Business Continuity Management Policy

Table of Contents

Policy statement and principles

What

This policy covers the NZ Police approach for Business Continuity Management (BCM). BCM is about:

- managing the risk of disruptions impacting our ability to operate; and
- building resilience across our business.

Why

Police is relied on by the public, our partners, and Government to be prepared to continue carrying out policing functions to the best of our ability, regardless of the circumstances.

If we are unable to carry out our functions we may be unable to achieve Our Business - including our Vision (to have the trust and confidence of all), Mission (to be the safest country), and Purpose (Be safe, Feel safe).

Police Essential Services

Police has a number of legislative functions, which are underpinned by a range of enabling functions - both operational and corporate - that enable us to continue operating effectively. Together, these legislative functions and enabling functions make up our “Essential Services”.

Each of our legislative and enabling functions relies on many components across Police - and a wide range of people, information, and physical assets - working together to deliver, and so our Essential Services are reliant on all parts of Police understanding their role in delivering these, dependencies, and risks to their ability to continue doing so.

Although our Essential Services are non-negotiable, the priority of each at any one time will depend on the nature of the disruption and the context in which it occurs.

Legislative functions - s9 Policing Act:

a. Keeping the peace;
b. Maintaining public safety;
c. Law enforcement;
d. Crime prevention;
e. Community support and reassurance;
f. National security;
g. Participation in policing activities outside New Zealand; and
h. Emergency management.

Enabling functions:

In order to carry out our legislative functions we rely on a range of other functions across our business which maintain and support our people, information, and physical assets, or ensure we continue meeting other legal, regulatory, and organisational requirements to operate.

What is a disruption?

The form, scale, source, and effects of potential disruptions are varied, however generally a “disruption” is anything that happens which:

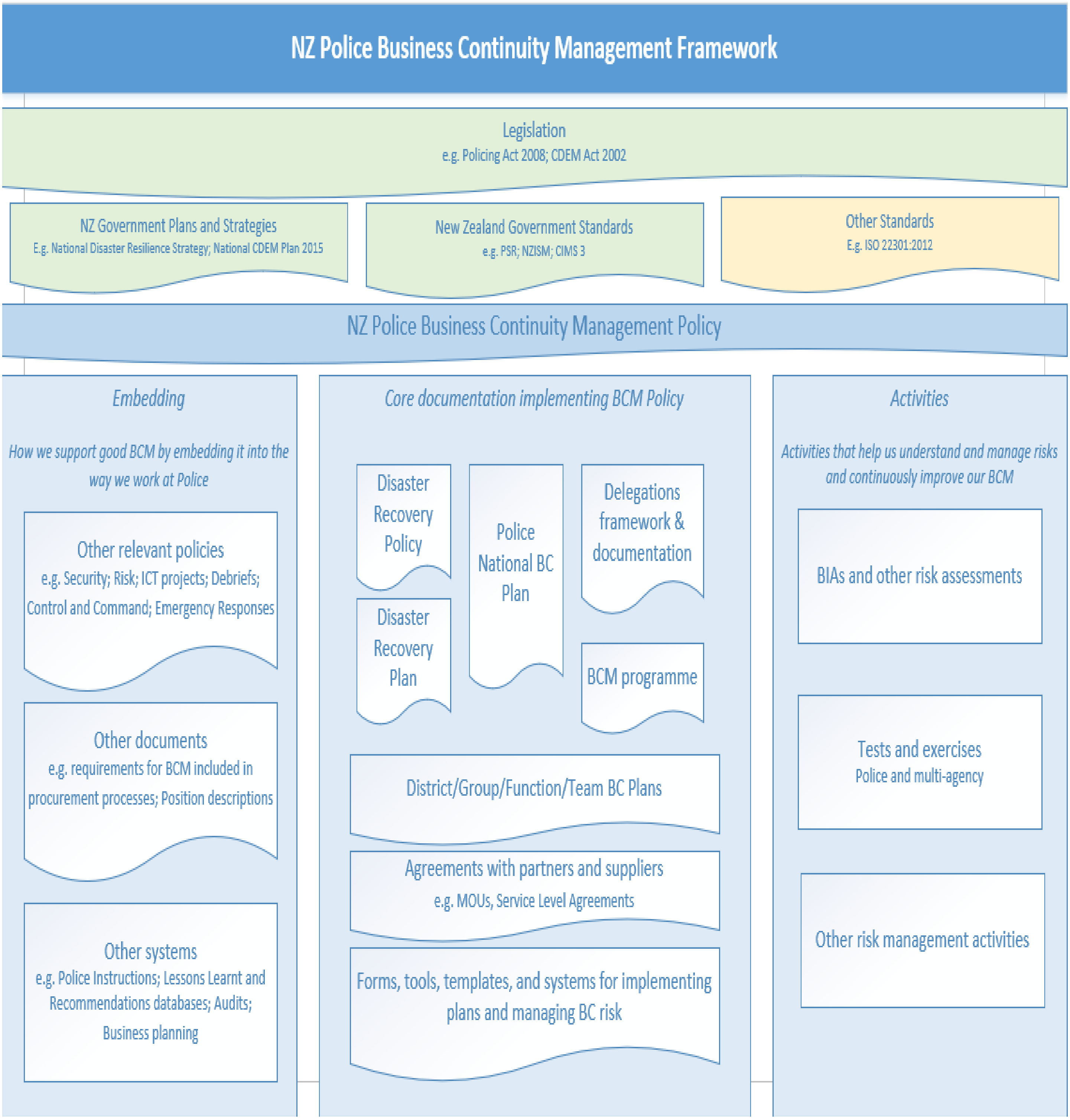
- is unexpected or outside of BAU;
- affects one or more of our assets - our People, our Information (including access to information), or our Physical assets (including buildings, kit, IT infrastructure); and
- affects our ability to carry out one or more components of our Essential Services for a period of time.

