# Resilience Management Framework

**Authority Source:** Audit and Risk Management Committee (ARMC)

**Approval Date:** 30/11/2017

**Publication Date:** 05/12/2017

**Review Date:** 30/11/2020

**Effective Date:** 30/11/2017

**Custodian:** General Counsel and University Secretary

**Contact:** risk.management@canberra.edu.au

**Accessibility:** Public

**Status:** Published

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

## PURPOSE:

The University of Canberra regards effective risk and resilience management as an integral component of the University's efficient operations. Therefore the University has adopted a consistent and structured approach to identify, assess and manage significant risks and to ensure efficient and effective utilisation of resources, informed decision-making and organisational resilience. The purpose of this Resilience Management Framework (Framework) is to:

- provide the foundation to effectively manage risks involved in all University activities to an acceptable level
- ensure risk management processes are embedded consistently across all areas of the organisation
- contribute to strengthening management practices, while protecting our community's interest, and maintaining trust and confidence
- provide assurance to stakeholders that the University is prepared and able to effectively manage a major or critical incident
- enable the University to embed a systematic and pro-active approach to risk as part of overall University governance.

**Policy Statement**

The Vice-Chancellor and Council are committed to the implementation and maintenance of a formal resilience management system, including the integration of risk management, throughout all levels of the University. This is fundamental to achieving the University's strategic and operational objectives, whilst protecting and enhancing the University's reputation.

In its application of this Framework, the University is committed to:

- achieving its business objectives while minimising the impact of significant risks that the University can meaningfully and realistically control;
- the allocation of appropriate resources for the achievement of University business objectives and effective resilience management;

- behaving as a responsible and ethical organisation, protecting staff, students and the broader community from harm and protecting physical property from loss or damage;
- communicating and collaboration with key stakeholders, and providing appropriate training, to enable implementation of policies and procedures;
- deciding the criteria for accepting risks and the acceptable levels of risk;
- establish the right balance between the cost of control and the risks it is willing to accept as part of the environment within which the University operates;
- the promotion of excellence in regard to business management processes, record keeping, performance improvement and monitoring;
- protecting and enhancing the University's reputation;
- ensuring privacy and confidentiality in accordance with legislative requirements and University policy; and
- conducting management reviews and audits of elements of the framework.

The University considers risk management, business continuity, critical incident management, emergency management, disaster recovery, fraud control and health, safety and wellbeing management as crucial components of its Resilience Management Framework.
This Framework applies to the UC Group (i.e. all members of the University of Canberra and controlled entities), unless otherwise agreed. Resilience management is a whole-of-University activity and as such, it is the responsibility of all members of the University community to contribute to the identification, management and reporting of risks. The University is committed to embedding this Framework into its organisational culture, governance and accountability arrangements, planning and reporting and improvement processes.

## SCOPE:

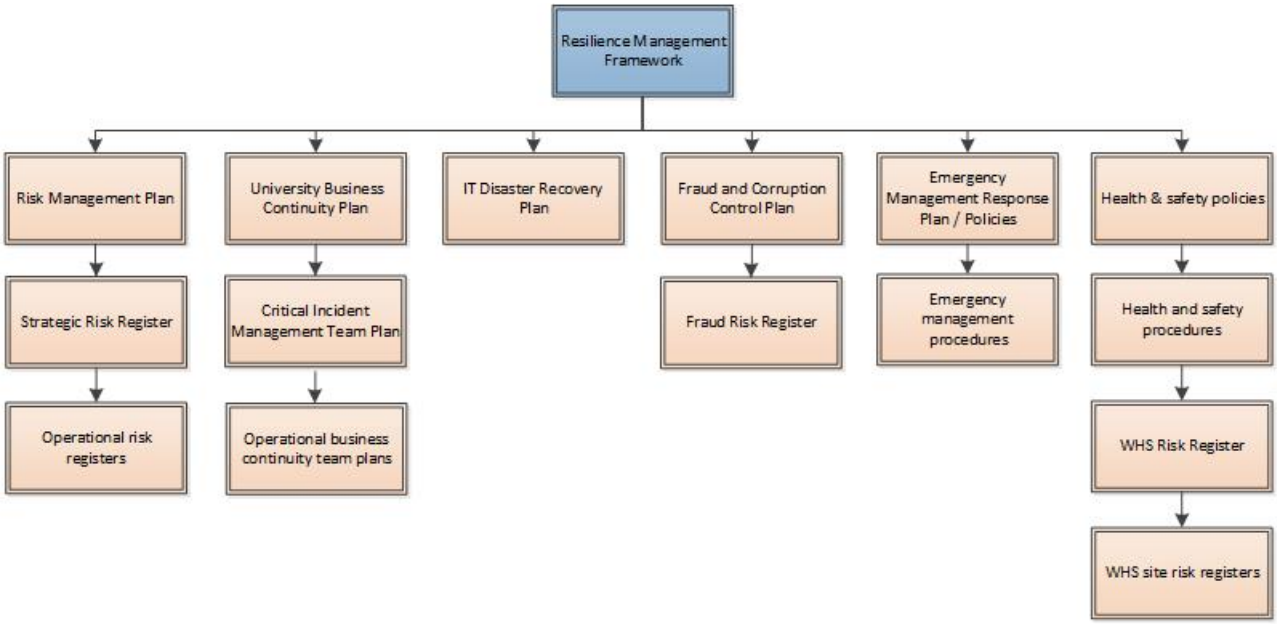
The University's approach to resilience management is based on a holistic organisational-wide model in order to achieve effective governance and assurance. This Framework describes the arrangements of this model, including:

