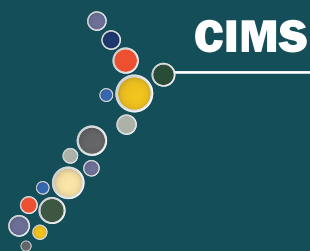




New Zealand Government

Coordinated Incident Management System (CIMS)

Third Edition



Coordinated Incident Management System (CIMS)

Third edition

August 2019

ISBN 978-0-478-43525-2

Published by the Officials' Committee for Domestic and External Security Coordination

Department of the Prime Minister and Cabinet, PO Box 55, Wellington, New Zealand.

This edition replaces the second edition published in 2014 by the Officials' Committee for Domestic and External Security Coordination, Department of the Prime Minister and Cabinet.

© New Zealand Government

**Urupare ki ngā
hiahia hāpori**
Responsive to
community needs

Ngāwaritanga
Flexibility

Mahi ngātahi
Unity of effort

Foreword

New Zealand's Coordinated Incident Management System (CIMS) establishes a framework of consistent principles, structures, functions, processes and terminology for response and the transition to recovery. First introduced in 1998, CIMS has continued to develop in terms of both its focus and uptake among agencies. This 3rd edition represents the next step in a development approach that keeps pace with the times by accommodating continuous improvement, changing environments, and new expectations, while at the same time recognising the importance of preserving a well-established and proven foundation.



The 3rd edition of CIMS builds on the 2nd edition by incorporating new experience since 2014, as well as the Government's decisions announced in August 2018 relating to the Ministerial review into *Delivering better responses to natural disasters and other emergencies*.

Enhancements introduced by this edition include:

- Strengthening the core foundations that CIMS is based upon, including its strong community focus.
- Highlighting the importance of the inclusion of iwi/Māori in response and recovery.
- Introducing a holistic consequence assessment approach to ensure all consequences (including those not immediately evident) are considered in any response and recovery.
- Expanding on the CIMS supporting protocols and systems by the introduction of an 'Incident Classification' system, expanding on the description of 'Governance', and introducing a 'Strategic Communications' role.
- Including a section on the application of CIMS, to demonstrate how CIMS can be applied across the range of response levels - from Incident through to National level.
- More fully describing the CIMS Functions, including Recovery (in response), and expanding on previous appendices.

The Government signalled its intent to require all relevant agencies in the emergency response system to use the latest edition of CIMS. I therefore acknowledge and thank the increased number of agencies and organisations that took part in the development and endorsement of the latest edition.

With the publication of the 2nd edition, it was decided that CIMS should be reviewed every five years. To ensure it remains current with legislation, another review may be required pending any amendments to the Civil Defence Emergency Management Act that might take place before the next review cycle.

A handwritten signature in blue ink, reading "Brook Barrington".

Brook Barrington
Chair, ODESC

Endorsements

This version of CIMS is the result of a collaborative effort by New Zealand emergency management agencies and is endorsed by the Officials' Committee for Domestic and External Security Coordination (ODESC).

Acknowledgements

The development of this version of CIMS was overseen by the CIMS Steering Group, chaired by the Ministry of Civil Defence & Emergency Management. Agencies represented on the CIMS Steering Group at the time of publication were:

Ambulance New Zealand (St John; Wellington Free Ambulance)

Civil Defence Emergency Management Groups (16), collectively represented

Department of Conservation

Department of Corrections

Department of the Prime Minister and Cabinet

Fire and Emergency New Zealand

Maritime New Zealand

Ministry for Primary Industries

Ministry of Business, Innovation and Employment

Ministry of Civil Defence & Emergency Management

Ministry of Foreign Affairs and Trade

Ministry of Health

Ministry of Social Development

New Zealand Customs Service

New Zealand Defence Force

New Zealand Police

Oranga Tamariki—Ministry for Children

Contents

Section 1 Introduction.....	5
1.1 Purpose — A common and modular framework	5
Section 2 CIMS Foundations	8
2.1 CIMS in the context of the 4Rs of emergency management	8
2.2 CIMS principles and characteristics	8
2.3 Lead agencies and support agencies	11
2.4 Engaging iwi/Māori.....	12
2.5 Doctrine, training and development, and incidents.....	13
2.6 Command, control and coordination.....	14
2.7 Unified Control	16
2.8 Holistic and integrated response and recovery	17
2.9 The incident management structure.....	18
Section 3 Supporting Protocols and Systems.....	23
3.1 Response levels.....	23
3.2 Incident classifications	27
3.3 Governance.....	31
Section 4 The CIMS Functions	35
4.1 Introduction	35
4.2 Function colours and responsibilities (summary).....	36
4.3 A networked hierarchy	36
4.4 Control	37
4.5 Safety.....	42
4.6 Intelligence	43
4.7 Planning	46
4.8 Operations	49
4.9 Logistics	53
4.10 Public Information Management	57
4.11 Welfare.....	62
4.12 Recovery (in Response)	67
Section 5 Application of CIMS	69
5.1 Incident level response	69
Example: Incident level response involving a single organisation (vehicle accident).....	70
Example: Incident level response involving a single organisation (business disruption).....	71
Example: Incident level response involving multiple organisations.....	74
5.2 Local or regional level response	76
Example: Local/regional level response.....	77

5.3 National level response.....	80
Example: National level response.....	80
Appendix A The full CIMS Hierarchy.....	84
Appendix B The Intelligence Cycle	85
Appendix C The Planning Process.....	89
Appendix D The National Security System.....	93
Appendix E Handovers	95
Appendix F Demobilisation	96
Appendix G Recommended Template Content	97
G.1 Status Report	98
G.2 Situation Report	99
G.3 Action Plan	100
G.4 Request for Assistance / Resource Request	102
G.5 Response to Recovery Transition Report.....	104
Appendix H Glossary and Acronyms.....	106

Section 1 Introduction

Coordinated Incident Management System (CIMS) was first developed in 1998 to provide emergency management agencies with a framework to coordinate and cooperate effectively in a response. It is based on similar systems used in North America and Australia (NIMS and AIIMS respectively).

This third edition of CIMS replaces the previous versions. It describes how New Zealand agencies and organisations use the CIMS framework to manage incident responses of any scale, the respective functions of the response structure, the levels of response and the relationships between them, and how a response can be structured at each level. CIMS is the primary reference for incident management in New Zealand.

An incident is an event that needs a response from one or more agencies or organisations. Incidents range from small to large — simple to complex — and can be managed at one or multiple levels. While CIMS uses the term “incident” for any event in this range, incidents can be “emergencies” under the Civil Defence Emergency Management Act 2002.

The CIMS framework has been developed by a Steering Group that consists of representatives from eighteen CIMS stakeholder organisations, and it is endorsed by the Officials’ Committee for Domestic and External Security Coordination (ODESC). CIMS is reviewed every five years, or more frequently if necessary.

1.1 Purpose — A common and modular framework

The purpose of CIMS is to enable personnel to respond effectively to incidents through appropriate coordination across functions and organisations — both vertically and horizontally — by:

- establishing common structures, functions and terminology in a framework that is flexible, modular, and scalable so that the framework can be tailored to specific circumstances; and
- providing organisations with a framework that they can use to develop their own CIMS-aligned processes and procedures that support both own-organisation responses and multi-organisation interoperability, giving due consideration to each organisation’s unique responsibilities, resources and legislative authority.

1.1.1 Mandates

New Zealand’s emergency management arrangements are coordinated by the Civil Defence Emergency Management (CDEM) Act 2002 and associated National Civil Defence Emergency Management Plan Order 2015. The CDEM Act operates alongside a range of other legislation to give agencies the authority to respond and the means to work together.

Emergency-related legislation give response personnel access to special powers such as powers of compulsion, entry, direction, exclusion and removal. Most powers of the CDEM Act require a state of emergency to be declared before they can be used, while other statutes allow for the use of emergency powers by appropriately appointed people. In most responses, incident management occurs without these powers being required or used.

When an incident is an emergency under the CDEM Act, the responsible Controllers (Local Controller, CDEM Group Controller, and/or National Controller) are statutory roles.

Various acts have provisions for responding to incidents; the following list is not exhaustive.

- Biosecurity Act 1993
- Building Act 2004
- Civil Aviation Act 1990
- Civil Defence Emergency Management Act 2002
- Conservation Act 1987
- Corrections Act 2004
- Crimes Act 1961
- Defence Act 1990
- Epidemic Preparedness Act 2006
- Fire and Emergency New Zealand Act 2017
- Fisheries Act 1996
- Government Rounding Powers Act 1989
- Hazardous Substances and New Organisms Act 1996
- Health Act 1956
- Heritage New Zealand Pouhere Taonga Act 2014
- Immigration Act 2009
- Intelligence and Security Act 2017
- International Terrorism (Emergency Powers) Act 1987
- Local Government Act 2002
- Marine Reserves Act 1981
- Maritime Security Act 2004
- Maritime Transport Act 1994
- National Civil Defence Emergency Management Plan Order 2015
- National Parks Act 1980
- Policing Act 2008
- Railways Act 2005
- Reserves Act 1977
- Resource Management Act 1991
- Search and Surveillance Act 2012
- Terrorism Suppression Act 2002
- Wildlife Act 1953

1.1.2 When to use CIMS

The National Civil Defence Emergency Management Plan Order 2015 expects emergency services to use the CIMS framework to guide the coordination of each emergency service's operations, and for those fulfilling key roles at the national, CDEM Group, and local levels during response to be trained and practised in its use.