Not all disruptions will activate BCM provisions - this will depend on the internal and external context in which the disruption occurs, the Police assets affected, and how this impacts our Essential Services.

How do we manage disruption-related risk?

Police’s framework for managing disruption-related risk is set out below. The framework includes legislation and NZ Government standards we must comply with, under which sits this policy - containing Police’s expectations and approach, and then all of the different documents, systems, and activities across our business that help us implement our policy and embed BCM best practice into the way we work.

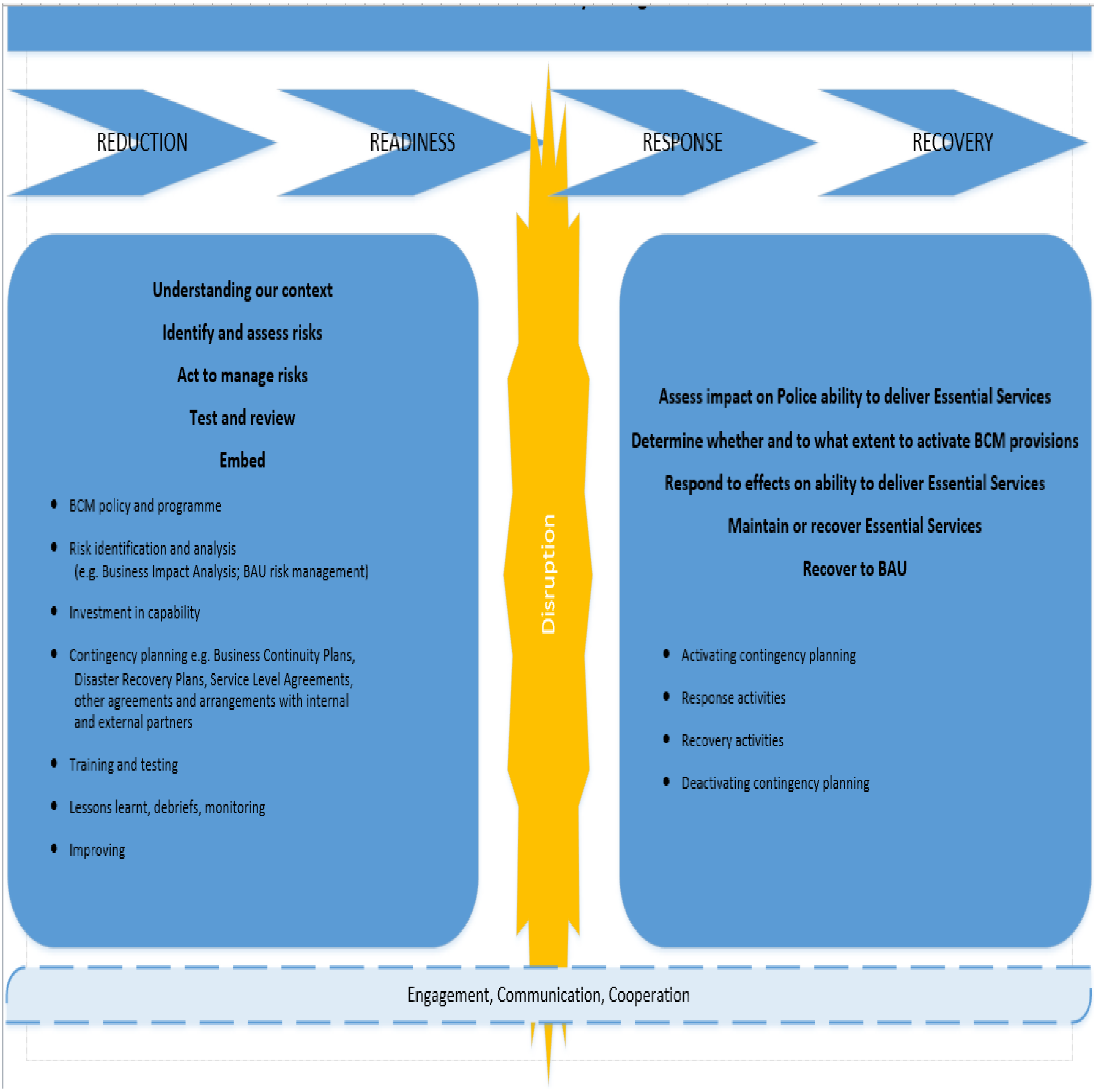
Proactively released by New Zealand Police


NZ Police Business Continuity Management Framework
Legislation
e.g. Policing Act 2008; CDEM Act 2002
NZ Government Plans and Strategies
E.g. National Disaster Resilience Strategy; National CDEM Plan 2015
New Zealand Government Standards
e.g. PSR; NZISM; CIMS 3
Other Standards
E.g. ISO 22301:2012
NZ Police Business Continuity Management Policy
Embedding
How we support good BCM by embedding it into the way we work at Police
Other relevant policies
e.g. Security; Risk; ICT projects; Debriefs; Control and Command; Emergency Responses
Other documents
e.g. requirements for BCM included in procurement processes; Position descriptions
Other systems
e.g. Police Instructions; Lessons Learnt and Recommendations databases; Audits; Business planning
Core documentation implementing BCM Policy
Disaster Recovery Policy
Disaster Recovery Plan
Police National BC Plan
Delegations framework & documentation
BCM programme
District/Group/Function/Team BC Plans
Agreements with partners and suppliers
e.g. MOUs, Service Level Agreements
Forms, tools, templates, and systems for implementing plans and managing BC risk
Activities
Activities that help us understand and manage risks and continuously improve our BCM
BIAs and other risk assessments
Tests and exercises
Police and multi-agency
Other risk management activities

The 4 Rs and BCM

BCM is about managing risk, and Police's approach to BCM, as with all other risks we help to manage, aligns with the Government's wider 4R model - which emphasises risk Reduction, Readiness, Response, and Recovery. See sections below for how the 4Rs apply to managing disruption-related risk:

- **"Reduction and Readiness"** - how we prepare for and reduce the likelihood or consequences of disruptions; and
- **"Response and Recovery"** - how we respond to a disruption of our Essential Services and recover to BAU.