- details of the main components resilience management framework;
- an outline of the principles of risk management which should be applied across the UC Group;
- an overview of the roles and responsibilities for managing risk; and
- details of internal and external communication and reporting mechanisms.

The Framework recognises that resilience management is an integral part of all University processes. It is embedded in all elements of the University's core business, and is not a standalone activity.
The Framework also identifies five key components that are critical to the successful implementation of resilience management at the University. These are:

- risk management
- business continuity management;
- critical incident management;
- emergency management
- IT disaster recovery
- fraud and corruption control
- health and safety.

Each of the key components listed are supported by corresponding plans, which underpin this Framework and its embedded policy. These plans describe the processes and arrangements to be used to manage the University's key risks. The structure of this approach is illustrated below:




## PRINCIPLE:

**Risk Management**

1. All organisations face a variety of risks, either from internal or external sources (which may be largely out of the immediate control of the organisation). Risks arise both at the strategic (organisation-wide) level and at the operational (business process) level. The University will maintain processes and procedures to provide a systematic view of the risk faced in the course of its academic, administrative and business activities.

2. The University of Canberra Risk Management Plan supports this Policy, detailing the processes and procedures, consistent with Australian and New Zealand Standard *AS/NZS ISO 31000:2009 Risk Management – Principles and guidelines.*

3. The processes described in the Risk Management Plan are to be applied in all the University's activities to ensure that risks associated with the University's strategic and operational objectives are identified and effectively integrated with the University's annual planning processes. Reviews of controls and mitigating strategies that link with University planning objectives will be detailed in the University's strategic and operational risk registers.

4. The administration of the risk management program component of this Framework is the responsibility of the Associate Director, Risk and Audit.

**Business Continuity Management**

1. The University will develop arrangements to prepare staff should a major unplanned and disruptive event occur which impacts the University's operations. These arrangements will be consistent with the Australian and New Zealand Standard *AS/NZS 5050:2010 Business continuity – Managing disruption-related risk* and will be documented in the University of Canberra's Strategic Business Continuity Plan (BCP) and supporting operational BCPs.

2. The business continuity plans will enable key management staff to plan and manage both the immediate and longer-term consequence of incidents that impact on the University's operations.

3. The administration of the business continuity management component of this Framework is the responsibility of the Associate Director, Risk and Audit.

**Critical Incident Management**

1. A critical incident is any situation that affects University staff or students' its operations, environment. viability and /or reputation.

2. The University will maintain a Critical Incident Management Team (CIMT) to control the University's response and provide executive decisions and strategic directions in relation to planning for and responding to critical incidents. This response will be in accordance with the procedures incorporated in the University's Business Continuity Plan and Critical Incident Management Team Plan.

3. The University will develop arrangements and provide training to prepare staff to manage critical incidents should they occur, including critical student related incidents.

4. The administration of the critical incident management component of this Framework is the responsibility of the Associate Director, Risk and Audit.

**Emergency management**

1. The University will develop and implement systems and processes for appropriate, effective and speedy responses to, and management of, emergency situations.

2. These systems and processes form part of the University's emergency management system and will be developed in line with Australian Standard *AS 3745-2010 – Planning for emergencies in facilities*; *Building Fire Safety Regulations 2008, and Work Health and Safety ACT 2011*.

3. The University will aim for best practice in incident management responses and procedures, which will be documented in the University's Emergency Management Response Plan.

4. The administration of the emergency management component of this Framework is the responsibility of the Chief Executive People and Diversity.

**IT disaster recovery**

1. The University will develop a documented process to recovery and protect the University's IT infrastructure and business systems in the event of an incident.

