Risk Management Plan

Authority Source: Vice-Chancellor

Approval Date: 16/05/2018

Publication Date: 17/05/2018

Review Date: 17/05/2021

Effective Date: 16/05/2018

Custodian: General Counsel and University Secretary

Contact: risk.management@canberra.edu.au

Accessibility: Public

Status: Published

In developing this procedure the University had regard to the provisions of section 40B(1)(b) of the Human Rights Act 2004 (ACT).

PURPOSE:

The University of Canberra (**University**) is committed to effective and efficient identification, treatment and monitoring of risks that may affect the achievement of the University's strategic and business objectives. The Audit and Risk Management Committee (**ARMC**) and Council oversee the implementation and operation of risk management at the University.

The University pursues an effective risk management philosophy and culture through a governance framework that integrates its risk management activities with its Strategic Plan and supporting business and operational plans.

The objectives of the University's Risk Management Plan (**Plan**) are to:

- provide a detailed guide to support the implementation of risk management at the University;
- outline the risk management process to be followed by all members of the University, including controlled entities and contractors, where applicable;
- minimise the University's exposure to significant risks through the identification, assessment, management and reporting of risk; and
- enhance the University's ability to capitalise on opportunities through risk management and overall performance improvement.

SCOPE:

The Plan establishes the processes for risk management across the University. This Plan applies to the UC Group (i.e. all members of the University, including controlled entities), unless otherwise agreed by the governing board and the Vice-Chancellor.

The risk management process is designed to ensure that risk management decisions are based on a robust approach, assessments are conducted in a consistent manner, and a common language is used and understood across the University.

This Plan is consistent with the Australian and New Zealand Risk Management Standard - *ISO 31000:2018*

PROCEDURE:

The risk management process consists of the following:

1. Communication and consultation with relevant stakeholders;
2. Defining the scope of the process and understanding the external and internal context
3. Risk assessment which includes the process for identifying, analysing and evaluating risks;
4. Treating the identified risks;
5. Monitoring and review which includes determining whether the risk profile has changed and whether new risks have emerged. Checking control effectiveness and progress of the treatment plans; and
6. Recording and reporting to relevant stakeholders.

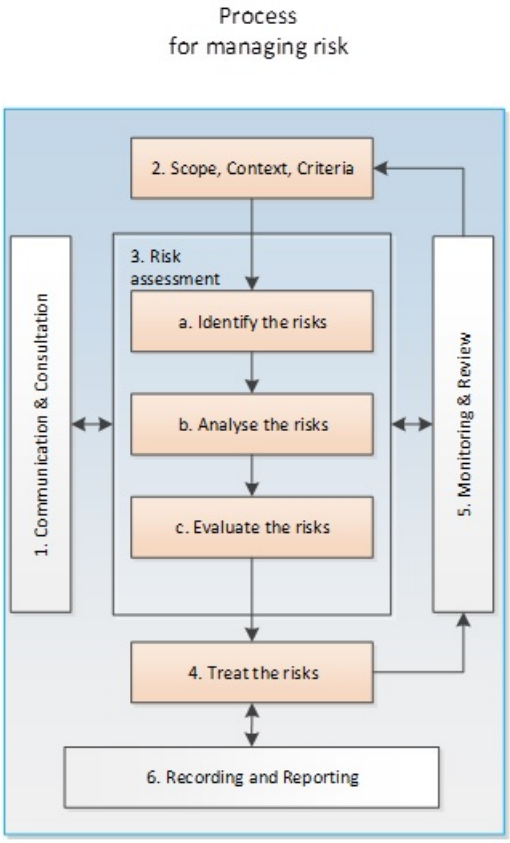


Diagram 1 – Risk management process followed by the University

Instructions on applying the risk management process are included at Attachment A, with details on the supporting tools to assist in the process included at Attachment B.

Risk assessments should be undertaken to assess:

i. Strategic risks – are the risks specific to the ongoing operations of the University which may impact the achievement of the Strategic Plan and objectives;

ii. Operational risks – are the risks specific to a single business unit, faculty, research institute or controlled entity; and

iii. Project risks – are the risks related to specific projects, including contracts, capital works, events, procurements, partnerships and business ventures.