CIMS applies to all hazards and risks and should be used to provide effective management of a wide range of incidents, including:

- biosecurity incursion incident;
- environmental damage incident;
- fire incident;
- food safety incident;
- hazardous substance incident;
- marine mammal stranding;
- mass maritime arrivals;
- missing person incident (search and rescue);
- natural hazard incident;
- business continuity disruption;
- communicable disease outbreak and pandemic;
- public disorder incident;
- public health and medical emergency;
- transportation accident;
- crime and terrorism; and
- technological failure.

CIMS can also be used for the pre-emptive management of potential incident-inducing situations such as planned events (e.g. celebrations, parades, concerts, official visits).

1.1.3 Audience

The intended audiences for CIMS are:

- agency and organisation planners and developers of standard operating procedures (SOPs);
- trainers and capability development personnel (internal and external);
- readiness, response and recovery personnel; and
- plan and SOP owners (Chief Executives / Managers).

Section 2 CIMS Foundations

This section describes the foundations of CIMS, including principles and characteristics, lead agencies and support agencies and the inclusion of and engagement with iwi/Māori. It also covers the relationship between coordination, command and control.

2.1 CIMS in the context of the 4Rs of emergency management

The primary goal of incident and emergency management in New Zealand is to protect people and property from all hazards and risks, both natural and man-made. While emergency management in New Zealand operates across [risk] reduction, readiness, response and recovery, CIMS primarily focuses on response to incidents and emergencies, but it must also be factored into readiness and recovery.

2.2 CIMS principles and characteristics

2.2.1 CIMS principles

The principles of CIMS are the fundamental tenets on which incident management is based. All responses should apply the following principles:

Responsive to community needs / Urupare ki ngā hiahia hapori

Any response should mitigate and manage the consequences of an incident on the affected individuals, families/whānau and communities, including animals. Response personnel must recognise an individual's rights, treat individuals with fairness and dignity and ensure the needs of affected people and animals are identified and met throughout the response and into recovery. Communities must be able to actively participate in a response rather than wait passively for assistance. To allow this to occur, response personnel need to effectively communicate with communities to understand, integrate and/or align the community response.

Flexibility / Ngāwaritanga

Flexibility allows CIMS to be modular and scalable, and therefore applicable to incidents that vary widely in terms of scale, hazard or situational characteristics. CIMS is scalable and adaptable to any situation.

Unity of effort / Mahi ngātahi

Unity of effort ensures common objectives are met by coordinating response and recovery activities among the functions and organisations involved. Unity of effort allows organisations with specific mandates to support each other while maintaining their own authorities.

2.2.2 CIMS characteristics

The following characteristics are the features and qualities that define CIMS:

Common structures, roles and responsibilities

Common structures, roles and responsibilities make it possible for organisations to work effectively alongside each other and for personnel to interchange roles. They facilitate information flow and understanding of structures and relationships.

Common terminology

Common terminology for functions, processes and facilities prevents confusion, improves communications between organisations and supports more efficient and effective responses. See Section 4 and Appendix H for more information on the CIMS functions and definitions of the terms commonly used in CIMS.

Interoperability

Interoperability is the ability for systems, processes, personnel and equipment to effectively operate together. It is the intended result of the common approach established by CIMS and its supporting arrangements (e.g. doctrine, training and exercise programmes). Ideally, staff will be familiar with the environment they will work in and the personnel they will work with.

Management by objectives

Response objectives are established by the Controller, assisted by the Incident Management Team (IMT), who consults with Governance on desired outcomes (see Sections 4.4, 2.9.2 and 3.3 respectively). These objectives are then communicated to everyone involved so that they know and understand the direction being taken and work towards the same end so that unity of effort is achieved. Objectives are reviewed regularly against the situation and against progress towards resolving the incident.

The response effort aims to manage the consequences of hazards, support the affected communities and establish the basis for recovery. Examples of common response objectives are listed below (priorities will vary depending on the incident):

- Preserve life (including ensure responder safety)
- Provide safety and security measures for people and property
- Identify and attend to community needs
- Provide notifications and public messaging
- Prevent escalation of the incident or emergency
- Develop situational awareness
- Maintain law and order
- Provide for the wellbeing of people
- Provide essential services
- Preserve government
- Protect assets, including buildings and their contents
- Protect natural and physical resources
- Provide animal relief support services
- Preserve economic and social activity
- Put in place effective arrangements for the transition to recovery
- Manage the transition to recovery

Consolidated planning

Consolidated planning in response and transition to recovery is the process that establishes the basis for the overall response. The planning process requires input from all the functions and organisations involved.

Consolidated planning supports:

- the development of effective Action Plans, Long-term Plans, Contingency Plans and Recovery Plans;
- organisations involved to have a cohesive and efficient response;
- situational awareness between agencies and organisations;
- coordinated activities to achieve common response objectives; and
- reduced risk, duplication of effort and conflicting actions.

Integrated information management and communications

Integrated information management and communications between functions and organisations support

situational awareness through the development and evolution of a common operating picture. This is essential for effective planning and response coordination, supporting successful delivery of objectives and transitioning to recovery. A common operating picture is dependent on common information protocols, processes and procedures, and, as far as possible, interoperable information management systems and consistent data standards. Integrated communications supports consistent messaging to all stakeholders and communities.

Coordination of resources

Resource coordination involves the consolidation and control of resources. It maximises resource use across and between response elements, provides accountability and improves situational awareness. It requires an awareness of available capabilities and resources so that procurement and use of resources can be managed efficiently and appropriately. The Controller directs resource coordination with the support of the Incident Management Team (IMT).

Designated response facilities and locations

Designated response facilities and locations, with clearly defined functions or purposes, are essential in establishing the response structure and, when applicable, the hierarchy and relationships between response levels.

Manageable span of control

Span of control is the number of individuals or response elements one manager or Controller can manage effectively. The optimum span of control is between three and seven individuals or response elements, although this may be increased based on the:

- experience of the manager or Controller;
- administration and technical support available to the manager or Controller;
- individuals' or response elements' competence or experience;
- familiarity, stability and complexity of the incident, and the level of responsibilities and delegations; and
- availability of appropriate plans, processes and procedures.

2.3 Lead agencies and support agencies

2.3.1 Lead agency

A lead agency is the agency mandated through legislation or expertise for managing a particular hazard that results in an incident¹. While some hazards or risks are managed by the lead agency alone, many require the support of other organisations.

¹ The National Civil Defence Emergency Management Plan Order 2015 describes the lead agency role at the national level. It also lists examples of lead agencies at the national and regional levels in Appendix 1 of the Plan. A complementary resource is the National Security System handbook. The descriptions of lead agency and support agency are subject to legislative change.

The lead agency's role is to:

- monitor and assess the situation;
- plan for and coordinate the response;
- report to Governance; and
- coordinate the dissemination of public information.

A lead agency should develop and maintain capability and capacity to ensure it is able to perform its role, and may draw on the advice and expertise of others in doing so.

Where activities are required at national, regional and/or local levels, a devolved accountability model is used. For example, the Ministry of Health is the strategic lead for infectious human disease nationally, while District Health Boards (DHBs) are the regional leads. Maritime New Zealand is the national lead for a marine oil spill, while the regional lead is the affected Regional Council.

In response, the lead agency establishes control to coordinate the overall response to the incident; however this does not limit, is not a substitution for and does not affect the functions, duties or powers that other agencies may have in support of the management of an incident.

The lead agency may change as the incident evolves and the required authority or expertise changes. The lead agency may also change between [risk] reduction, readiness, response and recovery.

2.3.2 Support agency

Organisations supporting the lead agency are known as support agencies. Support agencies are required to develop and maintain capability and capacity to ensure that they are able to perform their role. Support agencies may have statutory responsibilities and/or specific objectives of their own, which they may need to pursue in addition to, or as part of, the support that they provide to the lead agency.

Integration of support agencies into the response is a responsibility of the lead agency Controller. While the lead agency Controller may task and coordinate support agencies' resources and actions, they must recognise and accommodate support agencies' statutory responsibilities and/or specific objectives. Sometimes a support agency might support the lead agency by repurposing an existing capability.

The type of incident, response requirements, and consequences being managed determine which support agencies are involved, and these agencies may change as the response changes. Besides government agencies, support agencies may also include entities such as Civil Defence Emergency Management (CDEM) Groups, iwi/Māori, communities/volunteers, private sector organisations such as lifeline utilities, and non-government organisations.

Support agencies must assist the lead agency in the development of Action Plans.

2.4 Engaging iwi/Māori

As Treaty partners to the Crown and members of the wider community, it is essential that whānau, hapū and iwi are involved in response and recovery (as appropriate to the scale of the incident). Iwi/Māori involvement occurs within a framework of traditional knowledge, values and practices, and is often indispensable to effective response and recovery.

Incident management benefits by engaging iwi/Māori in response and recovery through:

- strong networks;
- access to community focal points (i.e. marae);
- ability to mobilise resources appropriately;
- understanding of tikanga (marae protocol, burial practices);
- able to identify and assess iwi needs;
- understanding of the local landscape, including history and sacred sites; and
- an ability to link with other cultures.

It is important to note that while many iwi/Māori may share a similar worldview, there is still a need to recognise different dynamics within and between iwi, hapū, and marae, and to engage with each individually if not collectively represented. There is also a need to recognise that different iwi, hapū, and marae have different resource and asset bases and their ability to respond is dependent on this.

