Te Tari Taiwhenua
Internal Affairs

Incident Management Plan

August 2021

Table of Contents

Introduction

This plan outlines the Department's incident management arrangements for a response to a significant event which has a serious impact on DIA staff, operations, services and reputation; or to a national emergency; or a national response/lead agency.

'Incident Management' refers to the coordination of a response to major events, either internal to the Department or during external emergencies, by providing strategic direction, decision making, liaison with other agencies, and prioritisation and/or acquisition of resources.

Through invoking the incident management arrangements, the Incident Controller and the Incident Management Team will take control of the Department's response to incidents.

An incident is a situation with a high level of uncertainty that disrupts the core activities and/or credibility of an organisation and requires urgent action. These might include mass illness, loss of a DIA site or a significant privacy breach.

The Department follows a people first approach to response. The safety and wellbeing of our staff, contractors and customers is paramount and is to remain the centre of any response.

The objectives of the Incident Management Plan are to:

- Ensure the support of prioritising essential resources across business-critical functions and services
- Define the structure, roles and responsibilities of Incident management using the Coordinated Incident Management System (CIMS) framework.
- Document the process from initial activation through to the return to business as usual, including quick and effective response to, management of and recovery from the incident
- Provide for the safety and wellbeing of staff, contractors and customers
- Protect the Department's business and assets
- Minimise financial and reputation impacts on the Department
- Make sure appropriate communication strategies are in place both internally and for external stakeholders

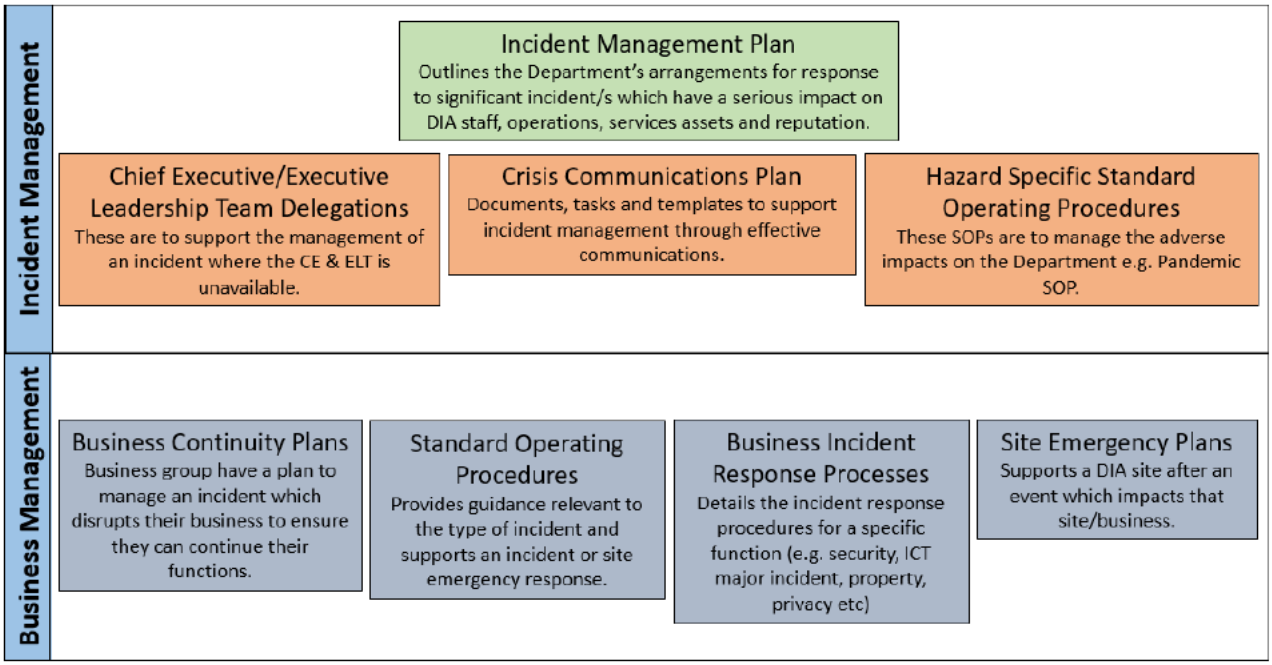
The nature and extent of an incident cannot be foreseen therefore this plan relies on a series of points for consideration, guidelines and checklists to determine the response to the incident.