A risk assessment may be undertaken at any time for any University activity. However a risk assessment should always be undertaken in any of the following circumstances:

- where required by a regulatory body, University policy or procedure (e.g. Work Health and Safety Act, international travel, field trips);
- at the commencement of any major project relevant to the University – a major project is defined as having a total value greater than $200,000, or where there is a risk that would have a potential consequence rating of Moderate or above (refer to the UC Risk Matrix for consequence ratings);
- to support decision-making, such as in determining the feasibility of a project or in supporting the requirement for additional resources or new equipment;
- prior to significant new initiatives being commenced by faculties, business units or controlled entities;
- prior to undertaking any significant new commercial activity, joint venture or partnership arrangement;
- as part of a significant procurement activity; or
- prior to the commencement of any activity where serious injury, significant property loss or adverse media attention may result.

A risk assessment for a project, procurement, contract and event can be applied across all phases of the lifecycle (i.e. from initial concept and definition through realisation to a final completion, decommissioning or disposal). It is important that consideration for a risk assessment occurs at the outset of an activity as this may assist in understanding the feasibility of the project due to the potential risks involved and ultimately, whether to proceed or not. A risk assessment can also be used to assist in determining the best option where alternative options or solutions are available.
During the design and development phase of a project/activity, a risk assessment contributes to:

i. defining the risk;
ii. ensuring risks are understood and tolerable;
iii. informing decision making processes;
iv. cost-effectiveness studies; and
v. identifying risks impacting on subsequent life-cycle phases.

As the activity proceeds, risk assessment can be used to provide information to assist in developing procedures for normal and emergency conditions.
Note: the University has specific policies and procedures for conducting risk assessments relating to work health and safety practices and international travel. Refer to the Policy Database for further details.

Developing a Risk Register

The development of a Risk Register involves risk identification and assessment where major strategic and operational risks, and potential sources of risks, are considered and identified. The University applies a five-point risk assessment scale to determine the seriousness of the **resulting consequence** if the risk does occur and **how likely** it is that any given risk will occur based on the consequence.. These two assessments are then brought together in a two-dimensional matrix and their interactions determine the rating of each assessed risk as **Low, Medium, High** or **Extreme (Risk Matrix).**
The Risk Matrix is located on the UC Portal - Risk Management website.
In practice risks are assessed on both a **Current** and **Residua**l basis.
The **Current** assessment considers the risk rating taking into account current controls that have been implemented.
The **Residual** assessment considers the risk rating taking into account the impact of any further controls and treatment strategies which will be implemented to mitigate the risks consequence and/or likelihood.

Assessing the risk profile

Each operating area within the University is required to develop a risk register identifying all risks that may impact on organisational activities and outcomes across the range of activities and processes undertaken. These risks are then assessed against the Risk Matrix, current and potential treatment and control actions and options are reviewed. A Residual risk rating is then applied by taking into consideration the Current risk rating and related current treatment and control action(s).

Operational risk registers are then aggregated to develop a University wide risk profile.

Developing Risk Treatment Action Plans and Risk Summary Reports

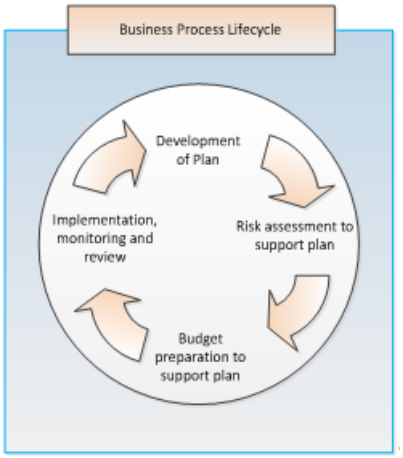
Executive Deans/Directors/Senior Managers/Managers must report on all risks currently rated as Extreme or High due to the potential impact on business activities that may result should these risks eventuate. This is done using risk treatment action plans and risk summary reports. The risk treatment action plans must include the risk reference number, detail of the risk, treatment/control measures and implementation progress of treatment/control measures. Risk treatment action plans must also indicate whether it is considered that Executive intervention is required.

The risk treatment action plans are analysed and summarised into risk summary reports. The Extreme and High level risks set out in these risk summary reports are presented to the ARMC (or relevant Boards for controlled entities) for monitoring and any further action, if required.

Risk assessment – business planning cycle

Operational and strategic level risk assessments should be undertaken as part of the University's business planning process. These plans include the University's Strategic Plan and operational plans. A risk assessment, including the review of existing risk registers, should be undertaken to support this process.