Engaging iwi/Māori in response and recovery should be based on:

- a partnership that is built on mutual respect and shared values, and that follows the Treaty Principles of Participation, Protection and Partnership;
- recognition of the capability and capacity of iwi/Māori and marae to support response and recovery; and
- collaboration between iwi/Māori and emergency management organisations before, during and after an event, and across all four Rs.

2.5 Doctrine, training and development, and incidents

Doctrine is the body of principles and practices that guide an organisation's actions in support of their objectives. It is authoritative but requires judgement in application. CIMS is an element of emergency management doctrine that organisations use to manage incidents.

To be effective, doctrine needs to be supported by robust education, training and professional development. Doctrine informs training and development, ensuring that the correct material and content is taught. Training and development then lay the foundation for effective response operations. Experience has shown that doctrine is not applied during response if personnel have not received sufficient training and development. This is particularly so in a multi-organisation setting at the higher levels of response.

Lessons identified from incidents are used to amend and update doctrine. Lessons are not learned until the doctrine has been updated and training and application reflects the new learnings — until then lessons have merely been identified.

The relationships between doctrine, training and development, and incidents are shown in Figure 1 below. This applies in both single and multi-organisation settings.

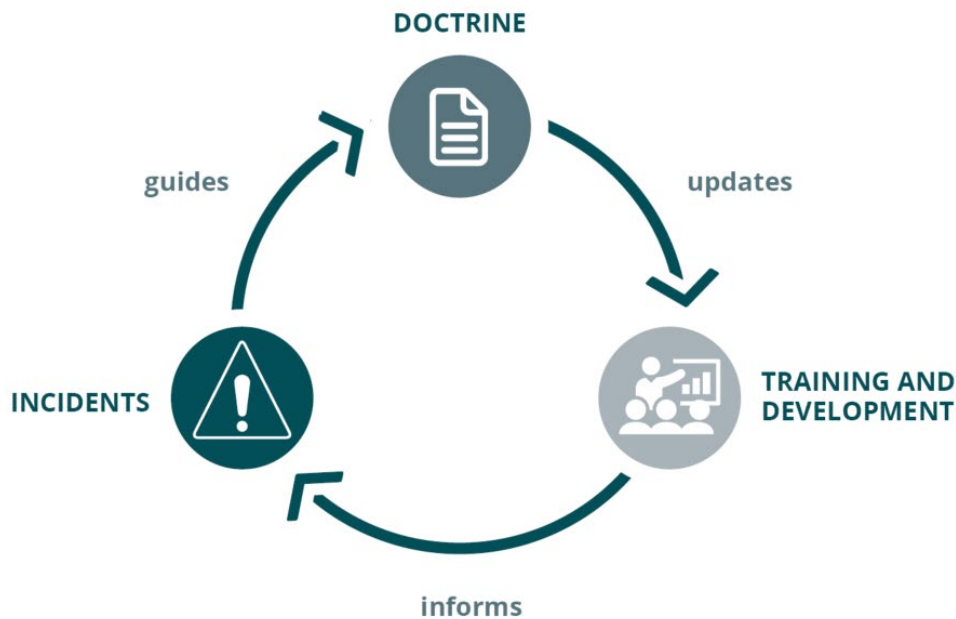


Figure 1: The relationship between doctrine, training and development, and incidents

2.6 Command, control and coordination

Command and control define who has the authority to make decisions and what the parameters of that authority are. Command and control then assist with coordination by defining authority between and within organisations. It is important to have a common understanding and application of these terms.

2.6.1 Command

Command is the authority within a team, unit or organisation and includes the internal ownership, administrative responsibility and detailed supervision of personnel, tasks and resources. Command cannot be exercised across teams, units or organisations unless specifically agreed.

2.6.2 Control

Control is the authority to set objectives and direct tasks across teams, units and organisations within their capability and capacity. This may include control over another team, unit or organisation's resources but does not include interference with that team, unit or organisation's command authority or how its tasks are conducted. Control authority is established through legislation, by formal delegation or by mutual agreement.

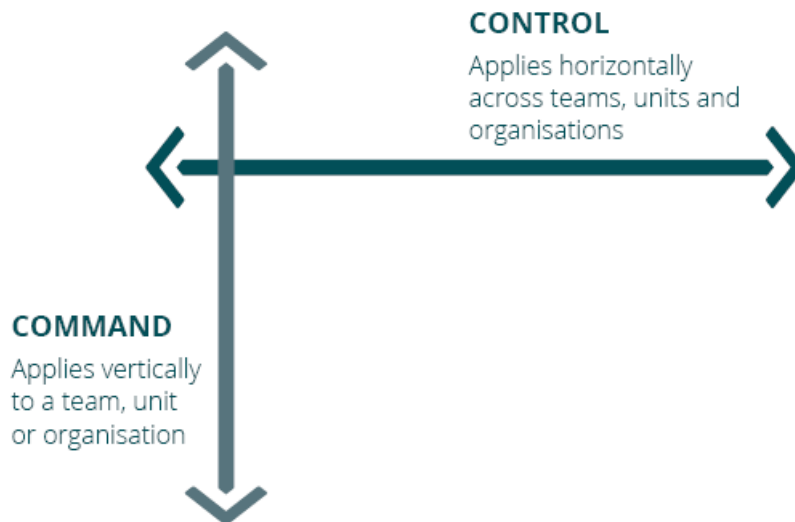


Figure 2: Command and Control

2.6.3 Coordination

Coordination brings together response elements and resources to ensure a unified and effective response. Command and Control assist with coordination by defining authority between and within organisations.

- Coordination in Command occurs within the applicable team, unit or organisation.
- Coordination in Control occurs across teams, units and organisations.

Response coordination in both Command and Control:

- requires consolidated planning, resource coordination and integrated information sharing and communications;
- may be explicit (e.g. briefings and plans) or implicit (e.g. liaison and working together);
- is more effective when information, intelligence and response coordination facilities are shared (when practicable); and
- applies between functions, response levels and agencies or organisations.

The Incident Management Team (IMT) (see Section 2.9.2) plays a key role in response coordination. In a multi-organisation setting, the Controller integrates support agencies into the response by:

- including senior support agency representatives in the IMT, as appropriate;
- ensuring close and ongoing inter-organisational liaison;
- including support agency personnel in the lead agency Coordination Centre;
- including support agencies in the development and implementation of Action Plans; and
- ensuring coordinated communication.

2.7 Unified Control

Unified Control allows for two or more Controllers from different agencies to be integrated into one Control function. The Controllers become Unified Controllers and collaboratively establish overall objectives and priorities and a consolidated Action Plan.

Unified Control does not affect any individual agency's authority, responsibility or accountability. The agencies forming Unified Control can change as the incident develops.

2.7.1 When to apply Unified Control

Unified Control should be considered when:

- more than one agency has a mandate to manage a particular incident; or
- the lead agency determines that a joint approach will be more effective.

Unified Control should only comprise agencies that:

- have legislative responsibility for the management of a sizeable part of the incident;
- are specifically charged with controlling, coordinating or managing a major aspect of the response; and
- have the resources to support management of the response.

Unified Control should be kept small (e.g. two or three agencies). Other agencies will continue to participate as support agencies and be included in the Incident Management Team (IMT). Likewise, Unified Control may include non-government agencies such as lifeline utilities (e.g. an oil company) or public facilities (e.g. a school) in the IMT when required.

2.7.2 Examples of Unified Control

Unified Control is often informally applied at a first responder situation (e.g. a vehicle accident) when the leads of the emergency services convene to jointly manage the incident.

In a rural fire on both Department of Conservation (DOC) land and private land, Unified Control can be formed by the DOC Controller and the relevant Fire and Emergency New Zealand Controller.

2.7.3 Unified Control in practice

Ideally, the Unified Controllers are co-located at the same Coordination Centre. In complex incidents, it is likely that the agencies involved in Unified Control will also activate their own Coordination Centres.

As individuals, Controllers making up Unified Control should have the necessary delegated authority. This includes being able to make decisions, approve the overall incident objectives, commit resources and make financial decisions. The Unified Controllers must agree to a division of responsibilities, but for the purpose of clarity of structure, the preference is that they agree on a Lead Controller among them.

2.8 Holistic and integrated response and recovery

The impact of any incident usually reaches wider than the immediately obvious. Response and recovery must therefore apply a holistic approach to recognise both the direct or immediate, as well as the wider consequences of an incident. This approach not only ensures effective response and recovery, it also ensures a seamless transition from response to recovery.

2.8.1 Consequence analysis across the four environments in response and recovery

To ensure the breadth of impacts, their resulting consequences on communities and the subsequent response and recovery stakeholders are understood, consequence analysis should be considered across the Social, Built, Economic and Natural environments. Not all incidents will result in consequences across all four environments, however, this can only be confirmed by applying this wider analysis approach.

The four environments are explained in Table 1.

Social environment	Built environment
Incorporates individuals, whānau and common-interest groups, and the relationships, communication and networks between them. Consequences can be categorised into: • safety and security; • health; • education; • welfare; and • psychosocial.	Includes the physical setting for human activity, including buildings and their supporting infrastructure. This includes assets such as: • residential housing; • commercial and industrial property; • essential services infrastructure; • rural infrastructure; • public buildings and assets; and • lifeline utilities.
Natural environment	Economic environment
Includes ecosystems and their constituent parts including natural and physical resources, the qualities and characteristics of areas and features and their amenity values, including: • air; • water; • land and soil; and • plants and animals.	Includes the production, distribution and consumption of goods and services with regards to: • individuals and households; • businesses and enterprises of all sizes, including the primary sector; and • government.

Table 1: The four environments

Holistic consequence analysis process

The holistic consequence analysis process applies three steps.

