

Risk and Resilience Management

- 1.0 Purpose
- 2.0 Scope
- 3.0 Objectives
- 4.0 Principles
- 5.0 Foundation Components
- 6.0 Review of Documents
- 7.0 Roles, Responsibilities and Delegations
- 8.0 Definitions

1.0 Purpose

Griffith University (University) is committed to managing risk in line with our values and to support the achievement of our core commitments.

The overall aim of risk and resilience management is to assist the University in achieving its objectives by appropriately considering threats and opportunities to make informed decisions and mitigate risks.

This Policy is the guiding document in the Enterprise Risk Management Framework (ERMF) and the Resilience Framework (RF) and is supported by a suite of risk and resilience artefacts.

The ERMF provides a detailed handbook and tools and guidance on the application of risk management across the University and details the roles and responsibilities relating to risk management and is aligned to the 'Three Lines of Accountability' model.

The RF provides detailed tools and guidance to assist the University to prevent, prepare for, respond to, and recover from any event that may negatively impact Griffith University's operational and strategic objectives.

2.0 Scope

This policy applies to all areas of the University's operations, including its staff, appointees of the University, its controlled entities, and to all activities authorised and conducted by or on behalf of the University.

3.0 Policy Statement

The University is committed to:

- Embedding risk management into day-to-day activities and operations, including strategic planning, project management, financial planning, and overall decision making
- Adopting a systematic approach to the management and oversight of risk with appropriate delegation
- Clearly defining roles and responsibilities of individuals and educating staff in the processes for managing risk
- Identifying, analysing, evaluating and treating risks in a manner consistent with the University's values and core commitments while recognising that opportunities for innovation and new business opportunities exist
- Anticipating threats to Griffith University's strategic and operational objectives
- Regularly considering and updating the University's Risk Register and Risk Profile including the identification of emerging risks

- Developing action plans to minimise the potential impact of key risks and maximise the return on investments, within the Council approved Risk Appetite
- Complying with applicable legislative and regulatory requirements
- Responding, reporting and learning from material incidents and breaches
- Providing timely assurance to the Committees and Council
- Undertake reviews of the ERMF and seek to continually improve the effectiveness of risk management
- Develop capability to prevent, prepare for, respond to and recover from business disruptions
- Empowering teams and individual leaders to develop resilience to manage disruption events and threats.
- Integrate all levels of risk and resilience to create a consistent and enterprise-wide approach
- Building on and supporting existing organisational knowledge, skills and systems to ensure practical adoption of risk management and resilience principles and capabilities.

4.0 Principles



Values

Our core principles of excellence, ethics and engagement guide our approach to managing risk

We support a positive risk culture through:

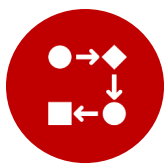
- If we see something, we take appropriate action
- We encourage a spirit of transparency and openness in the declaration of risks whether actual or perceived
- We encourage courageous conversations to challenge behaviours or activities not aligned with core values
- We support a safe environment where open communication, curiosity, diversity in thought and learning is encouraged
- In pursuit of excellence and high-quality education and research we include risk thinking before, during and after any activity or decision-making process
- We consider inclusion and diversity, environmental sustainability and social justice within our decision-making process



Accountable

We are each accountable for contributing to effective risk management across the University:

- We take ownership of risks, controls, mitigation plans, issues and obligations within our control or influence
- We collaborate to understand and mitigate risks that span multiple areas of the University
- We monitor our risks and provide timely assurance via established reporting mechanisms
- We regularly consider and report on emerging risks and issues



**Integrated &
Systematic**

Risk management is not an after-thought:

- We consider risk appetite in our choices
- We identify learning opportunities and ways to improve
- We aim to prevent and prepare for risks before they occur
- We aim to efficiently respond and recover from events if they occur
- We report potential or actual incidents in a timely manner