The following diagram illustrates this business process lifecycle:



Approval, maintenance and review

All operational risk registers should be submitted to the Risk and Audit team (risk.management@canberra.edu.au) to monitor the level of acceptable risk and the extent of which risks are being managed appropriately.

All risk registers must be finalised and formally approved by the appropriate level of authority when developed and on completion of formal review process.

All risk management documentation is to be recorded, stored and maintained in an appropriate manner and location. A current copy of strategic and operational level risk registers is to be held with the Risk and Audit team.

The level of approving authority and frequency for review is detailed in the following table:

Level	Approving Authority	Frequency
Strategic	Vice-Chancellor and Vice-Chancellor's Group (the latter for noting)	Bi-annual reviews (i.e. every six months) or more frequently as part of strategic planning or at a major environmental change
Operational	Portfolio Head, Executive Dean or Director	Bi-annual reviews (i.e. every six months) or more frequently as part of business planning or at a major environmental change
Project/Event	Project Manager or Project Steering Committee.	At key milestones or more regularly as required by project requirements.

Risk assessments and reviews should be conducted to align with development of plans (e.g. strategic, operational and project plans) and budgeting cycles where practicable.

A risk register review will entail assessing the state of each risk and updating the register to reflect the current status of the existing controls and further treatment actions to be undertaken. Reviews of the risk ratings based on any changes should also be considered. It is important that a review of the risk assessment be conducted when there is a change in context, as it may impact an existing risk or mean new risks may emerge.

Risk owners will have accountability for managing the risk and ensuring any associated risk treatment plans are implemented accordingly.

Reporting

Risk register reporting allows management to monitor and review risks. Risk reports draw information from the risk registers and, depending upon the requirements, may include:

- a demonstration of the link between objectives and risks;
- priorities, based on the risk rating, accompanied by information on key controls and treatments needed to modify the risk;
- risks that are getting worse, success of treatment plans and risks that require additional attention;
- new risks that may still need to be fully considered and understood;
- potential areas that require urgent attention;
- main areas of exposure;
- systemic control analysis;
- untreated risks and risk treatments that are overdue; and
- risk owners.

The Annual Internal Audit Plan will be developed in part on the basis of the Strategic Risk Register and operational unit risk registers with a view to testing and validating the risk registers and plans to ensure that treatments and controls are adequate.

CONCLUSION

The University takes its responsibility to students, staff, partners, affiliates and the wider community seriously. To this end, its approach to managing risks to its operations can be seen to have three key focuses:

- a risk management platform of defined guidelines and accountabilities supported by risk management tools and templates;
- a business practice approach to risk management, embedded into all levels including business, project and resource planning and reporting; and
- continuous identification and management of risks, supported by regular ongoing review and monitoring.

This Plan, in conjunction with the University's Resilience Management Framework, is one of the key governance measures designed to ensure that risks are properly identified, assessed and managed. In practice the Resilience Management Framework, and this Plan must be maintained as living documents, developing and evolving to reflect changing internal and external environments, and responding to new and previously unanticipated risks to the quality and effectiveness of its work.
It is expected that all staff will know, understand and support their defined role in the management of risks and in the development and application of this Plan.

IMPLEMENTATION AND REPORTING:

Implementation Officer
The Associate Director, Risk and Audit is responsible for the promulgation and implementation of this procedure. Enquires about the above process should be directed to the implementation officer by emailing risk.management@canberra.edu.au.

SUPPORTING INFORMATION:

Further Information
To access *ISO 31000:2018 Risk Management –Guidelines* standard go to http://www.canberra.edu.au/library/research-gateway/databases select 'standards on-line' and enter 'risk management' into the search field.
For further advice and assistance please contact the risk management team within the University's Risk and Audit team by emailing risk.management@canberra.edu.au.
Refer to tools and templates on the Risk and Resilience Management website on the UC Portal.

Review
This procedure will be reviewed every three years.

References
Australian and New Zealand Standard ISO 31000:2018 – Risk Management Guidelines.
Australian Capital Territory Insurance Authority (ACTIA) Risk Management Guide and Toolkit ACT Government.
University of the Sunshine Coast (2013) Risk Management Procedures. Maroochydore, Queensland.
Griffith University (2013) *Risk Management Framework,* Queensland.

ATTACHMENT A - Risk Management Process
Instructions on how to undertake risk management activities are detailed below.

