Enterprise Risk Management Framework

Section 1 - Introduction

(1) The purpose of the Enterprise Risk Management Framework ("ERMF") is to provide a comprehensive approach to managing risks within the context of ACU's current and potential operating environment. ACU recognises that having an industry best practice framework provides all stakeholders with confidence that risks are not only understood and managed by the Senior Executive at ACU, but also are consciously prioritised, mitigated and linked to strategy from a day to day operational perspective by all staff.

(2) In developing the ERMF, consideration has been given to the important relationship between the ACU Mission, Identity and Values and ACU Strategic Plan and the interplay and impact of vulnerabilities and opportunities that the concept of "risk" represents.

(3) Mission: ACU Mission, Identity and Values define our purpose. They provide direct insight into who we are, what we do and whom we serve. At ACU, our mission is expressed as: Within the Catholic intellectual tradition and acting in Truth and Love, Australian Catholic University is committed to the pursuit of knowledge, the dignity of the human person and the common good.

(4) Vision: Our Vision defines our aspirations. We express our vision in terms of creating a future of Hope, faith and reason through opportunity, innovation and ethics.

(5) Strategic Goals: To realise ACU Mission, Identity and Values, ACU has identified 6 Strategic Goals for 2020-2023:

- a. All our endeavors, grounded in mission.
- b. Distinctively Catholic, inclusive, dynamic and student-centered education.
- c. World-leading research, with impact.
- d. Vibrant academic culture, enriched by innovation and discovery.
- e. Deeply engaged, globally renowned.
- f. Service, stewardship and sustainability.

(6) Risk: In pursuing its mission, vision and strategic goals, ACU acknowledges the reality of uncertainty and how this might impact the success of ACU's objectives. The ERMF is designed therefore to support ACU's capabilities to manage risk.

(7) 'Risk' is therefore described as: Threats to ACU's ability to deploy, balance and manage its resources and environment as it pursues its Mission, Vision and Strategic Goals.

Section 2 - ERMF Key Objectives

(8) The ERMF is designed to:

- a. support ACU's capabilities to manage known risks, knowable risks and unknown risks;

b. provide structure and context for all business operations and decision making where risk prevails; and

c. assist management and staff in determining which risks are significant and which ones are not, so that time, energy and resources can be invested most effectively and efficiently.

Section 3 - ACU's Risk Management Obligations

(9) ISO 31000:2018 - Risk Management Guidelines (codified by the International Organization for Standardization) defines risk as the "effect of uncertainty on objectives". ACU's interpretation of risk aligns with ISO31000, as it considers its capacity to respond to elements or events that impact its purpose. It also aligns to the principles set out by COSO (Committee of Sponsoring Organizations of the Treadway Commission) in its 2017 Enterprise Risk Management – Integrating with Strategy and Performance (Integrated Framework).

(10) ACU seeks to comply with the following State and federal legislation relating to risk management:

Legislation and Standards	Requirement
Legislation and Standards Higher Education Standards Framework (Threshold Standards) 2021; National Code of Practice for Providers of Education and Training to Overseas Students 2018	Requirement 6.2.1(e) - Risks to higher education operations have been identified and material risks are being managed and mitigated effectively Provides nationally consistent standards and procedures for registered providers of education and training. (TEQSA is responsible for monitoring registered higher education provider's compliance with the National Code).
Legislation and Standards ASQA/ELICOS	Requirement Section 190 of the National Vocational Education and Training Regulator Act 2011
Legislation and Standards Australian Charities and Not-for-profits Commission Act 2012 (Cth)	Requirement Chapter 3 Part 3.1 Div. 45.5.1(c) registered entities must minimise the risk of mismanagement and misappropriation. Risks of terrorism, fraud and other forms of abuse must be reduced through good standards of governance and accountability
Legislation and Standards Work Health and Safety Act 2011 (QLD)	Requirement Part 2 1.1.(17) persons who have a duty to ensure health and safety must 'manage risks' by eliminating health and safety risks so far as is reasonably practicable, and if it is not reasonably practicable to do so, to minimise those risks so far as is reasonably practicable

Section 4 - Key Framework Components

(11) ACU's ERMF components include:

Foundations and Principles	• Risk Culture • Strategic and Business Planning • Risk Appetite
Facilitation and Governance	• Data and Infrastructure • Responsibilities and Accountabilities • Policies and Procedures
Risk Control	• Risk Management Process • Internal Control • Critical Incidents and Business Continuance Planning • Fraud Control • Stress Testing

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of staff printing this document to always refer to the ACU Policy Portal for the latest version.