2. The IT Disaster Recovery Plan (DRP) will be a comprehensive statement of consistent actions that are to be undertaken before, during and after an event. These arrangements will be consistent with *AS/NZS 5050:2010 Business continuity – Managing disruption-related risk.*

3. The primary objective of the IT DRP is to minimise the effects on the University including downtime and data loss, in the event that all or part of its operations and/or computer services are rendered unusable. The IT DRP will align with the University's business continuity arrangements.

4. The administration of the IT disaster recovery component of this Framework is the responsibility of the Director, Information Management Technology reporting through the VIce-President Finance and Infrastructure.

**Fraud and corruption control**

1. The University will implement fraud and corruption preventative and detective processes to reduce the University's exposure and vulnerability of fraudulent activity.

2. These processes will be documented in the University's Fraud and Corruption Control Plan and will align with Australian Standard *AS 8001-2008 Fraud and Corruption Control*. To support this Plan, a fraud risk assessment of the University's operating environment will be conducted and documented in a fraud risk register. Control measures and treatment strategies will also be documented and reviewed periodically.

3. The administration of the fraud and corruption control component of this Framework is the responsibility of the General Counsel and University Secretary.

**Health and safety**

1. The University recognises health and safety as a critical component of the Resilience Management Framework, the requirements for which are managed under the University's Health and Safety Policy and administered by the Chief Executive People and Diversity.

2. The health and safety policy and procedures have been developed in line with the *Work Health and Safety Act 2011* and associated regulations.

*Note: this Framework does not specify arrangements for the management of health and safety risks as these are documented in health and safety policies and guidelines, issued by the Chief Executive People and Diversity.*

## RESPONSIBILITIES:

The Framework identifies four levels of key resilience management arrangements at the University:

- Council has the overall fiduciary accountability to establish and maintain an appropriate Resilience Management Framework, with support and advice provided by the Audit and Risk Management Committee (ARMC)
- Vice-Chancellor and the Vice-Chancellor's Group are accountable to the ARMC and Council for implementation of the Framework
- Senior management is responsible for developing and administering programs and systems to address key components of the Framework
- All management and staff, and wider University community, have a responsibility to be "risk aware". They are required to comply with risk management processes and practices, cooperate with designated University risk management specialists, and identify, assess, manage and report risks and opportunities in day-to-day processes.

The responsibilities for resilience management within the University of Canberra are defined as follows:

| Role | Responsibilities |
|---|---|
| **Council** | • Oversees monitoring the assessment and management of risk across the University. |

| Role | Responsibilities |
|---|---|
| **Audit and Risk Management Committee (ARMC)** | • Advises Council on:<br>  ○ the adequacy and effectiveness of the University's control environment, including the implementation of the University's resilience management framework<br>  ○ major risks which may impact on the operation or reputation of the University and associated risk management activities (including fraud incidents).<br>• The Committee reviews, evaluates, approves and monitors, on the delegated authority of Council<br>  ○ the University's Resilience Management Framework and their implementation<br>  ○ the University's insurance program and liability protection portfolio. |
| **Vice-Chancellor** | • Endorse the University's Resilience Management Framework.<br>• Approve the plans and procedures relating to risk management, business continuity, incident management, fraud and corruption prevention and IT disaster recovery.<br>• Responsible for ensuring that risk management activities are carried out effectively within the University in accordance with the Framework.<br>• Review, update and approve the Strategic Risk Register, to present to the ARMC. |
| **Vice-Chancellor's Group** | Provides advice to the Vice-Chancellor on:<br>• the University's Resilience Management Framework<br>• the plans and procedures relating to risk management, business continuity, incident management, fraud and corruption prevention and IT disaster recovery<br>• the Strategic Risk Register, for presentation to the ARMC<br>• University Risk Profile. |

| Role | Responsibilities |
|---|---|
| **Senior Management Group (Executive/Deans/ Directors)** | • Integrate risk management principles in business and project planning.<br>• Assess and monitor risk exposures regularly.<br>• Review, update and approve operational risk registers, twice yearly.<br>• Implement effective risk treatment actions and monitor the effectiveness of control measures.<br>• Report twice yearly on operational risks to the ARMC, via the Associate Director, Risk and Audit.<br>• Draw any new Extreme or High risks to the ARMC attention immediately, via the VPGD.<br>• Report project or other risks to the ARMC as appropriate or as requested.<br>• Develop knowledge and skills in risk concepts and promote risk management awareness to enhance efficiency, effectiveness, responsiveness and integrity.<br>• Maintain and coordinate the implementation of operational BCPs. |
| **Critical Incident Management Team (CIMT)** | • Control the University's response and provide executive decisions and strategic directions in relation to planning for and responding to critical incidents. |
| **Risk and Audit, General Counsel and University Secretary** | • Maintain and coordinate the implementation of the University's Resilience Management Framework and supporting plans, including Fraud and Corruption Control Plan, Risk Management Plan and the UC Strategic BCP and Critical Incident Management Team Plan.<br>• Collation and maintenance of the University's Strategic Risk Register.<br>• Actively promotes the integration of risk concepts across the University at both strategic and operational levels.<br>• Provides advice and support into risk management activities and processes as required.<br>• Coordinates reporting to the ARMC on risk registers. |
| **Vice-President Finance and Infrastructure** | • Maintain and coordinate the implementation of allocated components of the University's Resilience Management Framework and supporting plans, including operational BCPs and the IT DRP. |
| **Chief Executive People and Diversity** | • Maintain and coordinate the implementation of allocated components of the University's Resilience Management Framework and supporting plans including Health and Safety policies and procedures and the Emergency Management Response Plan. |