REDUCTION

READINESS

RESPONSE

RECOVERY

Disruption

Understanding our context

Identify and assess risks

Act to manage risks

Test and review

Embed

- BCM policy and programme
- Risk identification and analysis (e.g. Business Impact Analysis; BAU risk management)
- Investment in capability
- Contingency planning e.g. Business Continuity Plans, Disaster Recovery Plans, Service Level Agreements, other agreements and arrangements with internal and external partners
- Training and testing
- Lessons learnt, debriefs, monitoring
- Improving

Assess impact on Police ability to deliver Essential Services

Determine whether and to what extent to activate BCM provisions

Respond to effects on ability to deliver Essential Services

Maintain or recover Essential Services

Recover to BAU

- Activating contingency planning
- Response activities
- Recovery activities
- Deactivating contingency planning

Engagement, Communication, Cooperation

Reduction and Readiness

Understand our context

To manage disruption-related risk effectively we must understand our internal and external context, including:

- What our Essential Services are, and how the work we do contributes to these;
- What and who we rely on to carry out our components of our Essential Services;
- How we are expected to manage risks across Police;
- How our partners manage risks; and
- Changes in our internal and external operating environment and how these may affect us.

Identify and assess risks and controls

Understanding our context helps us to identify and assess risks that may prevent us carrying out our Essential Services e.g.:

- Strengths and weaknesses in the way we operate;
- Gaps in existing contingency plans (e.g. Business Continuity Plans);
- Dependencies on third parties;
- Inherent vulnerabilities;
- Unknowns; and
- Known resilience issues.

This can be done as part of a Business Impact Analysis and/or other risk assessments.

Act to manage risks

Once we understand our risks we can decide how best to manage these, including through:

- **Business Continuity Plans (BCP)** and other contingency plans and arrangements to support these - please see Organisational Resilience for information on what should be in a BCP, how to develop plans, and examples;
- Building our capabilities and assets to reduce the likelihood or impact of failure or increase our ability to respond;
- Changing the way we work to avoid reliance on weak systems or processes; or
- Escalating risks we do not have the capacity or authority to manage ourselves.

Testing

We cannot be prepared for every potential disruptive scenario. Regular testing of BCPs and other contingencies helps us empower our people to respond to uncertainty and make consistent, risk-based decisions. Police will:

- develop and deliver a BCM exercise programme; and
- where possible align this programme with Police operational exercises and the Government-wide

National Exercise Programme.

Review

Risk management is an ongoing process that requires us to continually assess new information against our existing way of working. We ensure our BCM is as strong as possible through:

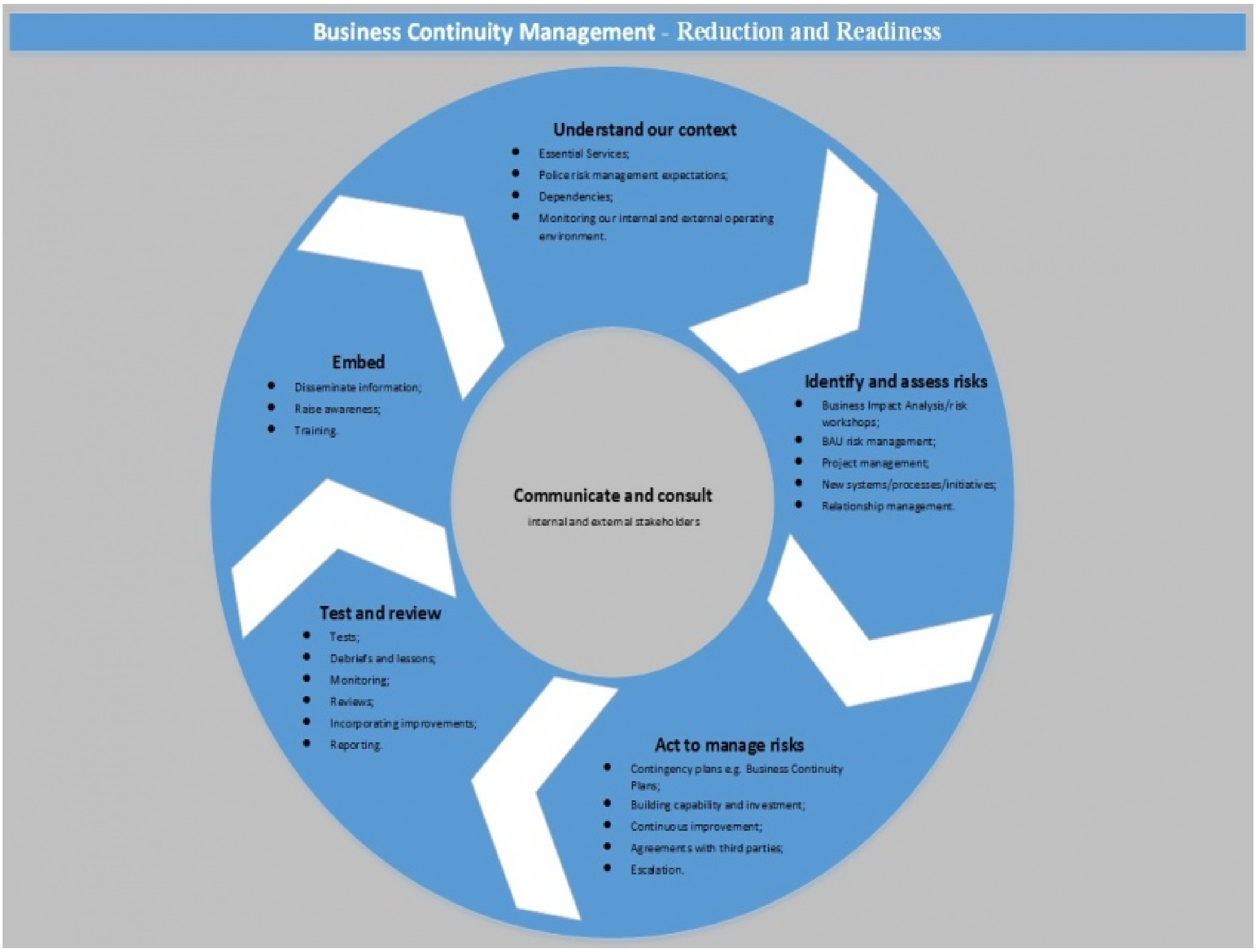
- debriefing relevant events;
- monitoring of legislative, regulatory, corporate, and operational changes; and
- all Police employees escalating risks and identifying lessons as part of BAU.

And ensuring these lessons, risks, and changes are reflected in our annual BCM programme, including:

- annual review of this policy and the BCM framework;
- annual reporting to the Executive on the status of BCM, including major risks; and
- annual and as-required reviews of National, District, and Service Group BCPs and supporting arrangements such as Service Level Agreements; and
- the Police BCM exercise programme and National Exercises where appropriate.

Embed

BCM must be incorporated into BAU risk management at NZ Police. All employees are expected to consider disruption-related risks and resilience as part of their roles, and to escalate risks and improvements as required.



Business Continuity Management - Reduction and Readiness

Understand our context

- Essential Services;
- Police risk management expectations;
- Dependencies;
- Monitoring our internal and external operating environment.

Identify and assess risks

- Business Impact Analysis/risk workshops;
- BAU risk management;
- Project management;
- New systems/processes/initiatives;
- Relationship management.

Act to manage risks

- Contingency plans e.g. Business Continuity Plans;
- Building capability and investment;
- Continuous improvement;
- Agreements with third parties;
- Escalation.

Test and review

- Tests;
- Debriefs and lessons;
- Monitoring;
- Reviews;
- Incorporating improvements;
- Reporting.

Embed

- Disseminate information;
- Raise awareness;
- Training.

Communicate and consult

internal and external stakeholders

Response and Recovery

Not all disruptions will activate BCM provisions. In a disruption we must first assess:

- the impact on our ability to deliver our Essential Services; and
- whether this impact can be managed as part of BAU.

Depending on the type of disruption and the context in which it occurs, the disruption to Essential Services may be acceptable and manageable as part of BAU, or it may require BCM provisions (e.g. a BCP, or a lesser arrangement such as a contractual agreement) to be activated.