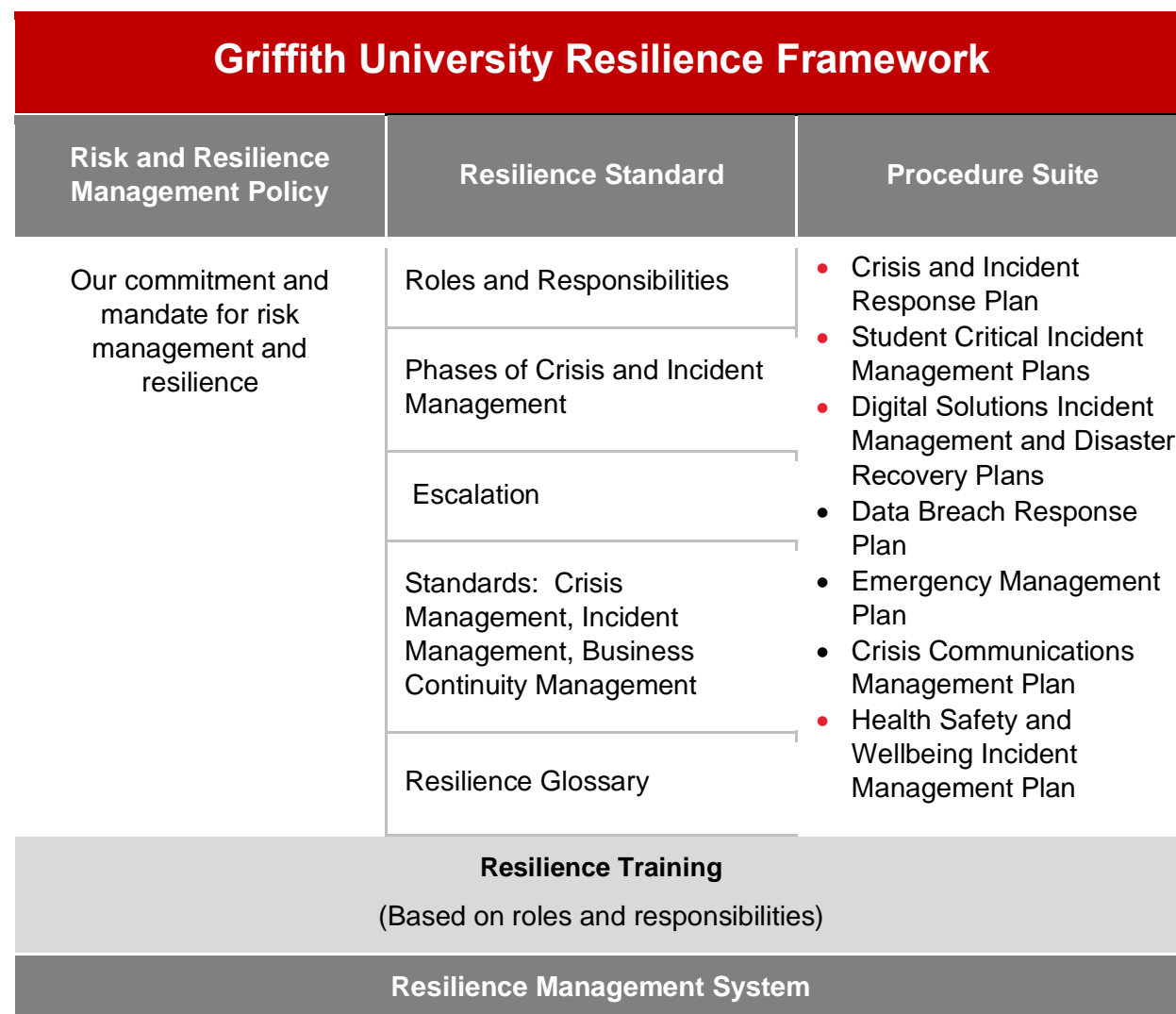
5.0 Foundation Components

This policy is operationalised through the Enterprise Risk Management and the Resilience Frameworks each include a set of components and artefacts that provides the foundations, processes and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management and BCM throughout the University.