This plan is owned and maintained by the Principal Advisor Resilience and Recovery and will be regularly updated and reviewed. It will be tested annually, with learning incorporated and reviewed in line with the criteria in the Business Continuity Management Policy or following significant business change.

Resources supporting this plan are available in the Incident Management cohesion library.

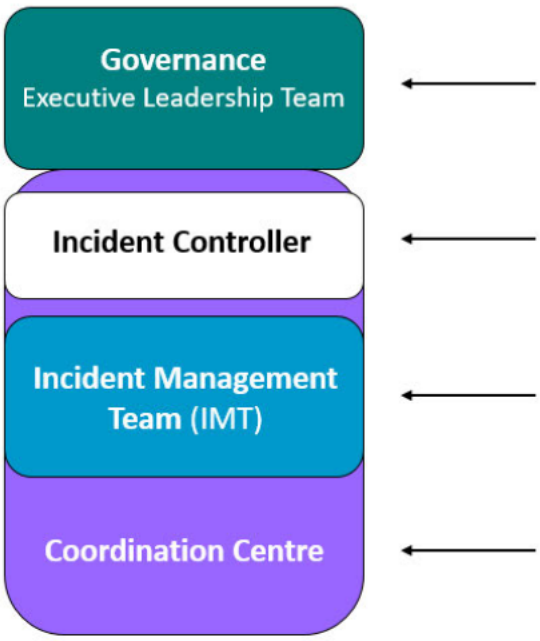
Business Continuity Management Toolkit

In an emergency or business disruption, this plan can be activated in conjunction with the following plans from within the toolkit:



Incident Management Team Structure

The overall incident management team structure outlined below describes responsibilities for the main components.



The Governance level, made up of the **Executive Leadership Team**, leads the strategic response to the incident e.g liaison with Ministers and strategic communications..

The **Incident Controller** (a member of ELT, or delegate) commands and controls the Department's response and leads the incident management team.

The **Incident Management Team** manage the tactical and operational response to the incident.