1. **Impact analysis:** Identification of the impacts of the incident across each of the four environments. This ensures a holistic response and recovery focus.

2. **Impacted communities analysis:** Interpretation of the impacts identified in step one in terms of their consequences for specific communities. This ensures that the community focus of the response and recovery can be targeted appropriately.
3. **Stakeholder analysis:** Identification of the stakeholders that should be involved in the response and recovery — by applying the analysis in steps one and two. This ensures that appropriately integrated response and recovery arrangements can be established.

The holistic consequence analysis process should be applied at the onset of a response. However, the analysis can be used by both response and recovery.

The consequence analysis should be documented for reference by others and to allow it to inform recovery planning.

The analysis should be reviewed and updated at appropriate intervals to ensure that new information and/or changes in circumstances are considered.

In a small-scale incident, the analysis can be a mental process conducted by the Controller or a discussion by the Incident Management Team (IMT). Documenting the analysis is still recommended to support planning and/or review.

Using the holistic consequence analysis in response and recovery

The Controller and Recovery Manager use the consequence analysis to determine their intent and objectives, which in turn provide clear direction for planning. Consequence analysis carried out in response informs consequence analysis and planning in recovery.

Applying consequence analysis in both response and recovery supports a seamless transition from the one to the other.

2.9 The incident management structure

2.9.1 Establishing the incident management structure

To manage an incident, the Controller will establish an incident management structure that is:

- based on functional management;
- flexible in its approach and adapted to the needs of the incident as required, such as delegating functions, combining functions or adding functions and/or function resources; and
- reflective of the scale and complexity of the incident, the tempo of operations and the evolution of the incident.

The Controller must use CIMS as a tool, and, as stated above, must be flexible and adaptable in their approach while testing their decisions against the principles and characteristics described in Section 2.2 and the incident classifications in Section 3.2.

For a small incident, or during the early phases of what may become a large or complex incident, the Controller may not need the assistance of an Incident Management Team (IMT) and may instead manage

all applicable functions themselves.

As the incident develops, the Controller may choose to delegate the responsibility for managing some or all CIMS functions (except Control) to other people (see Section 4 for more information on the CIMS functions). The Controller must ensure that people that are delegated functions have the appropriate skills, authority, freedom of action, and resources to perform their functions.

When determining the need to delegate any function, the Controller may consider the following.

- Whether span of control is (or is likely to become) unmanageable;
- the volume of information available;
- the threat to safety;
- the incident's size and complexity;
- the likely duration of the incident;
- the resources deployed or required; and
- the need for specialised advice and input.

The CIMS functions that the Controller may decide to establish are described in Section 4.

When building an incident management structure, the Controller must ensure that personnel with appropriate local knowledge are available to support the functions.

2.9.2 The Incident Management Team (IMT)

The Controller will establish a structure and personnel pool that reflects the scale of the response by delegating some or all of the CIMS functions.

To ensure appropriate coordination and communication between the respective functions and organisations, the Controller establishes an Incident Management Team (IMT). The IMT supports a Controller at any response level (see Sections 3.1 and 4.4).

The IMT typically consists of:

- the Controller; and
- function managers of the respective CIMS functions that have been established or delegated.

In addition, especially in complex incidents, the IMT should also include:

- a Response Manager;
- senior support agency representatives;
- a Recovery Manager;
- iwi-mandated representation;
- Technical and Science Advisors with knowledge relevant to the incident; and
- Risk and Legal Advisors.

Without removing the overall responsibility and ultimate decision making of the Controller, the Controller and their IMT collectively carry the responsibility for resolving the incident by:

- maintaining a collective understanding of what has happened, what is happening and what is likely to happen (i.e. a common operating picture) and communicating this;
- engaging with affected people and communities to determine their needs and intended actions
- agreeing on an Action Plan;
- supporting the establishment and sourcing of necessary resources;
- managing staff effectively;
- implementing the Action Plan and monitoring its progress;
- keeping the respective response elements informed of the decisions and the Action Plan; and
- determining when an incident moves to an emergency, as defined in the Civil Defence Emergency Management Act 2002.

The IMT should meet as frequently as necessary and ensure that records of their deliberations and decisions are kept.

The IMT allows the Controller to maintain an overview of the situation, develop high level objectives, link with Governance and, when applicable, maintain direct relationships with other Controllers in the response (see Section 3.3 for more information on Governance).

The IMT supports the Controller in managing up (within their own organisation and Governance structures), down (within their command lines) and across (the functions and organisations they work with) in accordance with the commonly agreed objectives.

2.9.3 Incident management facilities (Coordination Centres)

In establishing an incident management structure, the Controller must establish an incident control or coordination facility (or facilities) from where the incident management structure or structures will operate. CIMS refers to these facilities as Coordination Centres.

The size and complexity of the incident, in conjunction with the lead agency's internal or legislative arrangements, will determine the appropriate Coordination Centre to manage the response.

For instance, when multiple incidents are interconnected at the same response level, it is likely that they will be best managed by establishing a higher level Coordination Centre.

Regardless of the number of Coordination Centres and response levels that apply, it is important that only one Coordination Centre in the hierarchy or structure is the facility from which the overall incident is controlled. The exception may be in a Unified Control situation.

The following Coordination Centres are used in CIMS:

Response Level	Coordination Centre
Incident	Incident Control Point (ICP)
Local	Emergency Operations Centre (EOC)
Regional	Emergency Coordination Centre (ECC)
National	National Coordination Centre (NCC)

Table 2: Coordination Centres

At the incident level, a number of ICPs may be established to support the management of the incident.

The locations of EOCs, ECCs and NCCs are normally pre-established and they include the infrastructure needed to manage a prolonged and coordinated response.

Besides the Coordination Centres, there may also be a need for additional incident management facilities within the response structure. This may occur in situations when there are multiple ICPs that exceed a manageable span of control. In this situation, sectors may be established that coordinate multiple ICPs and report up to an EOC.

Some of the typical additional facilities are described in Table 3 below:

Facility	Purpose
Assembly Area	May be required if a significant amount of resources are being mobilised. It is used for receiving incoming resources, organising and storing them and then transporting them to where they are needed. Assembly Areas are normally established at local, regional or national levels.
Inner Cordon	Established directly around incident level response operations. Only personnel from the responding agencies operate in this inner cordon. All other people are evacuated.
Outer Cordon	Established further from the incident level response operations. Used to control access to the area of operations.

Staging Area	Used for gathering and organising resources at the incident level. Provides a safe location for: - resources to be received and held prior to deployment; - resources to be prepared for assigned tasks (equipment checks, planning, briefings and loading); and - response personnel to recover after returning from a task (cleaning, repairs, rest, meals, reorganisation and resupply). A Staging Area needs to be distinct from other response facilities, even when they are located together, to ensure resources and personnel are kept separate. More than one Staging Area may be required.
Safe Forward Point	Established for holding resources that are called forward for deployment, for briefings or to await movement to their task areas.

Table 3: Additional Incident Management Facilities

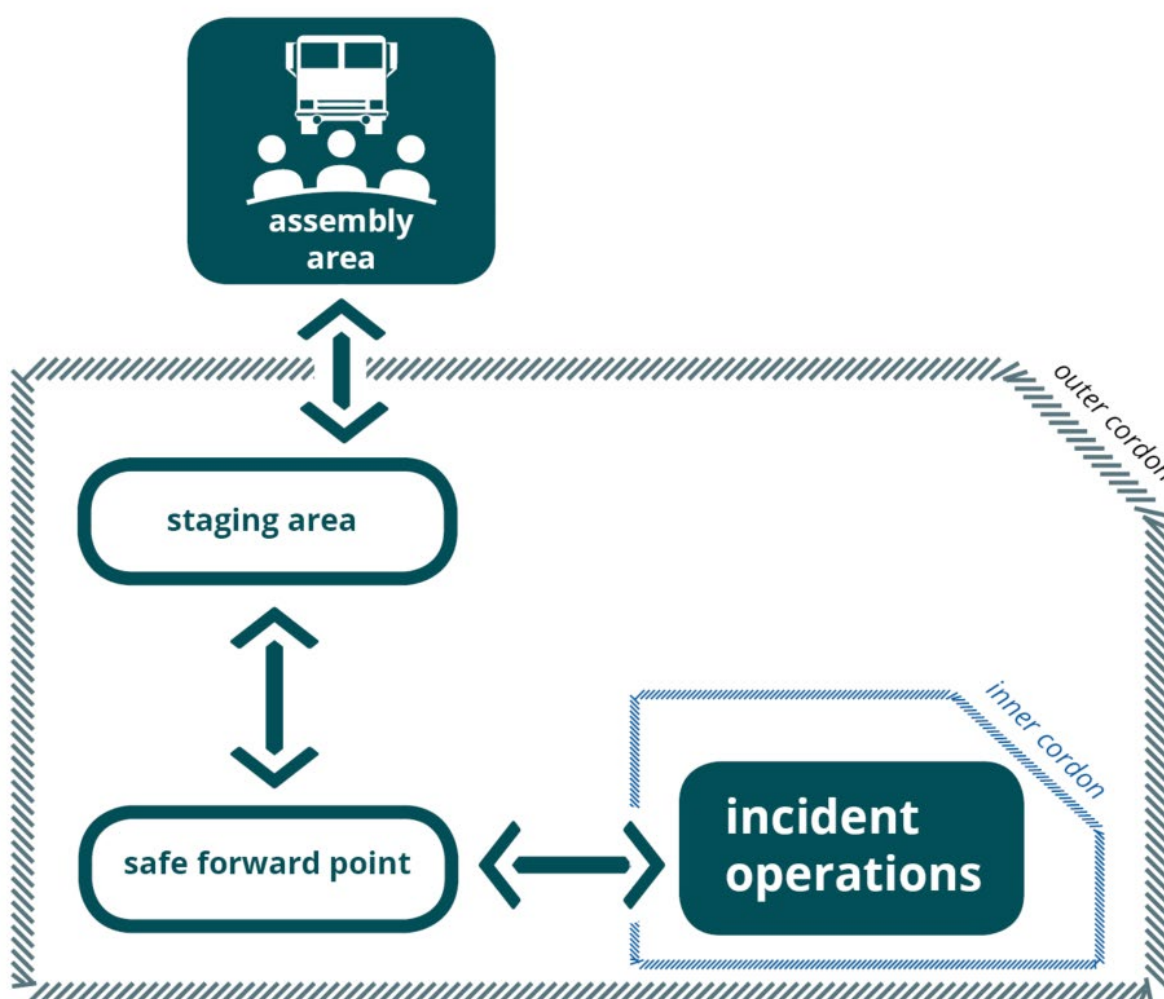


Figure 3: Additional Incident Management Facilities

Section 3 Supporting Protocols and Systems

This section describes the supporting protocols and systems of CIMS, including response levels, incident classifications, and Governance.

