Risk Management Procedure

Section 1 - Governing Policy

(1) The Risk Management Procedure is governed by Australian Catholic University's (ACU) Risk Management Policy.

Section 2 - Scope and Application

(2) Risk management is incorporated into all areas of the University's operations and is the responsibility of all staff. Whilst specific staff may have explicit risk management responsibilities, it is the responsibility of all staff to be proactive in the University's risk management.

(3) This Procedure details the process and is encapsulated in four steps:

a. capturing identified risks within a defined context;
b. assessing and analysing risks;
c. responding to risks and assigning actions and
d. monitoring and reporting risks.

(4) This Procedure applies for the development and management of Organisational Unit Risk Registers, the University Strategic Risk Register as well as all Activity Risk Assessments conducted throughout ACU.

(5) Critical incident management and work, health and safety risks are covered by specific University policies and procedures.

Section 3 - Overview

(6) The University's Risk Management Policy and this Procedure are aligned with the Australian and New Zealand Standard AS/NZS (ISO 31000:2018 - Risk Management Guidelines) codified by the International Organization for Standardization (Risk Management—Principles and Guidelines).

(7) Once a risk has been identified within a defined context, the risk will be captured, assessed, responded to, managed, monitored and reported on an ongoing basis at nominated levels within the University in accordance with organisational responsibilities.

Section 4 - Risk Ownership

(8) Risk ownership ultimately resides with the Senate. Oversight of risk management is delegated by the Senate in accordance with the Delegations of Authority Policy and Register to the Audit and Risk Committee. Members of the Executive and Senior Management team are responsible for implementing risk management and managing risk within their areas of responsibility which includes the timely and effective identification, analysis, treatment, monitoring, and evaluation, and reporting of significant risks in their relevant Organisational Units (including performance of risk assessments related but not limited to specific events, commitments, activities, projects, and student placements).

Section 5 - Risk Management Model

(9) The Risk Management Model outlines the University's approach to risk management and integrates the Risk Management Principles and Risk Management Process so that it aligns with ISO 31000:2018 - Risk Management Guidelines.

ACU Risk Management Model	
Defining Context	Identify objectives of the activity or circumstances and consider / relate them to internal and external parameters within which the risk must be managed. Make clear the reasons for carrying out a risk assessment and provide a backdrop of circumstances against which risks can be identified and assessed. • set the scope; • define objectives (align to strategic priorities); • identify relevant stakeholders; • gather background information.
Capturing Identified Risks	Identify, define and capture the risks and opportunities including: • sources of risk; • areas of impact; • key category of risk: ◦ community wellbeing; ◦ culture and principles; ◦ education; ◦ financial viability or sustainability; ◦ governance; ◦ operational; ◦ project; ◦ reputational; ◦ research; and ◦ strategic. (to be selected only for the Strategic Risk Register). • events (including changes in circumstances); • causes and potential consequences; • factors that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives; and • issues associated with not pursuing or missing an opportunity Consider: • What could happen? • What are the potential outcomes, intended and unintended, both positive and negative? • What might go wrong, or what might prevent the achievement of the relevant goals? • What events or occurrences could threaten the intended outcomes? • How could it happen? • Is the risk likely to occur at all or happen again? • If so, what could cause the risk event to recur or contribute to it happening again? • Where could it happen? • Is the risk likely to occur anywhere or in any environment / place? • Or is it a risk that is dependent on the location, physical area or activity? • Why and when might it happen? • What factors would need to be present for the risk to happen or occur again? • What might be the impact? • If the risk were to eventuate, what impact or consequences would, or might this have? • Will the impact be felt locally, or will it impact the whole University? • Who does or can influence this activity? • How much is within the University's control or influence? • Are delegations, resources, budgets informed? • Can quantitative and / or qualitative data be used to describe the risk and support the risk rating? Key risks that might have an impact on the strategic priorities, mission and vision of ACU should be recorded in risk registers via the CARM Risk Management System. Detailed procedures for entering risks into CARM are available within the CARM User Guide. For Risk Assessments performed on specific projects, placements, WHS concerns, events etc, Risk Assessment Templates maintained by Faculties and Directorates should be used. Procedures for completing Risk Assessment Templates are documented within the templates themselves.