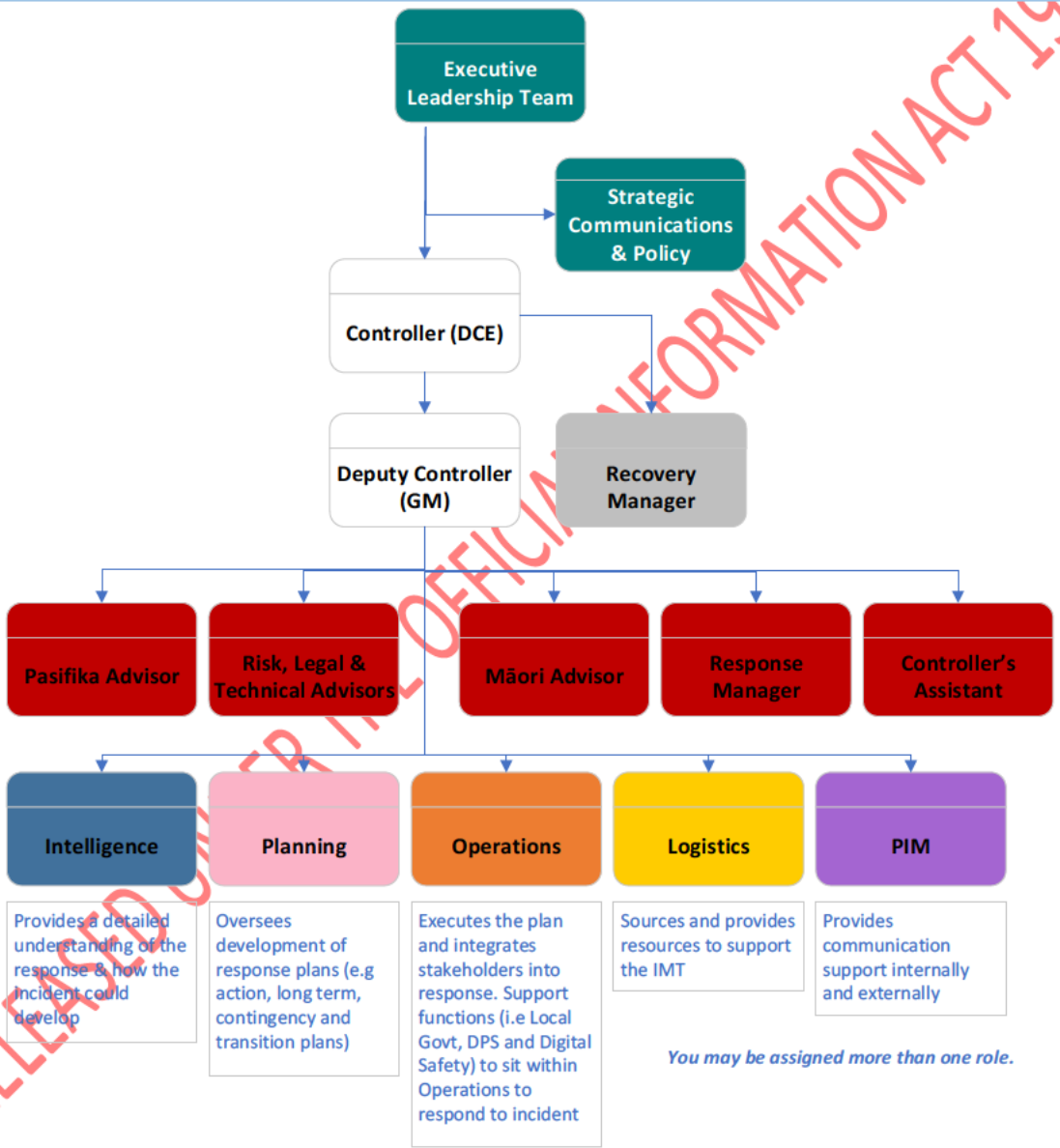
The **Coordination Centre** is the primary location for the Incident Management Team. This is a central hub for information collection and collation.

Coordinated Incident Management Systems (CIMS) Structure

The Department uses CIMS framework to manage an incident. CIMS is designed to be a modular framework scalable specifically for each organisation.
The full CIMS structure can be found in the CIMS Manual 3rd Edition.

The structure below gives a high-level view of a full incident response and has been designed to specifically align with the Departments structure.

Note: Details of each function responsibilities are outlined below in each of the role cards.



Governance: Provides strategic direction and quality decision making to support the response
Strategic Comms/Policy: Provides communications and advice to Ministers
Controller: Directs the response to an incident
Deputy Controller Assists the Controller in the management of tasks and resolving internal conflicts
Response Manager: Assists the Controller in the operation of the Coordination Centre

Supporting subfunctions

The supporting subfunctions are listed below. These can be stood up depending on what resources are needed for the response.

Intelligence	Planning	Operations	Logistics	PIM
Collections	**Action planning**	**Action plan execution** *Tasking the business if required working with tech advisor*	**Wellbeing** *Liaison for HR* *Provides health, safety and wellbeing support for IMT*	**Media liaison**
Analysis	**Long-term planning**	**Welfare** *To meet National Welfare Coordination Group requirements*	**Finance** *Liaison for the Finance team and provides financial advice*	**Online media management**
Dissemination	**Contingency planning**	**Officials coordinator** *Briefing and tracking DIA staff that are attending an officials meeting or watch groups*	**IT** *Liaison for TSS, manages response for major IT incidents and provides tech support to the IMT*	**Stakeholder management**
		Branch Coordinators *Managing branch reps and information flow including offshore offices*	**Facilities/Property** *Liaison for the Property team*	**Information and warnings**
		Emergency Site Managers Coordinator *Managing ESMs and information flow*	**Administration** *Manages information, appointments, catering and rostering for IMT, ensuring the IMT has equipment it needs*	**Internal communications**

Scaling Responses

Responses should be scaled to manage the type or size of incident.