3.1 Response levels

CIMS provides a framework where a lower response level can be supported or directed by a higher level. The five CIMS response levels are shown in Figure 4 below.

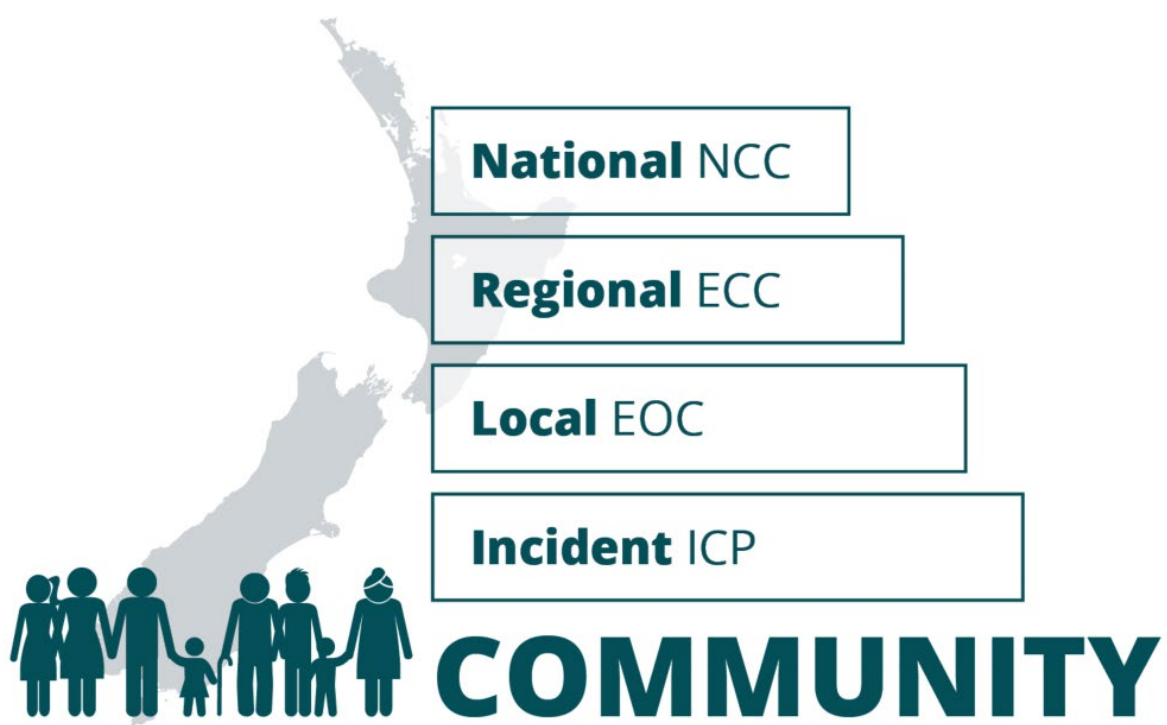


Figure 4: Response levels

The majority of incidents require the activation of only the incident level. The scale, complexity and/or consequences of an incident will determine whether higher levels of response are required, and which levels are appropriate in accordance with the lead agency's internal or legislative arrangements. When higher response levels are activated, they may either assume overall control of the incident or act in support of the response level where the overall control is vested.

The community level is included in recognition of the *Responsive to community needs* principle (see Section 2.2.1) and in recognition of community involvement in a response. This level usually does not form part of the formal response structure, although representation of key community groups may be included in the formal structure as required.

Response Level	Description
National	Includes national organisations' Coordination Centres and headquarters, and national level sector coordinating entities and clusters. Coordinated from National Coordination Centres (NCC).
Regional	Includes Civil Defence Emergency Management (CDEM) Groups, District Health Boards (DHBs), inter-regional DHB coordination, police districts, fire regions and regional organisation offices. Coordinated from Emergency Coordination Centres (ECC).
Local	Includes local authorities, DHBs and organisation offices at the local (district/city) level. Coordinated from Emergency Operations Centres (EOC).
Incident	The first level of official response. It includes first responders. Coordinated from Incident Control Points (ICP).
Community	The public, including individuals, families/whānau, community groups and businesses that participate in the response.

Table 4: Response level descriptions

3.1.1 Community level response

Individuals, communities, organisations and businesses self-respond to incidents, either as part of official pre-existing arrangements or on their own in a spontaneous or emergent manner. Agencies need to enable, accommodate, link with, support and coordinate community participation in response and recovery. Conflict in this regard should be brokered as far as possible; however, where this is not possible, the official coordinated response prevails.

Wherever possible, individuals, communities, organisations and businesses should be appropriately incorporated in response coordination planning before incidents occur. In a response setting, the affected communities must be clearly identified and engaged with.

Effective engagement with the affected communities ensures that:

- they are informed about the response and have a channel for communicating with the formal response structure;
- their needs are identified, assessed and met; and
- self-response initiatives are recognised, supported and coordinated effectively with official activities.

3.1.2 Incident level response

An incident level response is the first official level of response and is carried out by first responders. Response personnel perform physical actions such as clearing obstructed roads, treating casualties,

fighting fires and conducting rescues. Incident level responses may have from one or two personnel up to several hundred.

The Coordination Centre for an incident level response is an ICP, led by an Incident Controller.

Initially, the most senior first responder arriving at the scene assumes the role of Incident Controller and also performs all the relevant CIMS functions. As additional responders arrive, control may transfer to the lead agency for the response. As a response grows in size or becomes more complex, the lead agency may assign a more senior or qualified Incident Controller, and/or the Incident Controller may appoint others to perform relevant CIMS functions.

3.1.3 Local level response

A local level response is usually activated for the purpose of multi-organisation or multi-incident coordination in support of incident level response or to exercise overall control, depending on the lead agency's internal or legislative arrangements.

The Coordination Centre for a local level response is an EOC, led by a Local Controller. The EOC links with the incident level ICPs and, when applicable, with their associated regional or national level Coordination Centre.

Support agency representatives are included in the lead agency's EOC structure. Support agencies at the local level decide whether or not to activate their own Coordination Centres.

3.1.4 Regional level response

A regional level response is usually activated for the purpose of multi-organisation coordination across jurisdictions or local areas in support of local level control or to exercise overall control, depending on the lead agency's internal or legislative arrangements.

The Coordination Centre for a regional level response is an ECC, led by a Regional Controller. The ECC links with the local level EOCs and, when applicable, with their associated national level Coordination Centre.

Regional Controllers do not normally communicate directly with Incident Controllers or other incident level personnel, unless incident level response elements have been deployed directly by the ECC or no EOCs are involved (for example unitary authorities). Instead, staff fulfilling functions in ECCs usually communicate with staff in EOCs, who in turn communicate with staff in ICPs.

Support agency representatives are included in the lead agency's ECC structure. Support agencies at the regional level decide whether or not to activate their own Coordination Centres.

Some organisations combine local and regional level arrangements.

3.1.5 National level response

A national level response is activated for multi-organisation coordination at the national level in support of a local or regional response or to exercise overall control, depending on the lead agency's internal or legislative arrangements.

The Coordination Centre for a national level response is an NCC, led by a National Controller. The NCC links with the regional ECCs.

Support agency representatives are included in the lead agency's NCC structure. Support agencies at the national level decide whether or not to activate their own Coordination Centres.

3.1.6 The National Security System and the National Crisis Management Centre

The National Security System is activated by the Government for events that are nationally significant, or complex enough, to demand a coordinated strategic approach at the national level. The National Security System is part of Governance arrangements at the national level. While the National Security System understands the CIMS structure, it does not form part of the CIMS response levels and can be activated without CIMS. It is discussed in more detail in Appendix D.

The National Crisis Management Centre (NCMC) is a facility used to support the National Security System in the coordination of all-of-government responses. National agencies may also use the NCMC as their NCC in a combined or individual manner.

3.1.7 Response level relationships

In a response with multiple response levels, the different response levels have differing timeframes to act in and they consider the same activities in differing levels of detail. An Incident Controller may consider response actions in a period of minutes or hours, while a National Controller may consider them in terms of weeks or months. Likewise, an Incident Controller may coordinate small teams, while a Local or Regional Controller may coordinate the activities of many teams and a range of response elements.

