Business Continuity and Recovery Management Policy

1. Purpose

The purpose of this policy is to provide Auckland Transport (AT) with direction for its business continuity management for disruptive events that have an impact on the critical business functions of the organisation.

The Business Continuity and Recovery Management Policy sets out the roles, responsibilities, and principles by which disruption-related risk can be effectively and consistently managed throughout the organisation.

2. Scope

This policy applies to all business services/functions of AT and anyone engaged by AT to work on those services/functions. This includes:

- All AT employees;
- AT representatives (in accordance with the terms of their agreement with AT), including: :
  - Contractors and consultants,
  - Third party suppliers,
  - Agency temps (in accordance with the terms of the supplier agreement with AT),
  - Staff on secondment from other organisations/agencies,
  - Volunteers; and
- AT Board Directors.

This Policy does not apply to business continuity management or policies of third parties. AT is not responsible for developing business continuity management policies for any third parties operating on AT's behalf. Some third parties may be responsible for establishing their own business continuity framework and processes which AT may request for review, as per the relevant contract terms.

3. Policy Principles

By following the policy's principles, we help to do the following in disruption-related events:

- Ensure that the welfare and safety of all staff, contractors and customers is a primary focus.
- Maintain communication with the AT Board, staff, customers, contractors, partners, and agencies during operational disruption.
- Reduce the impact of significant operational disruption.
- Proactively manage the customer experience.
- Maintain public and customer trust and confidence, and AT's reputation.

- Promote and embed a consistent enterprise-wide Business Continuity process.
- Establish clear responsibilities for Business Continuity and Recovery Management.
- Support a culture where employees understand and proactively manage disruption-related risk.

Roles, responsibilities, and accountabilities are clear and understood

- Business Continuity and Recovery Management is a key component of risk management across the organisation. The accountability for people, process and systems are clearly defined to support this.
- The roles and responsibilities are clearly documented and detailed, to support effective recovery and continuity. See “Effective Plans” below.

Adequate resources are made available to implement and support the business continuity framework

- We need to commit an appropriate level of time and budget into business continuity management. By doing this, we help to ensure that the impact of a disruption is minimised.
- We recognise that if we do not dedicate adequate resource to business continuity management, the is a risk of greater disruption and cost.

Critical business functions and their interactions are identified and assessed

- To effectively plan and manage business continuity, we need to understand what AT’s critical business functions are. Each business unit needs to identify its critical business functions, including those functions and processes that are outsourced or managed by suppliers.
- When multiple critical business functions are concentrated in an area, or interdependent on each other, it creates risks of major operational disruptions. When assessing critical business functions, we need to also consider how they relate and impact others.
- We need to ensure that robust risk assessments are completed (and captured in AT’s risk register) to:
    - assess and analyse the impacts from such disruptions, and
    - manage and mitigate the risks

Level of protection and redundancy

- For each critical business function, it is important to assess the mitigations needed, and ensure that there is an appropriate level of protection and redundancy in the system to reduce both the likelihood and effect of disruptions. This should consider things like: key staff, information systems, supporting infrastructure, and business activities.

Effective plans

- Response and recovery **Plans** and processes are created to guide the continuity and recovery processes for each business area.
- These organisational plans need to be in sufficient detail to support effective continuity and recovery of the business processes that support prioritised activities, products, and services, in a consistent manner that is easily understood by end users.
- Technical response and recovery plans need to be created with sufficient detail to ensure the continuity of service for each respective technology asset, that support prioritised activities, products, and services in a consistent manner.

Continual improvement

- Strategies and regular reviews must be in place to ensure the plans remain current, relevant and can be practically applied.
- A programme of exercising and testing is in place, using multiple scenarios, to validate, over time, the effectiveness of the documented plans and associated strategies and solutions.

4. Definitions

Term	Definition
Business Continuity Management (ISO 22301)	The capability of an organisation to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption
Business Continuity (ISO 22301)	The capability of an organisation to continue the delivery of products or services at acceptable predefined levels following a disruption
Competence (AS/NZS 5050)	Ability of people, functions, processes and/or infrastructure to undertake required actions or activities.
Continuity	Used as a collective term to include response, recovery and resumption of activities impacted by a disruption
Crisis (AS/NZS 5050)	An unexpected, non-routine situation that is beyond the capacity of normal management structures and processes to deal with effectively, has both strategic and operational implications, and is often perceived as a potential existential threat
Critical Business Functions (AS/NZS 5050)	A business function or part thereof identified as essential for survival of the organisation and achievement of its **critical objectives**[1].