The Controller assigns CIMS roles to individuals or teams on a scale that reflects the resources required to respond to the incident. A response can be scaled up and down multiple times depending on the nature of the incident and response required.

A decision to scale the response structure needs to be based on the:

- Safety of the response personnel, DIA staff and contractors, the public and property
- Size and complexity of the incident and response required
- Span of control

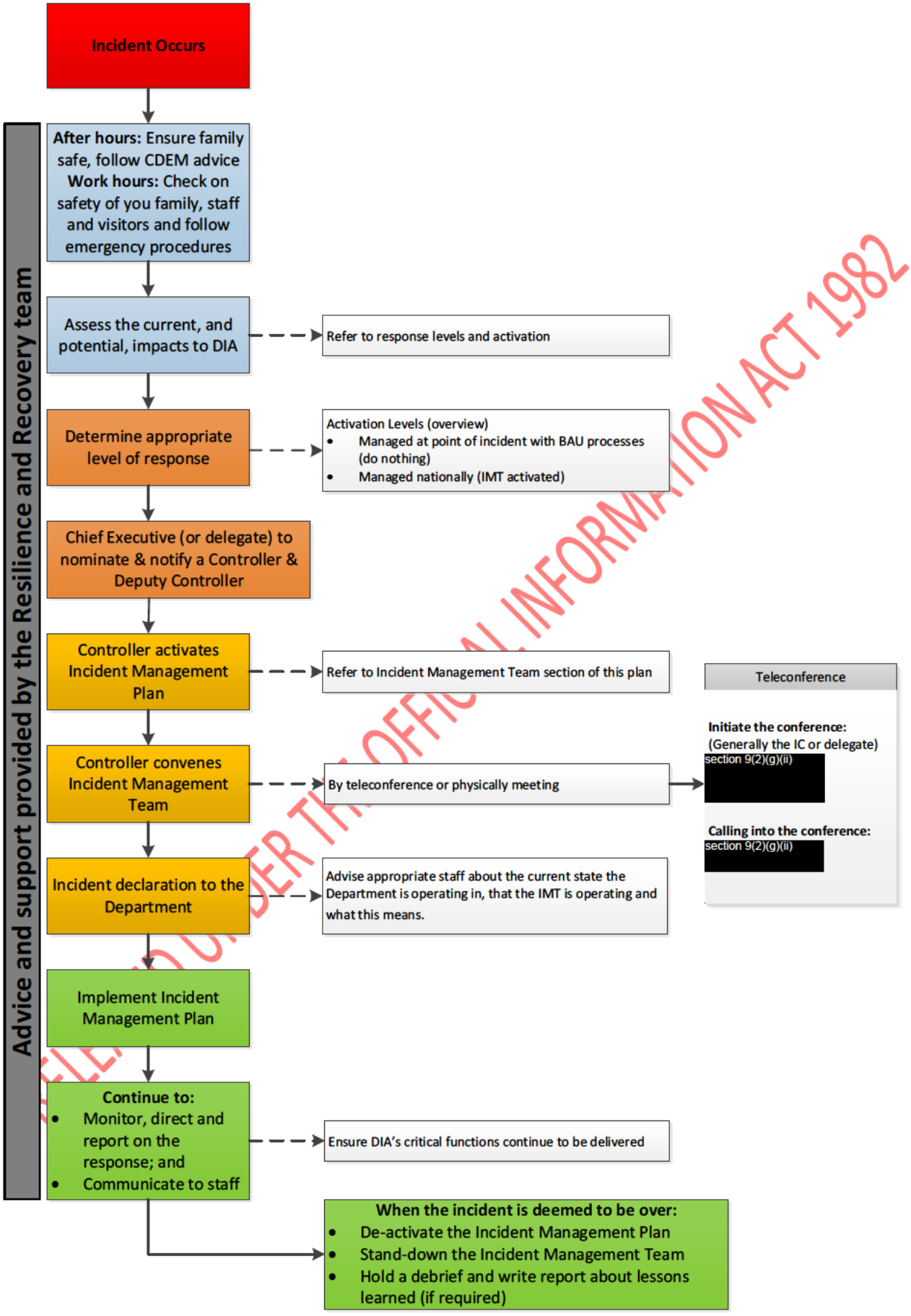
Activation

If there is any uncertainty of what action to take, escalate the situation to the Chief Executive, or delegate, to assess the need for an incident declaration or consult with the Principal Advisor Resilience and Recovery.