ACU Risk Management Model	
Assessing The Risk	Assess the risk to determine the likelihood and consequences of it occurring, and the effectiveness of existing controls. • Inherent Risk – consider the risk if no controls or other mitigating factors were in place in terms of likelihood and consequences. Rate the inherent risk using the Risk Matrix. • Existing Controls - Identify and record the existing controls and mitigating factors that are currently in place. • Residual Risk – Rate the risk again using the Risk Matrix considering how effective the existing controls are in reducing the risk. Have they impacted the likelihood and consequences of the risk occurring? Compare the residual risk against the Risk Treatment Tolerance Levels and determine if the risk is within or over acceptable limits.
Respond	For risks identified within proposed activities which ACU has not yet committed: • Before committing ACU to activities that expose the University to risk, it should be decided whether the individual or aggregate risks are reasonably acceptable, can be appropriately mitigated and managed, or preclude ACU from engaging and binding itself further to the activity. • Based on the risk assessment, if a risk is within tolerance levels, it can be accepted with no further treatment. This does not stop further treatment to be applied if considered practical. • If a risk is over tolerance levels, it should be mitigated appropriately with further action. • If a risk is over tolerance levels but mitigation is practically impossible, it must be referred to the Vice-Chancellor and President or the relevant member of the Senior Executive to the designated areas of risk ownership for acceptance. If that authority is not prepared to accept the risk commitment to the activity should not be provided and approved. For risks embedded in committed ACU activities: • Decide whether action is required to mitigate the risk with further action or controls. • If a risk is within tolerance levels, it can be accepted with no further treatment. This does not stop further treatment to be applied if considered practical. • If a risk is over tolerance levels, it should be mitigated appropriately with further action. • If a risk is over tolerance levels but mitigation is practically impossible, it should be referred to the Vice-Chancellor and President or the relevant member of the Senior Executive to the designated areas of risk ownership for acceptance. Risk Mitigation Strategies: Risk mitigation strategies and actions should be responsibly determined. Responsibility for actions and due dates should only be assigned with the agreement of all relevant parties in order to optimise the extent of effective application, as well as practical completion given resources and conflicting priorities. Ultimately, responsibility for management of risks remains with the risk owner, and not the action recipient and therefore it remains the risk owner's obligation to follow up actions to ensure risks have been properly mitigated. Risk mitigation controls can be: • Preventative – limit the possibility of the risk occurring. • Corrective – correct errors or system weaknesses. • Directive – encourage desirable activity (e.g. through policies and procedures). • Detective – identify through reviews, reconciliations, workshops etc. Other risk responses might include transferring the risk through insurance or contracting, or terminating the risk completely (e.g. activity or project)

ACU Risk Management Model	
Monitor and Report	The risk environment is constantly changing. It is important to continue monitoring and reporting risks to ensure management strategies remain appropriate. Monitor: • Context – for changes in circumstances, internal and external environment, University strategic or operational objectives, new sensitivities or appetites, stakeholders etc. • Elements and dimensions of risks that have been identified and captured previously as well as prevailing (new) risks. • Risk assessment likelihoods and consequences. • Response effectiveness, both in terms of application and whether they were successful in changing the risk's likelihood / consequence risk rating profile. All risks and the effectiveness of resposes should be reviewed by risk owners on a regular basis (at least monthly). Review: • The Assurance Unit will review and analyse risks reported throughout the University on an ongoing basis. Key risk reports will be provided to Senior Executives, Vice-Chancellor's Advisory Committee and Audit and Risk Committee in accordance with committee charters and terms of reference.
Communication	Effective communication and consultation are encouraged to enhance the risk management process and ensure the effective and timely decision making.

Section 6 - Risk Registers

(10) For the purpose of developing Organisation and Strategic (University / Executive) Risk Registers, ACU's enterprise risk management system (CARM) will be used. This system is a real time system, meaning that risks must be entered, updated, and managed on an ongoing basis. Likewise, actions must be updated and managed to ensure their status, related comments and context are current. Appendix 1 provides procedures for creating and managing ACU risk registers in ACU's enterprise risk management system.