Page 2 of 9

Performance and Effectiveness Reviews	• Quality Assurance • Variance analysis • Compliance • Reporting and Monitoring

Foundations and Principles

Risk Culture

(12) Risk Culture is described as the "norms and traditions of behaviour of individuals and groups in an organisation that determine how they identify, understand, discuss and act on risks" (ACU Risk Culture Review Internal Audit Reference 05/2017 ACU). Essentially, Risk Culture reflects management and staffs' collective ability to 'do the right thing' – to take the right risk, with the right controls, for the right return. It considers whether staff operate consistently within the organisation's risk appetite, what people do when they are not being watched, how they behave when they have not been told what to do and ultimately their genuine commitment to achieving the organisation's strategic goals.

(13) A positive risk culture necessarily underpins all risk management activity at ACU for without it, the ERMF remains vulnerable. ACU's approach to risk management is therefore consciously embedded through the organisation's culture, capabilities and practices.

a. Commitment to proactive risk management is set and supported by the Vice-Chancellor and President, Senate and Senate's sub-committees.
b. ACU supports an environment where all members of the ACU community are encouraged and empowered to identify and manage risk, or where appropriate, escalate it to a more senior level.
c. Risk management capabilities and competencies are considered within employment, performance and professional development practices. Where appropriate, Key Performance Indicators link reward to the outcomes of prior period risk decisions therefore providing an important lever to influence positive employee risk behaviour.
d. Ongoing education in risk concepts, compliance requirements and related practices are provided for all staff.
e. Internal and external risk management expertise supports ACU through advice, infrastructure, systems and quality assurance processes which have necessary authority to conduct activities in an effective and independent manner.

(14) Risk culture at ACU is subject to ongoing review in order to ensure that strengths, potential challenges and key opportunities continue to be identified and evolve positively. This ensures that ACU's ERMF continues to be anchored with solid foundations which promote a balanced risk / value based approached within all decisions, operations and activities.

Stragegic and Business Planning

(15) ACU recognises the essential link between strategy and business planning and risk. The ACU Strategic Plan and business unit planning process consciously considers an extensive myriad of risks within the current and future business context, and value-based risk mitigation responses (including strategy alternatives) are considered when developing plans to support performance objectives, targeted benchmarks and agreed KPI. Integrating enterprise risk management into strategic and business planning processes helps ACU to reduce surprises and related costs and losses, reduce performance variability, improve resource deployment and enhance enterprise resilience.

(16) In order to directly link and drive strategic performance, ACU has incorporated its six strategic priorities as per the 2020-2023 Strategic Plan into its CARM Risk Management system for capturing, assessing, responding and monitoring risks. Key Performance Indicators aligned to these strategic priorities and variance benchmarks thus from,

provide consequence baselines for assessing the impact of risks and assist to drive risk mitigation response and action when appropriate.

Risk Appetite

(17) Risk appetite represents the nature and level of risk that ACU is willing to accept in the pursuit of its strategic priorities, its mission and vision (as confirmed and approved by the Audit and Risk Committee (ARC) under the authority of Senate). ACU recognises the importance of risk appetite as a key component in setting the strategic direction of the University. It also acknowledges that risk appetite is not something that is fixed and rigid; rather it dynamically evolves through time, responding to a number of different drivers including but not limited to capital strength, business performance, employee capability and capacity, culture, infrastructure and system capability, competitor behaviour, exogenous macro-economic forces, regulatory and legislative requirements, and stakeholder expectation including the Catholic Church. It therefore reviews and approves its [Risk Appetite Statement](#) (RAS) annually.

(18) The [Risk Appetite Statement](#) reflects ACU's appreciation that:

    a. risk exists in the very nature of pursuing a purpose;
    b. risk underpins all efforts employed to achieve ACU's strategic goals;
    c. an overly risk-adverse attitude may hinder or minimise its ability to advance its purpose.

and its appetite for risk must:

    a. be congruent with its focus areas of opportunity, innovation and ethics;
    b. reflect due regard to its stakeholders, community and environment;
    c. be commensurate with potential reward;
    d. sometimes be different at an activity level from that at a whole of institution level;
    e. reflect its capacity to respond and manage risks.

(19) ACU also acknowledges that in determining its risk appetite, preservation of its license to operate, remains fundamental to its ability to pursue its mission, vision and strategic goals. As such, ACU acknowledges TEQSA's (Tertiary Education Quality and Standards Agency) interest the amount of risk ACU seeks and accepts, as they serve to protect student interests and the reputation of Australia's higher education sector.