Enterprise Risk Management Framework

Griffith University Enterprise Risk Management Framework		
Risk and Resilience Management Policy	Risk Appetite Statement	Risk Management Handbook
Our commitment and mandate for risk management and resilience	Setting the boundaries and embedding smart risk taking	1. Introduction and Overview
		2. Risk Management Process with Likelihood, Consequence and Velocity tables and the Risk Matrix
		3. Risk Assurance and Control
		4. Key Terms and Definitions
Risk Management Training (Based on roles and responsibilities)		
Enterprise Risk Management System		

Resilience Framework



6.0 Review of Policy

The Policy will be reviewed every second year or earlier if required by a change in circumstances. Any changes (other than administrative matters) should be approved by the Council.

7.0 Roles, responsibilities and delegations

ROLE

RESPONSIBILITY

Line 1

Vice Chancellor

Accountable for the implementation of risk management and allocation of appropriate resources

Sets a strong 'Tone from the Top'

Has oversight of the University's risk profile, risk management activities, and escalates risks that exceed the Council's risk appetite

Executive Group

Individually, responsible for the implementation of the ERMF, the risk profile and resourcing risk management activities for their Group / Element

Role models and reinforces positive risk behaviours and sets a strong 'tone from the top'

**Senior Leaders
(Including: Deputy Vice
Chancellors, Pro Vice
Chancellors, Vice Presidents,
Directors, Deans etc.)**

Designs and implements internal controls that help to manage risks to the desired level and within the Council's risk appetite

Monitors the status of risks and evaluates the effectiveness of controls and action plans

Promotes a culture of risk within the Group / Element

Maintains up to date risk registers

Works collaboratively with the Enterprise Risk Team

Assists in University risk reporting

Escalates High and Very High rated risks to the Executive Group

Management and Staff

Be aware of the risks that relate to their day-to-day role and promote a shared understanding of the risks among their team. All staff should be responsible for taking action to manage risks

Identifies new or changing risks and report the potential threat to their Manager

Managers should make sure that reasonable action is taken to assess reported risks and identify appropriate risk owners. The risk owner decides how to manage the risk

Shares information on current and emerging risk, issues or compliance concerns with their Managers

Liaises with the Enterprise Risk Team for support and resources

Line 2

General Counsel

Oversees the development of the ERMF, in conjunction with the Associate Director Risk & Resilience

Assists the Council and Audit and Risk Committee in meeting its risk oversight responsibilities

Assists the Executive Group in meeting its risk management responsibilities

Supports the development of a positive risk culture across the University

Facilitates and reviews risk reporting and communicating with the Audit and Risk Committee and Executive Group

Escalates strategies, plans, major projects or actions that may cause the University to exceed risk appetite to the Executive Group and Audit and Risk Committee and Council

Validates the University's external risk reporting obligations

Where necessary, calls upon external risk management specialist skills for support

Identifies and supports the development of capabilities needed for the risk function

**Associate Director Risk & Resilience
(Risk Function)**

Develops, implements and maintains the ERMF which aligns to the University's strategic commitments, better practice and the Three Lines Model

Provide assurance by advising and 'challenging' the effectiveness of the application of the risk management process, and the outcomes (e.g. risk assessments, profiles, controls, control monitoring)

Facilitates a positive risk culture across the University

Provides risk management support, coaching and guidance to Groups, Elements, Divisions and Schools to identify risks, provide risk training and assists in applying risk appetite to business strategies, plans or actions

Prepares risk reporting for relevant stakeholders and Committees

Prepares any external risk reporting obligations

Liaises with the risk champions / risk owners to assist in timely and accurate risk reporting

**Risk Champions
(Mix of Line 1 & 2)**

1st line responsibilities

Develops / maintains / reports on risk registers (coordinate with risk owners)

Develops / maintains key risk indicators (coordinate with data owners)