Section 7 - Risk Assessments

(11) So that ACU can transparently and responsibly determine and protect optimal value and wellbeing to the University and its stakeholder community, a risk assessment must be undertaken for new strategic and operational activities prior to ACU:

a. making a commitment (any binding agreement) including an educational partnership;
b. incurring a significant liability;
c. applying resources, including in-kind contributions of time, effort or space;
d. engaging in Projects as defined by the Project Management Policy;
e. engaging in events;
f. investing in technology, infrastructure, or material plant and equipment; and
g. Committing staff or students to international travel.

(12) A risk assessment must also be undertaken with regards to ACU Workplace Health and Safety (WHS) requirements:

a. during annual and more frequent reviews of risks;
b. whenever working and learning areas are proposing to introduce changes that impact upon existing practices and risks; and
c. whenever Riskware reports expose gaps in the application and management of risk.

(13) Likelihoods and consequences (aligned consistently to ACU's enterprise exposure) must be considered to determine a risk rating and actions must be considered, to mitigate risks that are assessed to be over acceptable risk tolerance levels (as per the Risk Appetite Statement including the Risk Matrix and Likelihood and Consequence Baselines). Consultation with relevant stakeholders (including Office of General Counsel where appropriate) should be undertaken and if the commitment / liability / project / event / investment / travel etc is to be approved, then material risks identified must be transferred to the appropriate Strategic or Organisational Risk Register in ACU's enterprise risk management system for ongoing management and reporting. (Note: WHS risks must be categorised under "Community Wellbeing" and sub-categorised under "Work Health and Safety Management System".) These risks musts be reviewed on an ongoing basis to ensure mitigations are effective.

(14) ACU's general Risk Assessment Template (see also Section 14 – Appendix 2 below) and WHS Risk Assessment Form provide assistance in performing risk assessments.

(15) Risk Assessments must be stored appropriately within Directorates and Faculties, so that they may be easily accessible if required for information, analysis, review or evidencing purposes.

Section 8 - Workplace Health and Safety (WHS) Risk

(16) ACU maintains policies and procedures for the management of general and specific workplace health and safety risks with which all relevant stakeholders must comply. A comprehensive suite of WHS policies and procedure is provided on the People and Capability – Safety and Wellbeing portal.

(17) All identified hazards and incidents must be recorded appropriately and as soon as practical, within ACU's WHS System ("Riskware").

(18) Each Faculty, Directorate, School etc which maintains a ("CARM") Risk Register, must manage a minimum of 5 key workplace health and safety risks inherent within their operations, within their Risk Register. These WHS risks must be categorised under "Community Wellbeing" and sub-categorised under "Work Health and Safety Management System" within the CARM System to allow for accurate WHS reporting.

Section 9 - Roles and Responsibilities

Role	Responsibility
Audit and Risk Committee (a sub-Committee of Senate)	Reviewing the risk management practices of the University. This includes overseeing the University Strategic Risk Register and ensuring significant risks to the University are reported to the Senate. Approval of Risk Management Procedure.
Members of the Senior Executive and Members of the Executive	Risk management within their Portfolio or Organisational Unit. This includes overseeing the development, monitoring and reviewing of risk registers and co-ordinating risk considerations with organisational and strategic planning.
Vice-Chancellor's Advisory Committee	Monitoring, reviewing and updating the University Strategic Risk Register; Endorsing the University Strategic Risk Register prior to its submission to the Audit and Risk Committee; Oversight of key organisational risks including high+ and over tolerance risks; and Providing updates to the Vice-Chancellor and President and Audit and Risk Committee as appropriate.

Role	Responsibility
Organisational Unit Risk Owner	Establish and continually monitor and review a Risk Register appropriate to their designated area; Ensure risks are appropriately identified, captured, and assessed based on ACU's Risk Appetite Statement, Risk Matrix and Likelihood and Consequence Baselines; Design and implement actions within appropriate timeframes, that will effectively mitigate risks where required; Ensure key risks to operational plans are considered and recorded and managed in risk registers.
Assurance Unit, Legal, Assurance and Governance Directorate	Assisting with the development, monitoring and review of the Organisational Unit and University Strategic Risk Registers, which may include assisting staff with the risk management process; and Reporting matters relating to risk to the Audit and Risk Committee, Vice-Chancellor's Advisory Committee and Senior Executive.
WH&S and Wellbeing	Reporting and management of workplace health and safety incidents, hazards and risks within ACU.