These differing viewpoints require understanding on the part of response personnel at the respective levels. Likewise, personnel need to adjust their viewpoints as they move between response levels.

The difference in viewpoints is reflected in Action Plans. An incident level Action Plan may cover some of the same activity as a local level Action Plan, but in greater detail and over a shorter timeframe.

Each response level must establish and maintain a direct connection with the response levels at either side (below and above) to ensure an appropriate line of communication and, where applicable, control.

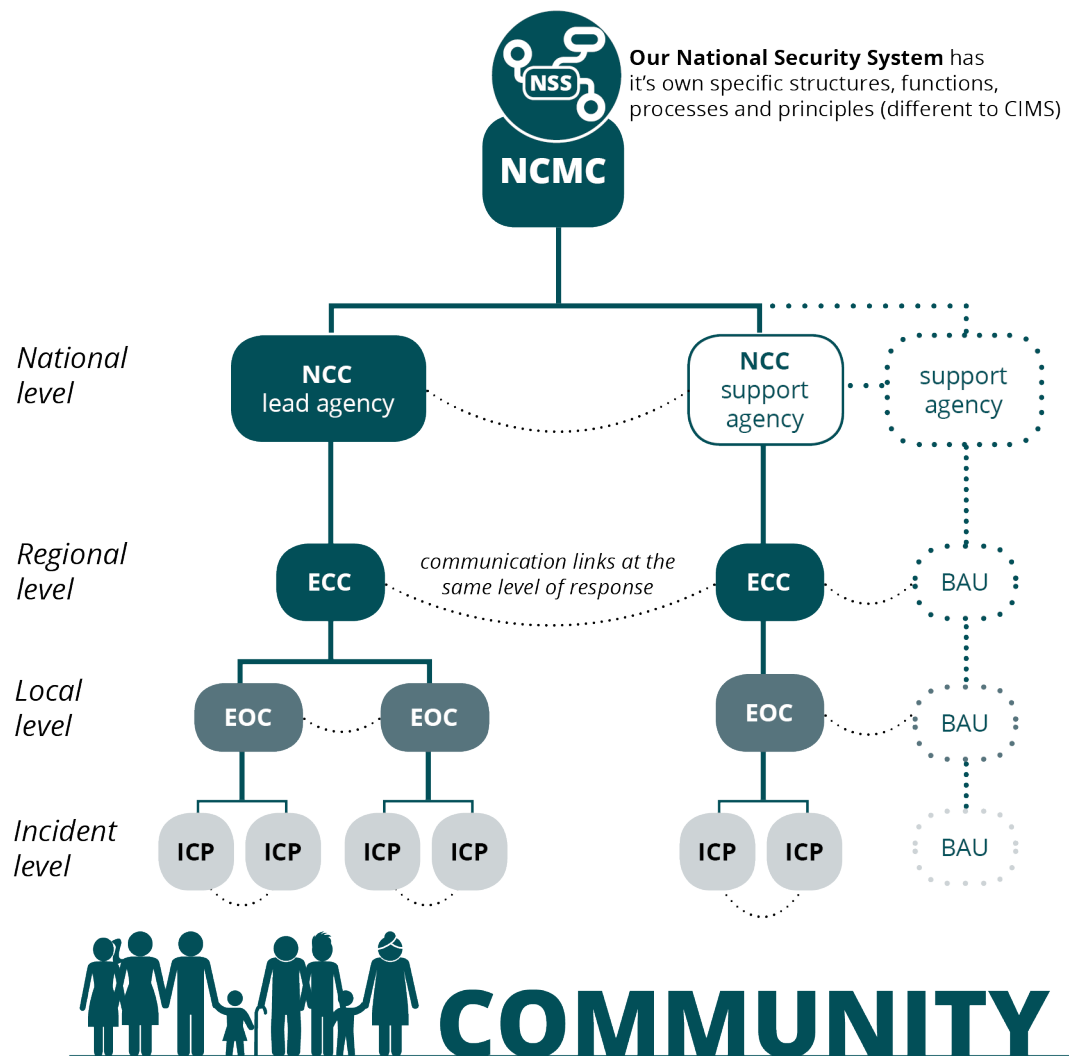


Figure 5: Relationships between the different response levels

Community level response can be supported from local, regional and national levels, depending on requirements. Some agencies may support a response using their business-as-usual (BAU) structures.

3.2 Incident classifications

The classification of an incident provides organisations with a common language with which to communicate the complexity and severity of an incident and the likely level of response required to manage it.

An incident classification will indicate the potential consequences and impacts, resources required, likely political and media interest and response and recovery characteristics.

In addition to aiding communication across organisations, incident classifications may also be used to:

- signal the level of commitment, seniority and skills required or potentially required;
- guide current or future resourcing and associated planning;
- gauge the stress factor across the emergency management system at points in time, and provide an indication of whether higher response levels should be activated;

- measure and monitor trends to inform and support decision making, particularly whether response activities should be scaled up; and
- ensure that those involved in the management of an incident are appropriately skilled, authorised and resourced to perform their role to the standard required for that incident.

3.2.1 Application

CIMS identifies four incident classifications that can apply to a response at any level:

		Severity			
		1 Minor	2 Moderate	3 Major	4 Severe
Response level	National (N)	N1 A minor national level response	N2 A moderate national level response	N3 A major national level response	N4 A severe national level response
	Regional (R)	R1 A minor regional level response	R2 A moderate regional level response	R3 A major regional level response	R4 A severe regional level response
	Local (L)	L1 A minor local level response	L2 A moderate local level response	L3 A major local level response	L4 A severe local level response
	Incident (In)	In1 A minor incident level response	In2 A moderate incident level response	In3 A major incident level response	In4 A severe incident level response

Table 5: Incident classifications

The categories and their descriptors for the respective incident classifications are provided in Table 6. They apply across all response levels.

		Severity				
		Examples of aspects to be considered	1 Minor	2 Moderate	3 Major	4 Severe
Category	Consequences/ impacts	Health and life, infrastructure, culture, community, Treaty obligations, reputation, trade, economy, environment, shelter and accommodation, recovery	A small number of the population in the area are / would be / could be impacted	Some of the population in the area are / would be / could be impacted	Many of the population in the area are / would be / could be impacted	A majority of the population in the area are / would be / could be impacted
	Resources	Capacity and capability to manage (e.g. availability of technical expertise and resources, responders) and finances available	Manageable within available resource and capacity	Requires some allocation of resource	Resource limits and capacity are full	Resource limits and capacity are exceeded
	Public, political and media interest	Degree of expected public, political and media interest (i.e. local interest only, through to global interest), and at what level it should be managed	Minimal to no interest Routinely managed	Some degree of interest Senior leadership and executives are engaged	Significant degree of interest Elected officials and ministers are engaged	Global interest Elected officials and ministers are engaged
	Response and recovery characteristics	Containment, stability, location, spread, number of entities involved, urgency, novelty (e.g. a new event, agencies working with unfamiliar partners etc.), disruption, decisions required, timeframe / expected duration, cost	Familiar/routine/ predictable Known solutions to familiar/routine/ predictable problems	Mostly familiar/routine/ predictable with some degree of irregularity Known solutions to known but irregular problems	Mostly irregular with some degree of familiarity and predictability Mostly known solutions to irregular and possibly unknown problems	Unfamiliar/ unprecedented/ unpredictable Unknown solutions to unknown problems

Table 6: Incident classification descriptors

Classification determination

An incident classification is determined by the Controller, supported by the IMT to ensure consistent understanding, using the categories and descriptors provided in Table 6. The categories and descriptors are applicable across all response levels, although they may not be relevant across all incidents or responses.

If a response involves multiple Coordination Centres, a classification should be determined by the Controller for each centre where a Controller is present.

Communication

The incident classification must be communicated effectively to all responders and support agencies. The classification must be recorded in each Situation Report (SitRep) and Action Plan. A response will be referred to by the first letter (capitalised) of the response level at which the Controller is operating (e.g. L for a locally controlled response), followed by the incident classification attributed to the response by the Controller (e.g. 2). However, should an incident classification at the Incident level be used, the first two letters are used (In) to clearly distinguish Incident from Local.

Escalation and de-escalation

If a response looks like it might escalate or de-escalate in the future, this is recorded.

Examples:

- This response is an N2 escalating to N3 — at the national level, this response currently has a classification of 2 but it might escalate to a 3 in the near future.
- This response is a L2 de-escalating to L1 — at the local level, this response currently has a classification of 2 but it might de-escalate to a 1 in the near future.

The figure below shows how direction of the response is indicated in a field that appears on the SitRep. The example in this figure shows a regional level response at classification 2 that is escalating towards a 3.