BCM provisions can be activated and run at the Operational level (team or function), Organisational (Service Centre, Group, or District) level, or Strategic (Police National) level, but they can also be activated at one level and then be escalated or de-escalated as required by the circumstances and our ability to manage the disruption.

BCM provisions will focus first on:

- responding to the effects on our ability to deliver Essential Services; and
- recovering or maintaining these at an acceptable level.

BCM provisions are deactivated when our Essential Services are able to return to BAU.

Response

Police use the Coordinated Incident Management System (CIMS) to respond to incidents, including those which affect our own ability to operate. Sometimes, where a disruption affecting Police's Essential Services also requires an operational response by Police (or there are one or more unrelated Police operational responses required at the same time as a disruption to Police Essential Services), we will be required to run two or more CIMS responses at the same time. Where this happens, it may be appropriate for the Controller and Incident Management Team to be the same for the business continuity responses and operational responses, however wherever possible these should be different, to enable sufficient focus on each of the responses required. Appointment of Business continuity Controllers and activation of business continuity Incident Management Teams must be included in relevant BCPs.

Recovery

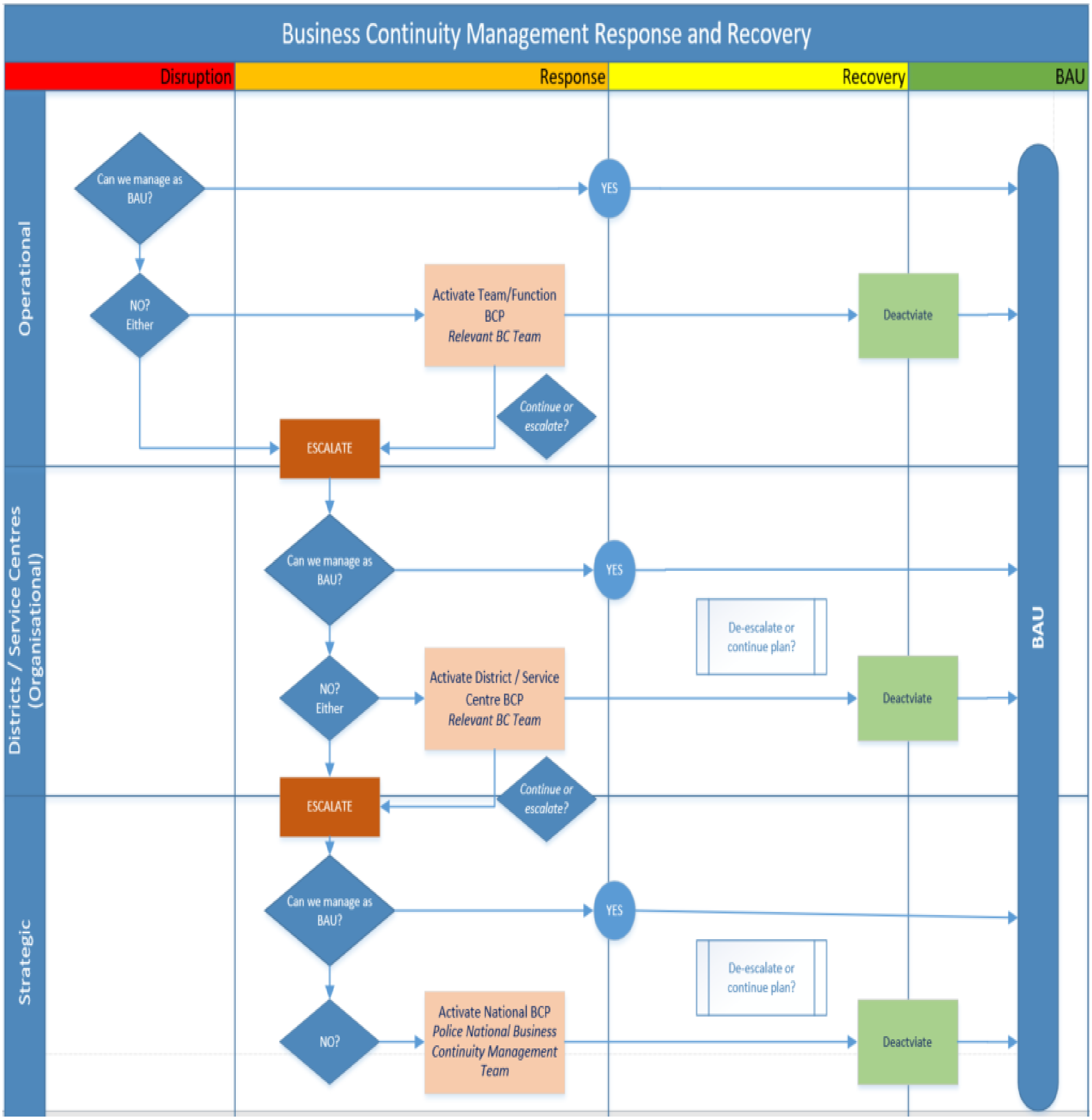
BCPs must include a decision point and criteria for Recovery to BAU. These will depend on the nature of the different components supporting our Essential Services, and the context of the disruption.