ACTION: Use the following checklist to activate the Incident Management arrangements.

	Action	Responsibility
☐	Refer to response levels and activation table and escalate up to your DCE (through BAU line management).	All staff
☐	Assess the current, and potential, impacts to DIA: - Staff - Services & Systems - Operations - Taonga - Assets - Reputation	Deputy Chief Executive *with support from the Principal Advisor, Resilience and Recovery & CE's Office*
☐	Determine the appropriate level of response by using the response levels and activation table below. Include the CE's office in this discussion.	Deputy Chief Executive *with support from the Principal Advisor, Resilience and Recovery & CE's Office*
☐	Make a recommendation to the CE to activate the Incident Management arrangements ***Note:*** *In the event the CE cannot make the decision to active two or more members of the ELT who can be contacted can agree the situation warrants an incident response. If no other acting delegation is in place the Delegated Authority comes into effect.*	Deputy Chief Executive *with support from the Principal Advisor, Resilience and Recovery*
☐	Nominate and notify a Controller and a Deputy Controller	Chief Executive (or delegate)
☐	Determine time and location for initial meeting (this should be within 30 minutes of a declaration, see action below)	Controller
☐	Convene the Incident Management Team for the initial meeting (see teleconference numbers in setting up the coordination centre)	Controller
☐	**Only action in full activation:** Declaration to the Department (or appropriate audience) with a direct email to ELT (and SLC if appropriate). **ACTION:** If a declaration is made that this decision (and time made) is subsequently recorded in a Decision Log.	Controller

Overview of activation process



Decision making when activating

An incident is a situation with a high level of uncertainty that disrupts the core activities and/or credibility of an organisation and requires urgent action.

Control is assumed by the Incident Management Team:

- When instructed by the Chief Executive or delegate; or
- When two or more members of the Executive Leadership Team who can be contacted agree that the situation warrants a coordinated Incident management response.

In the event that the Chief Executive is impacted by the incident and is unable to carry out their role and no other acting delegation is in place the Delegated Authority comes into effect.

There are three choices in any situation:

1. Do nothing (or manage within existing response structures)
2. Monitor the situation and be ready to respond in case of escalating risks
3. Activate the Incident Management Team

These key impacts are to support decision making when activating an incident response. If an event fits more than one of the impacts below, then escalation and activation should be followed.

Remember: It is better to activate, and then stand-down, than to wait until the situation naturally escalates and risk exposure for not taking action.

Why should a response should be activated?

- Response or resource coordination is required
- People may be/ are at risk
- Other agencies request support
- Uncertain conditions
- Risk to property/ environment
- Declaration of state of emergency is in place
- Public expectation
- Contingency for a planned event

Note: If an incident declaration will **not** be made and the incident is deemed to be manageable through BAU response processes, determine which characteristics of the incident must change to escalate. Agree these criteria and place the Incident Management Team on stand-by to monitor the situation. This will ensure that a declaration can be made swiftly should the incident escalate at a later point.

Response levels and activation

RESPONSE LEVEL			Harm to people	Disruption to Systems	Disruption to Operations	Disruption to Services	Information	Asset Damage/ Site Disruption	Damage to reputation
Level 1 BAU Processes	Level 2 IMT Standby & Monitor	Level 3 IMT Activation	Large area affected (City/Province) Single or multiple injuries or fatalities Mass illness requiring additional resources	Major loss of IT critical systems	Long term loss of operations	Long term loss of services	Significant loss of information or privacy breach with significant risk of harm	Significant damage to structures, facilities or equipment which seriously affects daily operations Property and assets at risk Loss of site for multiple days	Major loss of trust in the Department from the public and Ministers
			People at risk	Loss of IT critical systems that have a wider impact on Department	Loss of operations for 1 week and wider impact on Department	Loss of services for 1 week and wider impact on Department	Loss of information or privacy breach that requires more resource than BAU processes with a medium risk of harm	Accident or damage to facilities or equipment which could affect daily operations Disruption affecting a large site for a day	Loss of trust in the Department from the public and Ministers
			Illness or injuries of a minor nature Significant near-miss	Loss to systems and BCP plans activated e.g. Network outage	Loss of operations and BCP plans activated	Loss of services and BCP plans activated	Information loss or privacy breach with low risk of harm	Minor disruption to departmental operations Minor damage to facilities or equipment able to be dealt with by Property Group	Local or regional concerns with potential to escalate. National or international media interest / activity