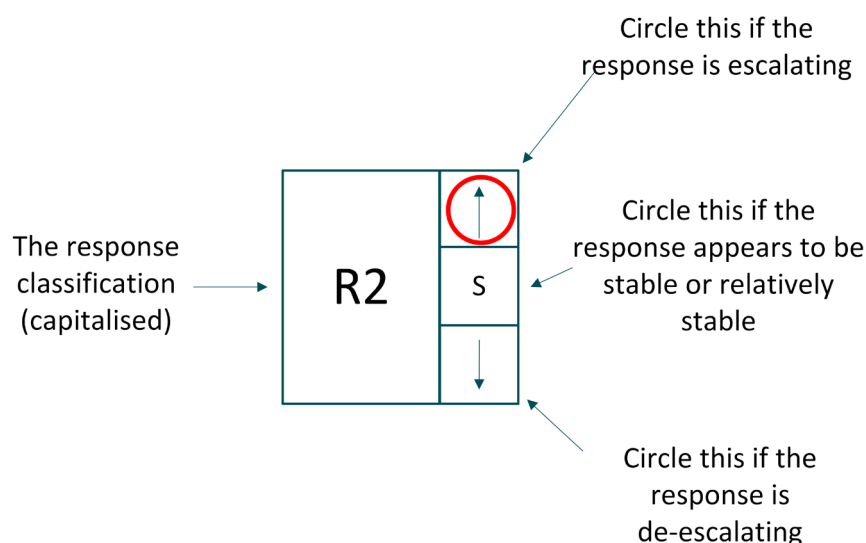


Figure 6: Indicating the incident classification on the Situation Report

Highest level classification

When recording a single, overall classification for a response, post-response, the highest level of classification reached by the lead agency will be used to represent the overall response classification. For example, if a response spans one week and varies in its lead agency classification from In2 at its onset to R2 at its peak before de-escalating to an In1, the overall classification of the response would be R2.

Customisation

Although organisations are expected to adhere to the overarching incident classification approach, they may want to contextualise the descriptors to aid clarity within their organisation. It is important however that any contextualisation or modification does not distort understanding of the classifications as this could be counterproductive to the general intent and utility of the system.

3.2.2 Considerations

While the response level should be relatively evident, it may not be so simple to determine which classification to give the response. The response may not fit cleanly into one level of classification. For example, a 2 may be appropriate for media interest but a 3 for resourcing.

There are no prescribed weightings, although some descriptors may be given greater weight than others depending on the circumstances. The overall classification is provided at the discretion of the Controller, as based on their best judgement at the time of classification.

If an individual organisation wants to provide additional criteria around weighting to suit their particular environment, this is acceptable as long as it does not distort the common understanding of the system.

3.2.3 Limitations

The Incident Classification System is a guide, so there may be grey areas. Classifications are also fluid as opposed to rigid — it is expected that they will change as the response changes.

Classifications require subjective judgement from Controllers and their Incident Management Teams. As such, they should be considered an indicator of the scale of the potential consequences, impacts of an incident and resourcing needs for the response.

3.3 Governance

Every response has executive oversight, known as Governance. Governance arrangements can be complex and dynamic. Formal structures may be less important than relationships between individuals and organisations. Influencers outside of Governance may play key roles, which may or may not be explicit.

Governance does not manage a response. That responsibility falls to the Controller who must have the formal delegation and/or endorsement for the role in accordance with statutory provisions or internal arrangements.

Governance input may be provided at any response level, but must always connect with the highest activated response level. In a large response or for a complex incident, the National Security System may be activated to coordinate the highest level of oversight (see Appendix D).

In complex incidents, Strategic Communications and/or Policy may support Governance (see Section 3.3.3).

3.3.1 Layers and roles of Governance

The following layers of Governance interact to provide, influence and guide the strategic direction of a response.

Governance Layer	Who (e.g.)	Role
Political	Ministers, mayors, chairs, councillors, CDEM Group Joint Committees	- Communicates and influences the strategic direction outside the operational response at a national, regional or local level. May act as spokesperson. - Executes legislative authority (e.g. declaring a state of emergency). - As elected officials, may be held accountable by communities for the overall response outcomes.
Senior Management	Controller's immediate superiors, higher commanders, Chief Executives / executive managers, CDEM Group Coordinating Executive Groups	- Has oversight, assigns resources, and may impose constraints (e.g. deadlines, cost and resource limits) and assign objectives. - Assigns resources; may influence or assign objectives. - Communicates and influences the strategic direction outside the operational response. - Interacts with and is accountable to Political Governance. - May be accountable for the outcomes of the response (in particular the lead agency).

Table 7: Layers of Governance

3.3.2 Governance inputs and outputs

Governance needs to understand its role in different settings — for example when a state of emergency is declared under the Civil Defence Emergency Management Act (2002), the roles of mayors and chief executives change.

More generically, the following approaches apply to Governance at any layer.

Inputs

Governance depends on the following inputs:

- The capability of Governance members.
- The human and financial resources committed and their status.
- Quality and timely information.
- A collective commitment to common goals, while acknowledging different drivers.

Outputs

Quality decisions:

Making quality decisions involves:

- considering broader factors and balancing uncertainty with timeliness;
- considering the health, safety and wellbeing of response staff;
- being comprehensive and courageous (challenging the status quo);
- basing decisions on detailed risk assessment and analysis; and
- prioritising response and recovery against other work.

Clear strategic direction:

Clear strategic direction is:

- explicit, preferably in written form and suitable as a basis for action planning;
- well-considered;
- backed by resources and commitment;
- well-matched with mandates of the organisations represented;
- supportive of management of the response, based on assurance and oversight; and
- regularly reviewed.

3.3.3 Governance support

Strategic Communications

Strategic Communications provides high-level oversight and issues management with a particular emphasis on providing advice and communications support to elected officials, chief executives and key stakeholders. Strategic Communications brings a well-attuned radar for political, reputational and stakeholder risks and opportunities.

Strategic Communications is usually only activated in complex and/or large-scale incidents. The decision to activate will be made by either Governance or the Controller. Strategic Communications personnel may be deployed at any response level.

Strategic Communications uses the information produced by the Coordination Centre. It operates in a complementary capacity to the Public Information Management (PIM) function (see Section 4.10),

enabling PIM to focus on their core responsibilities of providing information and safety advice to the public, staff and media.

Strategic Communications is not a formal CIMS function and is not mandated to direct other functions, but may provide advice and relay tasks on behalf of Governance. It provides a consistent point of liaison and support between the Controller and the PIM function, and Governance.

Strategic Communications enables:

- elected officials, chief executives and other key stakeholders to be well briefed and advised from a strategic and reputational viewpoint;
- consistent messages to be disseminated among elected officials and key executives;
- political, reputational and stakeholder relations risks to be identified, escalated where necessary and mitigated; and
- PIM to maintain its core focus on keeping the public, staff and media informed.

Strategic Communications responsibilities include:

- bringing cohesion and a joined up approach to communications matters across multiple organisations, stakeholders and elected officials;
- providing or supporting the briefings, consistent messages and communications advice to elected officials, executives and iwi;
- strategic stakeholder relations;
- working with PIM to brief Governance spokespeople;
- working with PIM to support media briefings involving elected officials and/or executives;
- supporting PIM with coordination of VIP visits; and
- risk and issues management.

The nature of Strategic Communications will vary depending on the complexities of the incident and the scale of the response and the degree of public and political interest. Where Strategic Communications responsibilities overlap with PIM responsibilities, the two are expected to work collaboratively. When Strategic Communications is activated, a clear understanding must be established with the Controller and the PIM function about the responsibilities of Strategic Communications, how Strategic Communications will interact with and complement Coordination Centre functions and what deliverables are required.

Policy

At higher response levels, a Policy component may be required to support Governance with the preparation of committee papers and minutes, briefings to executives and elected officials or approvals to enact legislative provisions.

Policy must use the information produced by the Coordination Centre and maintain a close relationship with the Controller, as the Controller must approve any Policy papers before they are submitted to Governance. Like Strategic Communications, Policy is not a formal CIMS function.

Section 4 The CIMS Functions

This section provides an outline and examples of how the CIMS functions can be applied in incident response. For the purpose of CIMS, a function is an activity or grouping of activities that addresses some of the core responsibilities of a response.

4.1 Introduction

Incident response involves a range of activities to be carried out. CIMS divides the responsibilities for these activities into CIMS functions, which are established as required, and then operate in a networked hierarchy (see Section 4.3).

The CIMS functions are:

- Control (and Controller's Support)
- Safety
- Intelligence
- Planning
- Operations
- Logistics
- Public Information Management (PIM)
- Welfare
- Recovery [during response]

Detailed descriptions of the CIMS functions, including responsibilities and sub-functions, are given in Sections 4.4–4.11. The sub-functions described represent the most common outputs associated with the function. In establishing and reviewing the response structure, the Controller will determine which sub-functions apply to their situation and needs. Some sub-functions may be established or combined (or combined with the sub-functions of other functions), or some new ones may be added. A full CIMS structure that shows all the functions and their sub-functions is given in Appendix A.

The CIMS functions do not represent a default response structure — depending on the incident classification and objectives some functions may not be required and some functions may be combined or condensed or even amended to suit the requirements. They can be carried out by a single person or by teams of dedicated personnel. The functions that are required are then represented in the response structure.

While all the CIMS functions report to the Controller, they operate in a networked approach with each other. For instance, all the functions need to be involved in Planning, Intelligence needs input from all the functions, Logistics supports the resource requirements of all the functions, Operations tasks all the functions and receives implementation reports from them, etc.

4.2 Function colours and responsibilities (summary)

Functions are identified by colours and text on vests, nametags or armbands. The identification colours and responsibilities for each of the functions are summarised in Table 8.

Function	Colour	Responsibilities
Control	White	Controls and coordinates the response.
	Red	Controller's Support
Safety	Green	Advises on measures to minimise risks to response personnel.
Intelligence	Dark blue	Collects and analyses information and produces intelligence related to context, impacts, consequences and forecasts.
Planning	Pink	Plans for response activities and resource needs.
Operations	Orange	Tasks, coordinates and tracks execution of the Action Plan.
Logistics	Yellow	Provides personnel, equipment, supplies, facilities and services to support response activities.
Public Information Management	Purple	Develops and delivers messages to the public and liaises with the impacted community. Develops messaging for Governance when Strategic Communications is not activated.
Welfare	Light blue	Ensures planned, coordinated and effective delivery of welfare services to affected individuals, families/whānau and communities, including animals.
Recovery	Grey	Starts the recovery management process during the initial response phase and ensures the recovery process is integrated with the response.