Section 10 - Definitions

Term	Definition
Action Owner	The person that is responsible for implementing the future treatments.
Activity Risk Assessment	A risk assessment undertaken prior to committing ACU to a new activity. Refer Appendix 1.
Causes	The origin of the risk and / or the mechanisms that fail.
CARM User Guide	A useful guide of procedures and instructions to assist with the operation of ACU's proprietary risk management system 'CARM'
Consequence Rating	The extent to which the risk will affect the Organisational Unit and / or the University if it occurs. (Refer to the Risk Appetite Statement)
Due Date	The date the response / actions will be resolved or reviewed.
Existing Treatments	The existing treatments that are in place, which may include procedural or administrative policies or physical barriers.
Inherent Risk	The profile of a risk before any controls are applied whatsoever.
Impacts	The consequences or outcome that the Organisational Unit and / or University can expect if the risk eventuates.
Likelihood Rating	The chance that the risk will occur.
Material Risk	A risk that may adversely affect ACU's ability to deliver on its mission, vision, strategic or operational / organisational unit plans.
Response / Action	Specific treatments that will further prevent and / or mitigate the risk event.
Risk	Threats to ACU's ability to deploy, balance and manage its resources and environment as it pursues its mission, vision and strategic goals'. 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 ISO 31000:2018 - Risk Management Guidelines, as it considers its capacity to respond to elements or events that impact its purpose.
Residual Risk	The amount of risk that remains depending on effectiveness of treatments and controls.

Term	Definition
Risk Appetite	How much risk ACU is willing to strategically pursue in order to fulfill its mission, vision and strategic plan.
Risk Appetite Statement	ACU's statement of risk appetite.
Risk Category	10 key risk categories should be used to group and consider ACU risks into CARM: • Community Wellbeing; • Culture and Principles; • Education; • Finance; • Governance; • Operational; • Project; • Reputational; • Research; and • Strategic.
Risk Event	Occurrence or change of a particular set of circumstances. An event: • can consist of one or more occurrences, and can have several causes; • can consist of something not happening; • can sometimes be referred to as an 'incident' or 'accident'; and • where there are no consequences, can also be referred to as a 'near miss', 'incident', or 'close call'.
Risk Identified	A brief description of the risk that impacts on the achievement of the University's objectives.
Risk Management	Coordinated activities to direct and control risk.
Risk Matrix	Risk Matrix
Risk Owner	The person who takes responsibility for the risk and ensures that the risk is effectively managed. The Risk Owner will usually be a member of the Senior Executive for the University Strategic Risk Register and usually a Member of the Executive for an Organisational Unit Risk Register.
Risk Tolerance	For a particular risk event, the maximum amount of risk ACU will accept relevant to its overall desired risk appetite.
Stakeholder	Person or organisation that can affect, be affected by or perceive themselves to be affected by a decision or activity, or persons having power or influence over the decision or activity.

Section 11 - Review

(19) This Procedure will be reviewed every two years at a minimum. Unless otherwise indicated, this Procedure will still apply beyond the review date.

Section 12 - Further Assistance

(20) For further assistance, please contact the Assurance Unit, Legal, Assurance and Governance Directorate.

Section 13 - Appendix 1: Procedures for Managing Risks in ACU Risk Registers using ACU's Enterprise Risk Management System (CARM)

(21) The 'CARM' Risk Management System is ACU's proprietary system for registering and managing risks. It is a "live" system, meaning that risks can be entered and updated on an ongoing basis to reflect ongoing changes and developments in ACU's strategy, organisational and risk management cycle.

Risk Registers In CARM

(22) For the purpose of developing Organisation and Strategic (University / Executive) Risk Registers, ACU's enterprise risk management tool CARM will be used.

(23) CARM is a real time system, meaning that risks should be entered, updated, and managed on an ongoing basis. Likewise, actions should be updated and managed to ensure status and related comments and context is current.

Access to CARM

(24) Access to CARM Risk Management System is controlled via Microsoft Teams and Power BI. Employees with access permissions to individual risk registers, will be set up within their "Organisational Business Unit Risk Register CARM-TEAM". The Risk Register owners are to advise the Assurance Unit to grant or remove access on Microsoft Teams and Power BI for staff that are to have or remove access.