Facilitation and Governance

Data, Human Resources and Infrastructure

(20) Central to the ERMF is the reliability of quality data, human resources and infrastructure that can support and deliver information, analysis and decision making accurately and efficiently. ACU's Data Strategy Framework has been developed to ensure that all data needed, created and stored at ACU is

    a. appropriately accessible,
    b. is accurate,
    c. is consistent,
    d. is supported by secure, efficient technology and
    e. is maintained in accordance legislative, industry and internal standards.

(21) ACU's Capacity Development Framework describes the essential competencies that are needed in all ACU staff to achieve our strategy and support our mission. Risk management training is provided to all staff relevant relative to their position and responsibilities, including at the very basic level:

a. workplace health and safety;

b. critical incidents;

c. discrimination, harassment and bullying; and

d. privacy.

(22) ACU's Campus Development Framework ensures infrastructure and project needs are well considered with respect to alignment to:

a. [ACU Strategic Plan](#)

b. theand the Mission and Identity of the University;

c. investment of capital

d. local and national perspectives for the student experience

e. community engagement and placemaking

f. campus context and heritage

g. sustainability

Responsibilities and Accountabilities

(23) Accountability for the management of risk at ACU exists at two levels. The first and primary accountability rests with the Senate (and its sub-committees). The second rests with Management in the execution of this ERMF and the application of the Three Lines of Defence model.

The Senate and Its Sub-committees and Governing Bodies

(24) The University Senate is the governing authority of ACU. Members of the Senate are the Board of Directors. The ACU Senate has 4 sub-committees which includes:

a. Finance and Resources Committee;

b. Audit and Risk Committee;

c. Senate Standing Committee;

d. Honorary Awards Committee.

(25) An Academic Governing Body (Academic Board) also operates under the direction and authority of the Senate and is served by:

a. the Chair, Academic Board;

b. the Courses and Academic Quality Committee;

c. Faculty Boards;

d. the Student Administrative Lifecycle and Policy Committee;

e. the Internationalisation Committee;

f. the University Learning and Teaching Committee;

g. the University Research Committee

(26) The management of risk is implied within the governance obligations and terms of reference within each Senate Sub-Committee and the Academic Board. However, the Audit and Risk Committee (ARC) has overarching responsibility for ensuring ACU risk management practices are effective and consistent, so that ACU maintains its status as a quality and low risk higher education provider. ARC sets the risk appetite of ACU (through development and recommendation for Senate approval) and confirms relevant risk management policies and key risk management procedures including the development and management of the University's strategic and operational risk registers. The ARC regularly

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of staff printing this document to always refer to the ACU Policy Portal for the latest version.

Page 5 of 9

engages with Management to oversee the status of risk management activities, adherence to risk limits and policies, quality assurance and issues raised through various risk management reports.

Auxillary Oversight Committees

(27) Auxillary Oversight Committees:

 a. Risk Advisory Group
 b. WHS Committee
 c. Cyber Security Risk Committee

Management and Employee Responsibilities

(28) ACU has a clear expectation that all Management and employees are responsible for risk. ACU has adopted the Risk Management Accountability - Three Lines of Defence Model to establish boundaries and assign responsibilities, to avoid gaps in controls and unnecessary duplication of coverage and to deliver strong, integrated and cost-effective University-wide assurance activities.

Delegated Authorities

(29) The Constitution of the Australian Catholic University enables Senate to delegate its powers under the Constitution to Officers of the University for devolved decision making across the University. Delegations are position-specific and represent not only the authority to commit the University and or incur liabilities for the University but strict limits on these authorities as well.

Policies and Procedurs

(30) Policies are an official position statement of the University and establish the key principles and provisions that govern decision-making processes. Policies provide details of the University's expectations and how it will act. While some policies can stand alone, most will be accompanied by associated procedures and / or guidelines to explain how the policy is to be implemented across the University. All Policies and Procedures are core to the University's ERMF. ACU maintains a Risk Management Policy and Risk Management Procedure which are cornerstone to ACU's risk management process.

Risk Control

Risk Management Process

(31) Risk management is an important part of University decision-making. It supports ACU's activities and ensures operational plans align with strategic priorities. ACU applies the ISO 31000 Risk Management Process to manage risk.

Internal Controls

(32) As part of the ERMF, internal controls have been implemented across ACU to ensure that risk is appropriately captured and identified, it is assessed correctly and consistently, appropriate response to manage risk occurs on a timely and effective basis and that risk is monitored and reported to responsible managers as well as the ARC. These controls support the proactive management of risk, including the regular maintenance of risk registers through the CARM Risk Management System.

(33) ACU aims to comply with all relevant laws, rules, regulations industry standards and codes, internal policies and procedures while keeping pace with changing community and stakeholder expectations. ACU acts quickly to correct incidents of non-compliance and determine whether a compliance failure is a breach that is reportable to regulators.