Liaises with the Enterprise Risk Team

Supports Managers and Senior Leadership to implement the ERMF and embed risk management into day-to-day work. e.g. Highlighting when a risk assessment may be needed as part of a decision-making process

2nd line responsibilities

Coordinates control self-assessments for 'key controls' with control owners

Monitors risk treatment plans

Assists in training delivery – risk, risk system (dual role with the Enterprise Risk Team)

Assists with plan exercises

Oversight of timely risk management and reporting

Line 3

Internal Audit

Carries out reviews and internal control advisory activities

Provides independent assurance to the Audit and Risk Committee and Council on the adequacy and effectiveness of the control environment and ERMF

Governing Bodies

University Council

Accountable for the management of risk across the University and assuring itself, through delegation to the Audit and Risk Committee, that this obligation is being met

Delegates approval of the ERMF and Risk Appetite Statement to the Audit and Risk Committee

Other detailed responsibilities outlined in the Griffith University Act, 1998 and Council Handbook

Audit and Risk Committee (ARC)

Reviews and make recommendations to the Council on the risk management policy and strategy

Monitors the implementation of the risk management strategies

Approves, with delegated authority from the Council the ERMF, the Risk Appetite Statement and risk Registers

Has oversight of risk identification and material risks being managed and mitigated

Has oversight of risk management, compliance and control practices across the University

Assesses the effectiveness of the risk management system and the various sources of assurance and their overall adequacy

Reports and advises the University Council as appropriate

Executive Group (EG)

Collectively, provides leadership on the desired risk culture

Reviews the risk profile of the University and evaluates and prioritises material and University-wide risks

Provides a strategic and holistic view of the University's operating and risk context

Identifies and discusses emerging risks

Monitors and reviews the effectiveness of the ERMF

Provides necessary support and resources to develop, implement and monitor the ERMF and internal controls

8.0 Definitions

For the purposes of this policy and related documents, the following definitions apply:

Business Continuity Management Framework means the set of components that provide the methodology, processes, definitions and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving preparing and responding to disruptive events.

Crisis events that threaten the University's strategy, viability, financial stability or reputation, and may involve high levels of public or stakeholder examination.

Enterprise Risk Management Framework (ERMF) means the set of components that provide the methodology, processes, definitions and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management.

Risk Appetite Statement. The documented amount and type of risk that the University is willing to pursue or retain in order to achieve our goals or pursue opportunities

Risk Management means the coordinated activities to direct the University towards realising potential opportunities whilst managing adverse effects of risks.

Risk Management Policy means a statement of the University's overall intentions and direction related to risk management.

Resilience refers to the University's capacity to adapt to new situations and thrive when faced with different challenges.

For advice and support contact policy@griffith.edu.au for Governance and Operational policy documents.

Information

Title	Risk and Resilience Management Policy
Document number	2024/0001095
Purpose	This Policy outlines the University's commitment to establishing and maintaining an Enterprise Risk Management Framework and a resilient University through an integrated approach to the management of the University's risks and establishing and maintaining an effective business continuity management (BCM) program.
Audience	Staff
Category	Operational
Subcategory	Risk
UN Sustainable Development Goals (SDGs)	This document aligns with Sustainable Development Goal: 16: Peace, Justice and Strong Institutions
Approval date	21 October 2024
Effective date	21 October 2024
Review date	2026
Policy advisor	General Counsel
Approving authority	University Council

Related Policy Documents and Supporting Documents

Legislation	Financial Accountability Act 2009 Griffith University Act 1998 Statutory Bodies Financial Arrangements Act 1982
-------------	---

Work Health and Safety Act 2011

Policy

Health, Safety and Wellbeing Policy
Student Critical Incident Management Policy

Procedures

Business Continuity Management Process
Business Continuity Management Standard
Crisis and Incident Management Guidelines
Crisis Incident Management Standard
Data Breach Response Plan
Emergency Management Plan
Enterprise Risk and Resilience Management Frameworks
Health and Safety Plan
Information Security Procedure
Risk Registers

Local Protocol

N/A

Forms

N/A