| Role | Responsibilities |
|---|---|
| **Managers and supervisors** | • Contribute to risk management activities in their business unit.<br>• Develop knowledge and skills in risk concepts and promote risk management awareness to enhance efficiency, effectiveness, responsiveness and integrity.<br>• Prepare risk assessments as required.<br>• Assess and monitor risk exposures regularly.<br>• Report any new risks to senior management attention as soon as possible. |
| **All staff** | • Identify, analyse and evaluate risk exposures (including current and potential risks) in work areas.<br>• Report risk exposures to managers and supervisors immediately and, where applicable, discuss and implement treatment strategies to reduce the risk(s) to an acceptable level.<br>• Develop and apply knowledge and skills in risk concepts.<br>• Act in accordance with the University's Code of Ethics.<br>• Follow the University's procedures in regard to incident reporting including injury, damage and loss. |

**Reporting Compliance**

Under the *Tertiary Education Quality and Standards Agency Act 2011* (TEQSA Act), the University is required to meet obligations for registered higher education providers in order to retain its accreditation. Furthermore, the University of Canberra must report on their risk management and internal audit policies and practices in annual reports. The University is required to confirm that it understands, manages and controls key risk exposures and that a responsible body or audit committee verifies the University's arrangements.

**Monitoring and Reporting of Risk Management**

The University is expected to report on risk management performance to the Council and Audit and Risk Management Committee. Regular monitoring and review must be a planned part of the risk management process to ensure that:

- supporting plans have been developed, endorsed and implemented as required under this Framework
- staff are aware of their roles and responsibilities in respect to resilience management
- controls are effective and efficient in design and operation
- lessons are learned from events, changes, trends, successes and failures
- changes in the external and internal context, including the risk criteria, are detected and revised
- emerging risks are identified and managed accordingly.

Where a risk is identified, or changes, between nominated review dates, and needs to be immediately reviewed, the risk should be immediately addressed and reported to the appropriate manager.

Systems for reporting and investigating incidents are fundamental to the management of disruptive events and incidents. The University is committed to ensuring appropriate effective reporting and investigation processes exist and are being followed accordingly.

**Implementation Officer**

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

## LEGISLATION:

The University is required maintain a critical incident policy and procedures to ensure the interests of students (including international students and students under the age of 18) and their families are managed appropriately under the National Code of Practice for Providers of Education and Training to Overseas Students 2018 (National Code 2018).

## SUPPORTING INFORMATION:

List related documents:

- Risk Management Plan
- University Business Continuity Plan and supporting team plans
- Critical Incident Management Team Plan
- IT Disaster Recovery Plan
- Emergency Management Response Plan, policies and procedures
- Fraud and Corruption Control Plan
- Health and safety policies and procedures
- IT Policy Manual.
- Privacy Policy
- Security Policy

**Review**

This Framework will be reviewed every three years (or more frequently following a major change to business operations and/or priorities). The Governance unit will work with all areas across the University to ensure that the Framework, embedded policy and associated business processes continue to meet local needs as resilience management matures and improves.

**References**


- Australian and New Zealand Standard *AS/NZS ISO 31000:2018 Risk Management - Guidelines*
- Australian and New Zealand Standard *AS/NZS 5050:2010 Business Continuity – Managing disruption-related risk*
- Australian Standard *AS 8001-2008 Fraud and Corruption Control*
- Australian Standard *AS 3745-2010 Planning for emergencies in facilities*
- Commerce and Works Directorate, ACT Government (2013) *Risk Management Framework and Policy.* Australian Capital Territory, Commerce and Works (v 1.0).
- Griffith University (2013) *Risk Management Framework.* Queensland.
- Griffith University (2014) *Risk Management Policy.* Queensland.
- University of Sunshine Coast (2013) *Enterprise Risk Management and Resilience – Governing Policy.* Maroochydore, Queensland.