Process Step	Purpose & Process	Tools
1. Communication and consultation – involves stakeholders (internal and external) and information sharing throughout the risk management process, at all levels across the University.	The objective of this step is to ensure that all relevant stakeholders are adequately engaged in the risk management process, therefore not limiting the opinions, insights and expertise to achieve the best outcome. Other advantages of communicating and consulting include: • bringing different areas of expertise together for each step of the risk management process; • ensuring different views are considered and limit any bias perceptions; • providing sufficient information to facilitate risk oversight and decision making; • building a sense of inclusiveness and ownership among those affected by risk; • those involved better understanding the basis for decisions and actions required; and • any lessons learnt being shared and transferred to those who can benefit from them. Consider consulting with, but not limited to, the following at any stage of the risk management process: • subject matter experts; • decision makers (executive and managers); • operational staff; • end-users; • people who do the job; • project manager/project sponsor; and • event coordinator.	• Internal training sessions • Risk assessment workshops • Steering Committees
2. Scope, Context, Criteria – defining the scope of the process and understanding the external and internal context.	The risks being identified should relate to the activity being undertaken e.g. business operations, a project, a procurement or an event. Developing a **Risk Context Statement** will assist in defining the activity and understanding the risk. **Defining the scope** As the risk management process may be applied at different levels (strategic, operational, project etc.), it is important to be clear about the scope under consideration, the relevant objectives to be considered and their alignment with organisational objectives. When planning the approach, considerations include: • objectives and decisions that need to be made; • outcomes expected from the steps to be taken in the	• Risk Context Statement

Process Step	Purpose & Process	Tools
	process; • time, location, budget and resources; • specific inclusions and exclusions; • appropriate risk assessment tools and techniques; • resources required, responsibilities and records to be kept; and • interdependencies/relationships with other projects, processes and activities. **External and internal context:** The external and internal context is the environment in which the University seeks to define its objectives. The context of the risk assessment process should be established from understanding the external and internal environment in which the University operates and activity(s) is being performed. • external factors (including social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment); and • internal factors (including governance, organisational structure, policies, strategies, available resources, information systems, decision making processes). **Defining risk criteria** Define the risk criteria to ensure risks are assessed in a consistent manner (i.e. nature and types, timeframes, level of risk, stakeholder reviews and perceptions). The University defines risk criteria using the **Risk Matrix**. **What information is available?** Gather any relevant documents that may assist in identifying risks relevant to the activity you are assessing, these may include: • strategic, operational and project plans; • policies and procedures; • annual reports; • audit reports and recommendations; • University website/intranet portal; • outputs from business and project planning processes, such as SWOT and PESTLE analyses; and • historical data or information (e.g. staff surveys).	

Process Step	Purpose & Process	Tools
3, Risk assessment – this is the overall process for identifying, analysing and evaluating risks. The purpose of the risk assessment is to provide information and analysis to support decisions on how to treat particular risks and how to choose between options where there is uncertainty. Risk assessments for the operational and strategic levels should be conducted as part of the University's business planning cycle. Further information is provided in the Risk assessment – business planning cycle section.		

Process Step	Purpose & Process	Tools
a. Identify the risks "Finding, recognising and describing risks." A **risk** has not occurred and may not happen. An **issue** is a risk that has occurred or 'been realised'.	The objective of this step is to identify and document all significant risks that could potentially have an impact on the University's strategies and operational activities. To undertake this process, consider the use of focus groups (using brainstorming approaches, SWOT/PESTLE analysis techniques, project categories or broad business categories), workshops and interviews, and conduct research activities internally and across the industry. To identify relevant risks follow the below process: 1. A **description** of the risk is the event ○ what can happen? Consider appropriate language e.g. Failure to… Breach of… Damage to… Loss of… Inadequate… Insufficient… Inability to… Lack of… Exceeding (authority, delegations, contract price etc.)… 2. The **source/cause** ○ what is the source, driver and contributors ○ what causes the risk - how can it happen? e.g. the source of the risks ***Damage to a building*** could be: Natural disasters (e.g. earthquake) Flood Fire e.g. the source of the risks ***Breach of legislation*** could be: • Lack of training and understanding by staff. • Time and resourcing constraints. • Poor control environment. • Deficient policies and procedures to support legislation. • Lack of monitoring and reporting. 3. The **impact/outcome**	• Risk Register • Risk assessment workshops