(25) All members of the Senior Executive will have universal permissions within the CARM. Members of the Assurance Unit will have administration rights and IT will have access to provide technical support.

Risk Register Owners

(26) The Risk Owner will usually be a member of the Senior Executive for the University Strategic Risk Register and usually a member of the Executive for an Organisational Unit Risk Register.

CARM Risk Management System User Guide

(27) The CARM Risk Management System is supported by a detailed user guide which outlines all steps necessary to capture, assess, respond, and monitor risks within the system.

CARM Risk Management System Process

(28) The CARM Risk Management System allows all key risks which may prevent or delay the achievement of the University's strategic goals and objectives to be captured, assessed, responded to, and monitored with appropriate reporting. It follows the processes outlined as ACU's risk management model.

(29) Risks will be captured into CARM in accordance with the input fields required (drop down or free text).

(30) Risks will be assessed in CARM in accordance with the Risk Appetite Statement noting ACU defined and approved likelihood and consequence baselines. This ensures all risks will be assessed consistently and from an overarching ACU enterprise viewpoint. Inherent risks (i.e. the risk in its completely uncontrolled form) will be assessed first.

(31) An inherent risk rating will be determined automatically by CARM using ACU's approved Risk Matrix. The inherent risk rating will be compared against ACU's approved risk tolerance level set by the Audit and Risk Committee for that key risk category.

(32) Existing treatments will be entered into the Existing Controls field.

(33) The risk will be re-assessed to consider the effectiveness of existing controls and to determine the residual risk remaining.

(34) CARM will automatically determine if the residual risk is over or within ACU's approved risk tolerance level set by the Audit and Risk Committee for that key risk category.

(35) The risk assessment will be saved.

(36) A Risk Response will then be required.

(37) If residual risk is within ACU's approved risk tolerance levels, the risk can be accepted or if necessary, mitigated with further action to reduce it even further.

(38) If residual risk is over ACU's approved risk tolerance levels, the risk must be mitigated.

(39) Risks can be mitigated by assigning actions, action status, action responsibility, action due date. Comments should be added to provide context.

(40) The Vice-Chancellor and President (all risks) and the relevant member of the Senior Executive, appropriate to designated areas of risk ownership, have the authority to approve a risk that is over the Risk Treatment Tolerance Levels if no acceptable treatment can be devised and assigned.

(41) Risk monitoring and reporting can be done via the Risk Monitoring function tab. Dashboards highlight key features of risk register profiles, actions, and include a risk matrix heat map. Filters and drill down functionalities can be used to select and refine risk data for analysis. Risk register reports can be reviewed, printed, and exported into Excel for further analysis and review.

(42) Risks entered into risk registers can be updated and reassessed on an ongoing basis. This allows ACU to be agile and responsive to changes in risk profiles, environments, and appetites.

CARM Risk Register Maintenance

(43) CARM Risk Registers should be maintained on an ongoing basis.

(44) CARM Risk Registers should be reviewed as part of the annual strategic and operational planning process.

Section 14 - Appendix 2:

Activity Risk Assessment								
Risk Identification		Risk Analysis				Risk Treatment (Future)		
Risk Category	Risk Event	Causes	Impacts	Existing Treatments	Risk Ratings (refer ACU Risk Matrix Page 12)	Future Treatments	Action Owner	Resolution / Review Date
Please Select a Risk Category					Likelihood Please select: Consequence Please select: Risk Rating Calculate and select via Risk Matrix:			
Please Select a Risk Category					Likelihood Please select: Consequence Please select: Risk Rating Calculate and select via Risk Matrix:			

Activity Risk Assessment								
Please Select a Risk Category					Likelihood Please select: Consequence Please select: Risk Rating Calculate and select via Risk Matrix:			

Status and Details

Status	Current
Effective Date	15th February 2024
Review Date	30th April 2024
Approval Authority	Audit and Risk Committee
Approval Date	15th February 2024
Expiry Date	Not Applicable
Responsible Executive	Diane Barker Director, Legal, Assurance and Governance
Responsible Manager	Dalton Langenhoven National Manager, Assurance
Enquiries Contact	Assurance Unit