Business Resilience Policy

Section 1 - Purpose

(1) The purpose of this policy is to establish RMIT's Business Resilience Framework to enable the University to anticipate, withstand, respond and recover from potential threats, and the resultant impacts to business operations. RMIT's priority is to safeguard people, processes, assets and place, in line with its dhumbali (commitment) to the Bundjil Statement.

Section 2 - Overview

(2) This policy outlines the principles, roles and responsibilities associated with RMIT's Business Resilience Framework which encompasses:

a. critical incident management (CIM)
b. business continuity management (BCM)
c. IT disaster recovery (ITDR).

Section 3 - Scope

(3) This policy applies to all employees, researchers, third parties and contractors of RMIT and its controlled entities.

Section 4 - Policy

(4) Business resilience activities are governed by RMIT's Business Resilience Framework (Framework). Adherence to this Framework enables the University to have a consistent and coordinated approach to business resilience.

(5) Each of the Framework's three capabilities (CIM, BCM and ITDR) will be considered as part of all key conversations, analysis, recommendations and decision making.

(6) RMIT will take a risk-based approach to business resilience and prioritise activities that address the greatest source of risks to the University.

(7) RMIT will effectively communicate information relating to incidents, disruptions or disasters to all University stakeholders. Incidents will be managed and responded to it in a coordinated, consistent and sustainable manner.

Business Resilience Framework

(8) The Business Resilience Framework defines the overarching capabilities, process, and roles and responsibilities that underpin business resilience for RMIT.

(9) The objective of the Framework is to ensure staff, student and visitor safety and wellbeing whilst ensuring RMIT's services to various stakeholders will continue to be available with minimal interruption in the event of a critical incident, business disruption and/or IT disaster.

(10) The Framework is underpinned by three capabilities which enable the University to plan for, respond to, and recover from different aspects of a disruptive event or incident. Depending on the nature and extent of the risk or threat, these capabilities may be activated independently, or in conjunction with each other.

a. Critical incident management (CIM) provides a systematised approach to the immediate response, management and direction of activities for critical incidents. It encompasses the strategic level management of critical incidents including, but not limited to, natural disaster (both onshore and overseas), injury, death, technology, security – both technical and physical - explosives, chemical, biological and nuclear hazards affecting RMIT buildings and assets.
b. Business continuity management (BCM) is a holistic management process that identifies potential threats to an organisation and the impacts to business operations if those threats materialise. BCM defines the foundations on which to build effective response capability to safeguard our stakeholders, people, technology, reputation, brand, premises and business processes.
c. IT disaster recovery (ITDR) protects the organisation from the effects of significant technology-focused disruptive incidents. Significant disruptive incidents are those that place RMIT's operations at risk, including cyber-attacks, equipment failures and data corruption.

Responsibilities

(11) The Vice-Chancellor's Executive is responsible for monitoring the ongoing development and implementation of a robust policy framework and effective management systems and processes aligned to the vision, mission and objectives of the University.

(12) The Director, Risk Management is responsible for oversight and management of the Business Resilience Framework.

(13) The Enterprise Risk Management is responsible for:

a. overseeing the implementation of the Business Resilience Framework including the execution of the following framework aspects:
    i. roles and responsibilities
    ii. business resilience process
    iii. interaction between the framework capability elements (i.e. BCM, CIM and ITDR)
b. assurance activities, including the conduct of reviews to assess the effectiveness of Business Resilience controls and processes.

(14) The Critical Incident Management Team is responsible for:

a. providing clear roles and responsibilities related to CIM
b. developing effective and clear approaches, processes and plans for CIM
c. collaborating with the business resilience teams to execute plans in both testing and live incident scenarios.

(15) The Business Continuity Management Team is responsible for:

a. providing clear roles and responsibilities related to BCM.
b. developing effective and clear approaches, processes and plans for BCM.
c. collaborating with the business resilience teams to execute plans in both test and live incident scenarios.

(16) The IT Disaster Recovery Team is responsible for:

a. providing clear roles and responsibilities related to ITDR.
b. developing effective and clear approaches, processes and plans for ITDR.
c. collaborating with the business resilience teams to execute plans in both test and live incident scenarios.

(17) All employees, researchers, third parties and contractors are responsible for:

a. understanding and adhering to any responsibilities they may have under this policy and the Framework, including those from the underlying CIM, BCM and ITDR capabilities.
b. contributing and participating in the identification, escalation and management of business resilience related risks.

Compliance

(18) Compliance with this policy will be monitored. Non-compliance may result in disciplinary action, which may include termination of employment or engagements. Breach of the law may also lead to personal liability such as fines or imprisonment.

Review

(19) RMIT's Business Resilience Framework and strategies will change over time. Business resilience will be monitored and reviewed to ensure the approach to business resilience remains appropriate and effective.

(20) This policy will be reviewed at least annually or more frequently if necessary.

Section 5 - Resources

(21) Refer to the following documents which are established in accordance with this Policy:

a. Business Resilience Framework

Section 6 - Definitions

(22) (Note: Commonly defined terms are in the RMIT Policy Glossary. Any defined terms below are specific to this policy).

Business continuity (BC)	The strategic and tactical capability of the organisation to plan for and respond to incidents in order to continue business operations at an acceptable pre-defined level.
Business continuity management (BCM)	A holistic management process that identifies potential threats to an organisation and the impacts to business operations, if those threats materialise. BCM defines the foundations on which to build effective response capability to safeguard our stakeholders, people, technology, reputation, brand, premises and business processes.
Business recovery plan (BRP)	A documented set of procedures designed to ensure that critical business functions can continue to be performed at a minimum acceptable level during an incident and to support the effective and rapid restoration of business-as-usual (BAU) activities.
Business impact analysis (BIA)	The business impact analysis (BIA) is a foundation step in business continuity management (BCM) to identify the organisation's critical business functions, supporting resources and people requirements, along with an identification of the negative impacts that would occur because of the inability to perform these functions over a period of time during an incident. The BIA enables the organisation to determine the business case, and the appropriate scope, for all continuity planning efforts.

Business Continuity Management Team	Responsible for the implementation and governance of business continuity management at RMIT globally. The team will develop and maintain the Business Resilience Policy, develop business continuity standards and framework and create the templates required to ensure a standard implementation approach and increase maturity.
Critical incident/crisis	A sudden, serious incident which may have severe legal, financial and/or reputational implications to RMIT and significantly affect RMIT-related people, facilities or equipment.
Critical Incident Management Team (CIMT)	The task-built team established by RMIT that manages the response and recovery effort in the event of a critical incident. This team can consist of operational, functional and specialist members depending on the type of incident and the breadth of impact on RMIT.
Incident	An adverse incident that has the potential to have a significant impact on the University's people operations, environment, its long-term prospects and/or reputation.
Maximum acceptable outage	The period of time beyond which the business impact caused by the inability to perform a specific critical business process becomes unacceptable. Triggers for unacceptable loss include accumulated financial loss, operational disruption, regulatory breach, OHS incident or reputational impacts.

Status and Details

Status	Historic
Effective Date	19th October 2020
Review Date	3rd June 2024
Approval Authority	Vice-Chancellor's Executive
Approval Date	26th August 2020
Expiry Date	1st August 2024
Policy Owner	Teresa Finlayson Chief Operating Officer
Policy Author	Sinan Erbay Chief Information Officer
Enquiries Contact	ITS Governance, Risk and Compliance