(34) Executive managers provide annual due diligence attestations to confirm the status of compliance within there

area of responsibility. This compliance status including actual and potential breaches is reported to the Standards and Compliance Committee as well as other oversight committees who have responsible interest.

Critical Incidents, Disaster Recovery and Bu siness Continuity Planning

(35) ACU maintains a Critical Incident Management Program which is the schedule of activities to ensure that the [Critical Incident Management Policy](#), [Critical Incident Management Procedure](#), roles and staff remain aligned. The Program falls within the overarching Critical Incident Management Framework.

Fraud Control

(36) ACU maintains a [Fraud and Corruption Control Framework](#) complete with policy, procedures and plan. It considers fraud in terms of two approaches: foundations of fraud (leadership, culture, governance and legislation) and strategic response (identification and assessment, prevention, detection, responsibility).

Stess Testing

(37) Improvements in risk management and planning are depended on properly understanding the consequences of change in the internal and external operating environment. To this end, "stress-testing" and scenario analysis is undertaken across key variables strategically critical to ACU's business, to better support Senate and management to assess risk, improve decision-making and support responsiveness and resilience.

Performance and Effectiveness

Quality Assurance

(38) ACU maintains a quality assurance programme which identifies and considers risks to ACU's quality management and continuous improvement commitment. Thematic and Functional Reviews are conducted as part of a rolling quality assurance schedule, to ensure that ACU is meeting the minimum standards of the [Higher Education Standards Framework (Threshold Standards) 2021](#), and ACU's continued alignment with its strategic priorities, mission and vision. Internal Audit consider risks to ACU's control environment and make recommendation upon strategic improvement. Annual reviews are conducted to ensure ACU's compliance with the [International Professional Practices Framework (IPPF)](#) and ongoing internal quality assurance surveys provide regular feedback on quality assurance effectiveness and application.

Variance Analysis

(39) Analysis of variances to budget and other key financial and strategic key performance indicators, including [TEQSA Risk assessment framework](#) is regularly conducted.

Compliance

(40) Compliance against the [Higher Education Standards Framework (Threshold Standards) 2021](#), ELICOS and [National Code of Practice for Registration Authorities and Providers of Education and Training to Overseas Students 2018](#) as well as requirements of key professional Accreditation bodies (e.g. AMNAC, AITSL etc) is managed on an ongoing basis at a functional and operational level with oversight by the Standards and Compliance Committee. Compliance with Workplace Health and Safety regulations are managed though the WHS Management System with oversight by the WHS Committee. Compliance with information technology security and protocols is managed through the Cyber Security Risk Committee among others. Registers are maintained with regards to complaints, academic and research integrity issues, and issues related to student safety are provided for review and attention of the Academic Board. Both Internal Audit and External Audit contribute further to ensuring ACU complies with relevant prudential reporting and regulatory requirements.

(41) Risks within the University are monitored and reported at operational, functional, and Executive management levels. Risk registers are used to record and report all key risks across each Directorate, Faculty and Institute on an ongoing basis via the CARM Risk Management System. Risk Owners and Executive management have direct oversight of risk levels assessed, active controls and responsible action progress. Regular executive reporting related to Risk Registers, Internal Audit and Quality Assurance Reviews as well as key risk related correspondence from regulatory and accreditation bodies, is provided to the Audit and Risk Committee, Risk Advisory Group and Academic Board in accordance with their terms of reference. Reports relating to identification and analysis of emerging risks are provided as necessary and in consultation with management, Senate and related sub and auxiliary committees.

Section 5 - ERMF Review

(42) ACU's risk management capability and risk environment are constantly changing and evolving. In order to maintain agility, the identification of improvement opportunities and risk management maturity, the University's EFMR will be reviewed at least every two years

Section 6 - Further Assistance

(43) For further assistance, please contact the Director, Legal, Assurance and Governance.

Section 7 - Review

(44) Unless otherwise indicated, this Framework will still apply beyond the review date.

Section 8 - Associated Information

(45) For related legislation, policies, procedures and guidelines and any supporting resources, please refer to the Associated Information tab.

Status and Details

Status	Historic
Effective Date	9th February 2024
Review Date	30th April 2024
Approval Authority	Audit and Risk Committee
Approval Date	9th February 2024
Expiry Date	20th October 2024
Responsible Executive	Diane Barker Director, Legal, Assurance and Governance
Responsible Manager	Diane Barker Director, Legal, Assurance and Governance
Enquiries Contact	Legal, Assurance and Governance Directorate

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of staff printing this document to always refer to the ACU Policy Portal for the latest version.

Page 9 of 9