Level 1 – Business as usual processes to manage the situation

Current processes to be followed to report and manage the situation, monitoring stage. E.g. health, safety and wellbeing, privacy, property and BCP processes.

Level 2 – Monitor and standby an Incident Management Team

The escalation process followed to a monitor or standby situation - fully activate if needed.

Level 3- Activation of the Incident Management Team

An Incident Management Team to be activated and all roles to filled (at the discretion of the Incident Controller).

Response

Coordination Centre Activation

ACTION: Follow the below steps to set up the Coordination Centre

Incident Occurs		
☐	The Chief Executive or Deputy Chief Executive makes the decision to establish the Incident Coordination Centre and nominates a location and nominates a Controller. Convene for a physical meeting or establish the Coordination Centre only if it is safe to enter the prescribed location.	CE/DCE Response Manager Lead Controller
☐	The Response Manager will clear room bookings and oversee the set up on the rooms (if held in Wellington). If Incident is being managed outside of Wellington the Response Manager will work with Property team to set up room/s at location provided by the CE (or DCE) and Lead Controller.	Response Manager
☐	The Response Manager will oversee the delivery of setting up the Coordination Centre with Technology Services and Solutions (TSS) and Property.	Response Manager
☐	The Property team will ensure the room/s are secure, and if required, restrict access (as appropriate). They will also provide ongoing support to the Coordination Centre for the duration of the response.	Property Team
☐	TSS will ensure the room/s are equipped with a working landline telephone, including VC and teleconference facilities. TSS will also ensure the Coordination Centre has sufficient devices that connect to the network/internet and has access to a printer and a television.	TSS

Coordination Centre locations (or Conference Call)

Location	Coordination Centre Room/s	Supplies located
Wellington (Primary)	Set up in rooms section 9(2)(g)(ii) [redacted], 45 Pipitea Street Rooms section 9(2)(g)(ii) [redacted] can be used if needed. Priority to all section 9(2)(g)(ii) [redacted] meeting rooms is given to the IMT (Bookable through Resilience and Recovery or the Property Team)	Level 2, South End, Desk 2.135, I&S Rohe

Wellington (Alternate)	Waterloo Quay Office Priority to all the largest meeting rooms is given to the IMT (Bookable	TBC
Auckland (Wellington alternate)	Carlaw Park Office Priority to all the largest meeting rooms is given to the IMT	

The Lead Controller (or delegate) will notify when a conference is being held.

1. Call one of the following:
   New Zealand: section 9(2)(g)(ii) [redacted]
   Australia: section 9(2)(g)(ii) [redacted]
   USA: section 9(2)(g)(ii) [redacted]
   Canada: section 9(2)(g)(ii) [redacted]
   UK: section 9(2)(g)(ii) [redacted]
   Local: section 9(2)(g)(ii) [redacted]

2. **Person setting up conference**
   Conf ID – section 9(2)(g)(ii) [redacted]
   Web/Chairperson Password – section 9(2)(g)(ii) [redacted]

3. **People calling into conference**
   Conf ID - section 9(2)(g)(ii) [redacted]

Deactivation of response

When the decision has been made by the Lead Controller to deactivate the IMT ensure the following steps are taken:

- Ensure all documents and emails relating to the incident are saved (securely if required) in the Cohesion incident folder
- Ensure any services managed by the incident are transitioned back to the Business
- Close the IMT rooms, open room bookings back up to the business and reset rooms
- Hold a debrief and lessons learned workshop and produce a report. *See SOP on how to hold a debrief session.*