[1] A business function which has the effect of protecting critical interests of the community or another stakeholder to which a duty is owned, may qualify as a critical business function.

Term	Definition
Critical Objectives (AS/NZS 5050)	Objectives that must be achieved during a period of disruption[2].
Disaster Recovery Plan (ISO 27031)	A clearly defined and documented plan which recovers information and communications technology (ICT) capabilities when a disruption occurs
Disaster Recovery (ISO 27031)	The ability of the ICT elements of an organisation to support its critical business functions to an acceptable level within a predetermined period of time following a disruption
Disruption (ISO 22301)	**Incident**, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organisation's objectives
Documented Information (ISO 22301)	Information required to be controlled and maintained by an organisation and the medium on which it is contained[3]
Emergency Plan	A written document associated with an asset, which defines the actions intended to protect people, the environment, and property from adverse consequences associated with emergency situations
Emergency Response	The performance of actions to mitigate the consequences of an emergency for human health and safety, quality of life, property and the environment, rapid IT response
Emergency (ISO 22300)	A sudden, urgent, usually unexpected occurrence or event requiring immediate action[4]
Exercise (ISO 22300)	A process to train for, assess, practise, and improve performance in an organisation
Incident Management	A defined process for logging, recording, and resolving incidents
Incident Management System (ISO 22300)	The system that defines the roles and responsibilities of personnel and the operating procedures to be used in the management of incidents
Incident (ISO 22301)	Event that can be, or could lead to, a disruption, loss, emergency, or crisis

[2] Critical objectives may reflect the requirements of external stakeholders.

[3] Documented information can be in any format and media, and from any source. Documented information can refer to:
- the management system, including related processes;
- information created in order for the organisation to operate (documentation);
- evidence of results achieved (records).

[4] An emergency is usually a disruption or condition that can often be anticipated or prepared for, but seldom exactly foreseen.

Term	Definition
Incident (H&S) (ISO 45001)	Occurrence arising out of, or in the course of, work that could or does result in injury and ill health[5]
Objective (ISO 22301)	Result to be achieved
Plans (ISO 22300)	The documented collection of procedures and information that is developed, compiled, and maintained in readiness for use in an incident. These plans include, but are not limited to: • **Crisis** Management • **Business Continuity** • **Disaster Recovery Plan**/Service Continuity • **Emergency Plan/Scheme/Procedure** • **Incident Management**
Prioritised (ISO 22301)	Activity to which urgency is given in order to avoid unacceptable impacts to the business during a disruption
Recovery (ISO 22300)	The restoration and improvement, where appropriate, of operations, facilities, livelihoods or living conditions of affected organisations, including efforts to reduce risk factors
Risk (ISO 31000)	The effect of uncertainty on objectives

5. Roles and Responsibilities

Role	Responsibility
All employees and representatives	• Adhere to and comply with the Risk Management Policy; and • Adhere to and comply with this policy and related procedures; and • Provide input and be familiar with the relevant functional Business Continuity and/or other plans; and • Adhere to all **Emergency** Management plans and procedures; and • Remain familiar with and adhere to all cyber security requirements.

[5] An incident where injury and ill health occurs is sometimes referred to as an “accident”.
An incident where no injury and ill health occurs, but has the potential to do so, may be referred to as a “near-miss”, “hear-hit”, or close call.