Recovery includes the coordinated efforts and processes to bring about the immediate, medium and long term holistic and strategic regeneration and enhancement of our business. The Recovery Phase should involve

- supporting the well-being of our people
- minimising the escalation of the consequences of the disruption
- reducing future exposure to risks - i.e. building resilience

- taking opportunities to regenerate and enhance our business in ways that will meet future needs.

Recovery should always include a debrief.



Stakeholder engagement, communication, cooperation

Police relies on all its stakeholders, be they within or outside of Police (including the private sector and NGOs), to maintain the effectiveness of our BCM. Proactive and ongoing communication and cooperation with all stakeholders is an essential part of our BCM.

Responsibilities

BCM responsibilities across NZ Police is aligned with our ‘Three Lines of Defence risk management approach’:

Responsibilities		Third line	Second line	First line
All Police personnel				**Identify and assess risks**; **Apply** this policy, BCPs as required, and other controls that help us manage risk; **Participate in tests and exercises**; and **Escalate** risks and control weaknesses.
District, Service Centre and work group Managers		**Ensure awareness** of dependencies and limitations between services reliant on each other	**Test** BCPs and other arrangements**;** **Develop, maintain, and implement** BCPs and other arrangements to manage risks**;** and **Discuss, act upon, and escalate** risks and control weaknesses as required	
Legal, HR, IT, Property, and other business groups as required		**Maintain and disseminate awareness** of NZ Police’s operational, organisational, legal, and regulatory context.		

Assurance Group	Business owner for resilience standards and settings	**Develop and maintain** the NZ Police BCM policy and relevant templates and tools to support work groups to manage disruption-related risk;
		Test Police's BCM capability; and
		Review, audit, and report on Police's BCM to the Executive.
			Develop and maintain the Police National BCP;
			Coordinate and oversee Police's overall BCM risks and dependencies;
			Develop and deliver an annual BCM programme; and
			Advise work groups on managing disruption- related risks.	

Deputy Commissioner Strategy & Service	Sponsor of BCM	**Promote** business continuity expectations throughout Police.	Act as SRO for National Business Continuity Plan.	
Executive Leadership Team	Owner of resilience risk	Provide **Governance** of Police's BCM; and Ensure **adequate resources** are available to allow our people to effectively manage disruption-related risk and build resilience.		

Related documents

This policy aligns with:

- Policing Act 2008
- Civil Defence Emergency Management (CDEM) Act 2002
- National Civil Defence Emergency Management Plan 2015
- National Disaster Resilience Strategy (G.7D2) April 2019
- NZ Police Risk Management Policy
- Police Instructions on Control and Command and Emergency Responses
- NZ Police Assurance Model
- ISO 22301:2012 Societal security - Business continuity management systems - Requirements
- Protective Security Requirements (GOV3) and NZISM
- Business Continuity Institute Good Practice Guidelines 2018
- Coordinated Incident Management System (CIMS) Third Edition