Process Step	Purpose & Process	Tools
	~~is the consequence of the event/activity~~ ~~if what can happen does happen?~~ The inclusion of the consequence summary in the risk description supports the consequence rating chosen when analysing the risk (refer to 2. Step 1 below). It also allows a view to be informed as to what is being managed. The consequence should be described in its most *usual form* and not the *extreme form*. e.g. the consequence of ***A paper cut*** is: • *usual form*: cut not requiring first aid treatment • *extreme form*: cut resulting in an infection, blood poisoning and death. **Note:** if the risk described has ***no consequence*** or it ***can't ever happen*** then what you have described is not a risk. 4. Assign a **Risk Owner** as it is important to assign accountability to ensure ongoing management of the risk. e.g. Project Manager, Vice-President Finance and Infrastructure or Exectuive Dean, Faculty of Business, Government and Law.	

Process Step	Purpose & Process	Tools
b. **Analyse the risks** – comprehending the nature of the risk and determining the level of risk exposure (consequence and the likelihood of that consequence).	The objective of this step is to sort the major risks from the minor ones and determine where resource effort should be focussed. A **risk control** is what is currently being done to manage the risk. Controls include any process, policy, device or practice or other actions, which modify risk. Controls may not always operate as intended and may potentially result in additional risks arising. In order to analyse risks it is necessary need to determine: 1. what **risk controls are currently in place** – the first step in analysing or rating risks is to consider what is currently being done to manage the risk (i.e. current risk controls) e.g. ○ policies and procedures ○ delegate approval, monitoring and review ○ regular training and development. 2. the **Current risk rating** assesses the risk as it is now, taking into account our current controls. Using the Risk Matrix, determine the following: ○ Step 1 **- Consequence** – what is the consequence level of the risk occurring in its most *usual* form? Consider the consequence in terms of the categories on the Risk Matrix (i.e. reputation, financial, teaching and learning, legal and compliance etc.) ▪ ○ Step 2 - **Likelihood** – determined by the likelihood of the consequence of the risk occurring. e.g. where the risk may occur every 3- 5 years it would be '*C – Possible'.* • Step 3 – rate the risk using the UC Risk Matrix **Consequence x Likelihood = Risk Rating** *4-Major x C-Possible = High*	• Risk Register • Risk Matrix

Process Step	Purpose & Process	Tools
c. Evaluate the risks – comparing the results of the risk analysis with the risk criteria to determine whether the risk is acceptable or tolerable.	This part of the process is required: • to determine whether the controlled risk is acceptable or whether further action to manage the risk needs to be taken; and • to identify the priority order in which individual risks should be treated. Use the **Control Effectiveness Rating (CER)** to consider whether what is ***being currently done*** to manage the risk is sufficient or should more be done? These can be evaluated as (refer to the UC Risk Matrix for definitions): • Inadequate • Room for Improvement; or • Adequate. To identify the priority order in which individual risks should be treated, monitored and reviewed, sort risks based on the level of risk it carries, the consequence of the risk and whether there is more that can be done to manage the risk.	• Risk Register • Risk Matrix
4.Treat the risks selecting one or more options for modifying the risk. Reassessing the level of risks with controls and treatments in place (residual risk), preparing treatment plans and implementing them.	The objective of this step is to identify treatments for risks that fall outside the University's risk tolerance. If the CER is rated as 'Inadequate' or 'Room for Improvement' it is necessary to determine what else could be done to manage the risk. 1. **Actions to be taken,** or additional controls, can be implemented to: ◦ **avoid** the risk by ceasing the operation (often not a viable option). ◦ **reduce** the risk for example, through: ◦ implementing policies, procedures, segregation of duties; ◦ implementing plans or planning processes (e.g. communication plans, business continuity plans); ◦ conducting formal reviews or audits; or ◦ inspection and monitoring of processes, activities and events. ◦ **share** the risk for example, through: ◦ taking out insurance policies; or ◦ contracting/outsourcing arrangements. 2. Assign a **Risk Treatment Owner** who will be responsible for implementing any additional actions to be	• Risk Treatment Action Plan Note: these are required for all Extreme and High rated current risks.