Role	Responsibility
Senior Leadership Team	• Allocate adequate **competent** resources to develop, implement, maintain, and test plans and procedures, as outlined in: ▪ Business Continuity and Recovery Framework ▪ Health and Safety Emergency Standards and procedures ▪ Business Technology Disaster Recovery and Incident Management Policies, Plans and Procedures ▪ NZTA / Waka Kotahi requirements for ATOC ▪ ATOC Incident Management ▪ AT H&S Incident management as required, within the business areas under their control; and • Ensure relevant staff are trained and exercised in implementing the plan/s.
Third Parties	• Critical or strategically significant Third Parties are required to provide evidence of Business Continuity, Service Continuity, Incident Management and Emergency Management capability as stated in individual supplier agreements.
Manager Risk Services	• Ensure the Business Continuity Framework complies with relevant regulatory and legal requirements as well as any directives that may be issued by regulatory authorities and shareholders; and • Ensure annual testing is conducted and regular updates of business continuity documents and processes by internal or relevant external party; and • Provide guidance to the ELT to support effective implementation of the Business Continuity across their business areas; and • Update and maintain the Business Continuity and Recovery Management Policy and Framework.
Executive General Manager, Health, Safety & Wellbeing	• Ensure the Health and Safety Emergency Standard complies with relevant regulatory and legal requirements as well as any directives that may be issued by regulatory authorities and shareholders • Prepare and maintain the standards and procedures for Emergency and H&S Incident Management to ensure that guidance to the business is provided to facilitate adequate Incident and Emergency Management coverage of AT occupied buildings and publicly used assets. • Provide support to ensure adequate preparedness for Emergency Management and H&S Incidents across AT locations, managed by Infrastructure and Place, Public Transport Services and Active Modes, People and Performance and Customer and Network Performance, and Emergency Management and H&S Incident Management requirements are included in Project Management process for new build of AT Assets (e.g., train stations).
Chief Technology Officer	• Prepare, maintain, and implement BT policies, frameworks, plans and procedures for IT Incident Management and Disaster Recovery.

Role	Responsibility
Chief Executive and Executive Leadership Team	• Review and support the Business Continuity and Recovery Policy, Framework, and strategies; and • Ensure effective implementation of the Business Continuity Framework or approach across their respective business areas; and • Allocate appropriate people, resources, and training to increase organisational awareness on business continuity and preparedness; and • Allocate appropriate people, and resources to develop and maintain plans; and • Ensure that all contracts made with critical or strategically significant third parties contain appropriate business continuity requirements and SLAs. • Ensure clear articulation of roles, responsibilities, authorities, and succession plans; and • Ensure that business continuity and recovery related matters are reported to the board of directors at least annually.
AT Board	• Approve the policy for managing Business Continuity and Recovery; and • Provide governance over the Business Continuity and Recovery process to protect value for stakeholders and support the achievement of the organisation's objectives; and • Understand and agree the board's role and expectations ahead of time so that AT can respond quickly and collectively to a crisis event.
Finance and Assurance Committee (FAC)	• Review and endorse the Business Continuity and Recovery Management Policy for approval by the Board; and • Monitor the organisation's management of Business Continuity and Recovery risks and related processes.

6. Supporting Information

Legislative compliance	This Policy supports Auckland Transport's compliance with the following legislation: • Civil Defence Emergency Management Act (2002) • Health and Safety at Work Act (2015) • Fire and Emergency New Zealand (Fire Safety, Evacuation Procedures, and Evacuation Schemes) Regulations (2018) • Fire and Emergency New Zealand Act (2017)
Supporting documents	• AT Business Continuity Management Framework • AT Risk Management Policy • Health and Safety Emergency Management Procedures HS11.1 • BT Disaster Recovery Policy • BT Disaster Recovery Strategy • Information Security Policy

Related documents	• AS/NZS 5050 (2020), Managing disruption-related risk • Auckland Council Business Continuity Policy 2018 • Coordinated Incident Management System (CIMS) 3rd Edition, National Emergency Management Agency • ISO 22300:2018, Security and resilience - Vocabulary • ISO 22301:2019, Security and resilience - Business continuity management systems – Requirements • ISO 27031:2011 Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity • ISO 31000:2018, Risk Management • New Zealand Information and Security Manual (NZISM) - Business continuity and disaster recovery • The Guide to the CDEM Plan 2015

7. Non-Compliance

Business continuity management supports the compliance to multiple governance, legal, regulatory, government and shareholder requirements. Non-compliance perceived or otherwise, with those requirements can lead to increased scrutiny, investigations and reviews, penalties and in extreme circumstances prosecution and fines.

8. Approval and Review

Policy Owner: Head of Risk & Assurance	**Policy Contact:** Risk Services Manager
Endorsed by:	**Approved by:**
Chief Executive **Effective date:** xx 2024	Auckland Transport Board **Next review date:** xx 2027

AT reserves the right to review, amend or add to this policy at any time upon reasonable notice to employees and representatives.