2 of 5

c. **Finance and Infrastructure Development Committee**: Responsible for the identification of risks to the University's financial viability and sustainability.

d. **Academic Board**: Responsible for maintaining oversight of academic risks, including academic and research integrity.

e. **Leaders**: Responsible for ensuring that risks to the achievement of the strategic goals are identified, assessed and managed and for ensuring that all parts of the University implement the requirements of the risk management framework.

f. **Colleges and Business Areas**: Responsible for identifying, assessing and managing risk within their own area of responsibility and for implementing the requirements of the risk management framework and for providing assurance to University executive management that it has done so.

g. **University Secretary**: Responsible for establishing and implementing high-quality governance practices, which includes risk management, to meet CDUs compliance obligations.

h. **Head of Risk and Assurance**: Responsible for:

   i. oversight of risk management, including oversight and challenge of the University's systems and controls in respect of risk management;

   ii. ensure the adequacy of risk information, risk analysis and risk training provided to staff;

   iii. report to the appropriate governing bodies on the University's risk exposures relative to its risk appetite; and

   iv. developing, implementing, maintaining and evolving the enterprise risk management framework and for challenging all aspects of decision making across the University from a risk perspective.

i. **All Managers**: Have responsibility for identifying, assessing and managing risk within their own area of responsibility, for implementing agreed actions to manage risk and for reporting activities or circumstance that may give risk to new or changed risk.

j. **Risk Owners**: Responsible for:

   i. complying with the risk management framework in respect of owned risk - identification, assessment, escalation, reporting and monitoring

   ii. overseeing the delivery of key action plans agreed with action owners;

   iii. documenting and keeping up to date the risk and control information in the relevant University risk register;

   iv. monitoring the status of owned risks with a particular focus on monitoring circumstances that may alter the severity of assessed risks; and

   v. providing reports on owned risks to the Executive Team and the Audit Risk and Compliance Committee, on request.

k. **All Staff**: Responsible for being aware of the requirements of the risk management framework; identify and escalate risk; and exercise a duty of care.

l. **Internal Audit**: Responsible for developing a risk-based internal audit programme to audit the risk processes across the University, receive and provide assurance on the management of risk, and report on the efficiency and effectiveness of internal controls in place and operating to manage risk.

5.2   Specific risk management responsibilities of the Council and its Boards and Committees are defined in their respective terms of reference.

6. NON-COMPLIANCE

6.1 Non-compliance with Governance Documents is considered a breach of the Staff Code of Conduct or the Student Code of Conduct and is treated seriously by the University. Reports of concerns about non-compliance will be managed in accordance with the applicable disciplinary procedures.

6.2 All staff members have an individual responsibility to raise any suspicion, allegation or report of fraud or corruption in accordance with the Fraud and Corruption Control Governance Framework, Fraud and Corruption Control Policy and Whistleblower Reporting (Improper Conduct) Procedures.

RELATED AND SUPPORTING DOCUMENTS

Legislation	N/a
Policy	CDU Strategic Plan 2021-2023 All CDU Policies
Procedure	All CDU Procedures
Other	International Standard for Risk Management ISO 31000:2018
Definitions	CDU Glossary

GOVERNANCE

Responsible Executive	University Secretary	
Implementation Officer	Head of Risk and Assurance	
Category	Governance	
Approving authority	Council	
Effective date	8 December 2021	
Review date	8 December 2022	
Version	3.00	POL-036
Content enquiries	governance@cdu.edu.au	

DOCUMENT HISTORY AND VERSION CONTROL

Version	Date Approved	Approved by	Brief Description
1.00	4 May 2008	Council	• Creation of original document and upload to CDU website.
1.01	29 Dec 2010	Governance	• Convert document to new template. • Add statement of authority, relevant definitions, document history and version control and essential documents in keeping with new policy format. • Amend minor grammatical and spelling errors

Once printed, this Policy is considered an uncontrolled document. Only documents in the online Library are considered the most current version.

Page 4 of 5

			• Amend Audit and Risk Committee to Finance, Risk and Review Committee to reflect change in committee title. • AS/NZS 4360 replaced with ISO31000:2009
1.03	10 Jan 2012	Governance	• Removal of reference to Finance, Risk and Review Committee as no longer active. • Amended position titles in accordance with new organisational chart. • Update hyperlinks • Minor changes to grammar and formatting
1.04	13 Feb 2013	Governance	• Converted document to current template • Addition of relevant definitions • Updated and added hyperlinks • Minor changes to wording, formatting and grammar
1.05	15 Dec 2017	Governance	• Conversion to new Governance template due to new University branding • Updated definitions • Updated hyperlinks
2.00	11 Jun 2020	Council	• Now called Enterprise Risk Management Policy • Complete review of document (internal Controls Policy now rescinded)
3.00	8 Dec 2021	Council	• Complete review of policy

Once printed, this Policy is considered an uncontrolled document. Only documents in the online Library are considered the most current version.

Page 5 of 5