Process Step	Purpose & Process	Tools
	taken. 3. The **Residual risk rating** is then determined. This is what the risk level will be after additional treatment actions have been implemented. The Residual risk rating can be assessed using the UC Risk Matrix and the same calculation process as the Current risk rating: **Consequence x Likelihood = Risk Rating** *3-Moderate x C-Possible = Medium* 4. Using the **Control Effectiveness Rating (CER)** consider whether what is ***intended to be done*** to manage the risk will be sufficient or is there more that could be done? 5. **Risk Treatment Action Plans** – must be developed for **all** risks currently rated as Extreme or High. These action plans include: ○ tasks to be undertaken to manage risk; ○ due dates or milestones for when actions should be completed; and ○ the Treatment Owner who is responsible for implementing the treatment action. **Note:** when identifying new controls it is important to consider whether any changes create new risks, additional resource effort required to implement and manage the new control.	

Process Step	Purpose & Process	Tools
5. Monitoring and review – determining whether the risk profile has changed and whether new risks have emerged. Checking control effectiveness and progress of the treatment plans.	Risk registers should be **reviewed every six months**, at key project/event milestones or more frequently when there is a major environmental change *e.g. implementation of a new policy.* The monitoring and review process should encompass all aspects of the risk management process for the purposes of: • providing currency of risk information; • identifying emerging risks; • detecting changes in the external and internal context, including changes to risk criteria and the risk itself, which can require revision of risk treatments and priorities; • ensuring all controls are effective and efficient in both design and operation; • providing feedback on control efficiency and effectiveness; • identifying whether any further treatment is required; • providing a basis to reassess risk priorities; and • capturing lessons learned from events (including near-misses), changes, trends, successes and failures. For further details on timelines for reviews of risk registers refer to the Approval, maintenance and review section of this Plan.	• Reporting • Risk Register • Risk Matrix • Risk Treatment Action Plan
6. **Recording and Reporting** - outcomes should be documented and reported through appropriate mechanisms.	Recording and reporting aims to: • communicate risk management activities and outcomes across the University; • provide information for decision-making; • improve risk management activities; and • assist interaction with stakeholders, including those with responsibility and accountability for risk management activities. The University uses the **Risk Summary Reports** to report on risks with an Extreme and/or High current risk rating to the ARMC.	• Risk Summary Reports

ATTACHMENT B - Tools and Templates

The following tools will be used consistently by all business areas across the University, including faculties, research institutes, controlled entities and key administrative business units, for conducting risk assessment and the ongoing management of risks.

Tool	Description
1. Context Statement	This is an overarching statement document to support the risk assessment process. It will: • define the risk assessment activities to be conducted; • define the activity, process, function, project or service; • detail the goals, objectives and scope of the activity; and • clearly define the roles and responsibilities in relation to the activity.
2. Risk Registers	Information from the risk assessment process is recorded, reported and monitored using the Risk Register. The Risk Register enables staff to document, manage, monitor, review and update strategic, corporate and operational risk information. For each risk the following will be captured: • a description of the risk; • the risk category; • the causes; • the impact of the expected consequences; • the existing controls being relied upon; • consequence and the likelihood of the expected impact; • the current risk rating; • the control effectiveness rating (CER); • the name of the risk owner; • additional treatment actions to be considered; • the name(s) of the treatment owner(s); • the residual risk rating; and • review timings.
3. Risk Matrix	Tool used to assess the level of risk based on the consequence and likelihood of the risk occurring. The Risk Matrix is located on the UC Portal - Risk and Resilience Management website.
4. Risk Treatment Action Plans	A Risk Treatment Action Plan will be prepared for all Extreme and High rated risks. A Risk Treatment Action Plan contains: • the tasks to be completed and the risks they address • the name of the task owners who have responsibility for implementation of treatment tasks • the timetable for implementation.

Tool	Description
5. Risk Summary Reports	Risk reports draw information from the risk registers and enable management to monitor and review risks in alignment with the Strategic Plan, business and operational plans, programs of change and other cascading plans. Risk Summary Reports are completed for the strategic, operational and project risks and used to report to ARMC, Academic Board, controlled entity boards, project control groups/steering committees, faculty visits and other university reporting requirements. Refer to Reporting section for details.
6. University of Canberra Website and Portal	Access to policy, guidelines and template documents are available on the University of Canberra staff portal.
7. Training and risk workshop facilitation	Risk management training courses are available to equip relevant University stakeholders with sound risk management knowledge and skills. These courses include: • a walkthrough of the risk management process • how to conduct a risk assessment • how to use the tools and templates available • ongoing monitoring, review and reporting requirements. Assistance is also available to staff when developing risk registers through workshop facilitation.

The tools and templates are located on the UC Portal - Risk and Resilience Management website.