Table 8: The CIMS functions — Identification colours and summary of responsibilities

4.3 A networked hierarchy

Organisations operate either as a hierarchy, which is a set structure that relies on command and control, or as a network, which is more flexible and is based on relationships between roles. CIMS operates as a combination of the two — a networked hierarchy. This is a necessary approach as it allows for both cooperation among response elements and focused decision making, direction and action.

CIMS uses the Command and Control approach of a hierarchical structure with the Controller being at the top of the hierarchy directing the various functions and organisations. But it also applies a networked approach through the relationships between functions and organisations, and between the response levels involved. Response elements, functions and organisations cannot operate in isolation — they must collaborate and coordinate with each other in a networked manner while still keeping the command and control structure at the centre. As a response escalates or de-escalates, the network can expand or contract to suit requirements.

CIMS requires functions to communicate and coordinate not just within their own Coordination Centre, but also with their peers in other Coordination Centres above, below and to the sides. For example, a Logistics Manager in an ECC should freely communicate and coordinate their activities with other logistics staff in an NCC, neighbouring ECCs and EOCs.

4.4 Control

The Control function involves the exercising of response leadership through:

- having overall responsibility for all activities and personnel involved in the response, including safety; and
- coordinating and managing the response objectives with organisations, communities, and people responding to or affected by the incident.

The Controller may be supported by an Incident Management Team (IMT) and, where appropriate, Deputy Controllers, a Response Manager, Technical and/or Science Advisors, Risk and/or Legal Advisors, Iwi/Māori Representation and a Controller's Assistant or Assistants.

The Controller must:

- have the formal delegation and/or endorsement for the role in accordance with statutory provisions or internal arrangements;
- be readily identified and their appointment well communicated and understood by all persons and organisations interacting with the response; and
- be competent for the scale and complexity of the incident.

4.4.1 Control when multiple response levels apply

The Control function can be represented at multiple interconnected levels of response and across organisations at the same time. Therefore, when the term Controller is used, it must be prefixed with the response level or agency that they represent, i.e. Incident Controller, Local Controller, Regional Controller, National Controller and/or [Organisation] Controller.

When multiple interconnected response levels apply, no Controller can work in isolation of the Controllers at the other response levels.

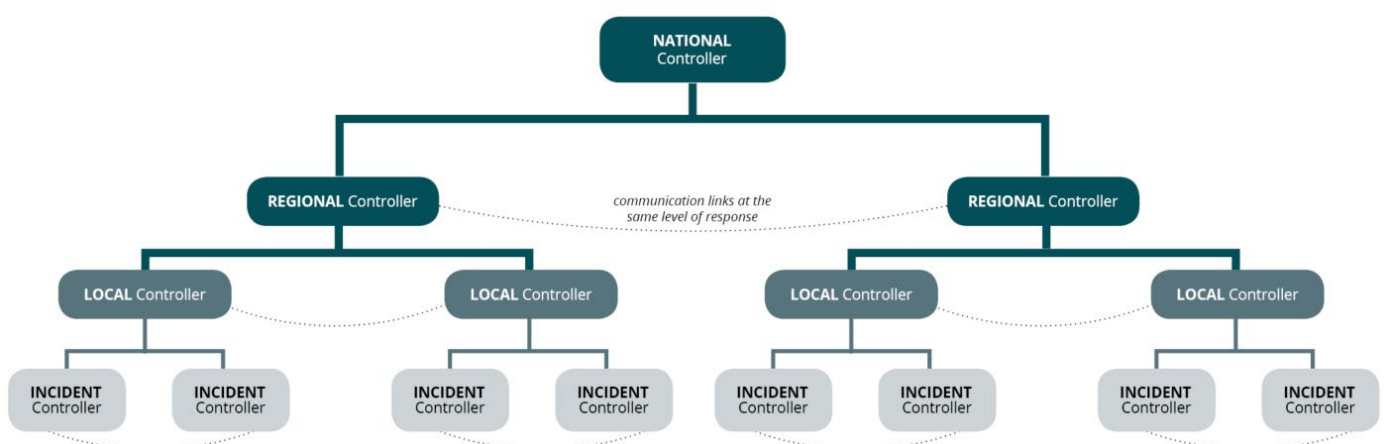


Figure 7: Example of Controllers at different response levels

4.4.2 Lead Controller

Only one Controller can be the Lead Controller who directs the overall response to the incident. The Lead Controller and the response level they operate at is determined by the protocols of the lead agency for the response and, in some cases, by statutory provisions. Where legislative powers associated with the role of the Controller apply, these will be vested only in the Lead Controller, while other Controllers will act in support of, or under authorisation of, the Lead Controller.

4.4.3 Responsibilities

The Controller is responsible for:

- taking charge through the setting of response intent and objectives and providing (or approving) an Action Plan that sets out how the objectives will be achieved;
- establishing the response structure and incident classification;
- directing and monitoring the response;
- maintaining situational awareness;
- keeping the affected people, animals and communities at the forefront of the response;
- applying a risk management approach, ensuring responder, public and animal wellbeing and safety;
- determining and obtaining critical resources, facilities and materials;
- establishing and maintaining liaison, cooperation, and communications with support agencies, affected businesses and enterprises, communities and Controllers at other response levels;
- communicating with Governance;
- acting as an operational spokesperson if a dedicated spokesperson has not been appointed;
- ensuring the response stays within prescribed resource and budget limits; and
- working with the Recovery Manager to manage the transition from response to recovery (see Section 4.12 and Appendix G.5).

The primary responsibility of the Controller can be summarised as providing ongoing direction and oversight of the response. In executing this, the Controller must be:

Clearly identified

The Controller must establish their presence among response staff, support agencies and other interconnected response levels. This is achieved through being present, establishing the IMT, conducting personnel briefings and having an Action Plan.

Situationally aware

The Controller operates amid a rapidly changing environment, usually marked by (initially) limited information and uncertainty. They must balance the need for accurate advice and information against the need for timely decisions. They must think forward and consider gaps and risks. Where applicable,

they must be aware of, and work according to, the intentions of Governance and the decisions of the Lead Controller.

Make decisions

Decisions must be timely, clearly noted and communicated and continually reviewed against the evolving situation.

Available

The Controller must be available to response elements for questions, decisions, approvals and authorisations, and direction.

In the absence of, or in support of, dedicated spokespeople the Controller must communicate with the affected communities and the public/media. This communication should be in a planned and organised manner, in person as well as through documented statements, and be supported by the Public Information Management (PIM) function where possible.

Controllers may also need to allocate time for servicing and briefing Governance. When this becomes a major task, the Controller should delegate and prioritise duties and tasks to their IMT and/or Deputy Controllers or Response Manager (see Section 4.4.4).

In order to perform their responsibilities, the Controller must ask frequent questions of the IMT, e.g. what do we know, what don't we know, what is our resource status and options, and what next?

4.4.4 Controller's support

Deputy Controller(s)

The Controller may delegate a Deputy Controller or Controllers to fill in when the Controller undertakes a rest period or to manage specific responsibilities or areas of complexity. The Controller always retains the primary oversight and decision making — Deputy Controllers must follow the direction and priorities set by the Controller. Deputy Controllers cannot change structures, processes, decisions or Action Plans without the consent of the Controller, unless a rapidly changing situation warrants a change in objectives and actions.

Response Manager

The Controller may appoint a Response Manager (sometimes also referred to as a Chief of Staff) to assist them in the management of tasks, the operation of the Coordination Centre and in resolving internal conflicts. They may be delegated to provide approvals in the absence of the Controller or represent the Controller outside the Coordination Centre. This frees the Controller from the operational details involved and allows them to think ahead and focus on priorities or higher level matters.

A Response Manager is responsible for:

- contributing best practice expertise and technical experience to the effective operation of the Coordination Centre;
- ensuring each function or team understands their role, the actions required under the Action Plan and how they need to work with other functions;

- ensuring alignment and coherence of actions across functions by reducing overlaps, gaps and performance issues;
- keeping functions on track, and maintaining pace and focus on interdependencies and deadlines;
- identifying capability and experience gaps and providing guidance, tactics and advice to get the job done;
- influencing and troubleshooting to resolve problems and to minimise escalation to the Controller;
- attending IMT meetings and keeping the Controller and IMT informed of the response management aspects of the response;
- setting and monitoring the schedule, ensuring information flows are current and effective across all parts of the response, and keeping the Controller advised on statuses and trends; and
- building a constructive and positive culture in a complex and pressured environment, modelling good behaviours and having response staff's wellbeing at heart.

Controller's Assistant(s)

The Controller's Assistant is responsible for recording meetings and decisions, managing the Controller's diary, answering calls and responding to emails, and managing the administrative arrangements for the Control function. The role of Controller's Assistant can be performed by more than one person.

Technical and Science Advisors

Technical and Science Advisors provide specialist advice on aspects of the response. This could include scientists specialising in the hazard (such as volcanologists during a volcanic eruption), environmental experts (such as hydrologists during a flood), medical experts (such as a Medical Officer of Health in an infectious disease incident) or industrial experts (such as fuel supply experts during a fuel disruption). These experts can also be assigned to Planning, Intelligence and/or Operations, but retain a direct relationship with the Controller. They may also serve as Liaison Officers if they are members of a support agency.

In a larger response where there is a shortage of Technical and Science Advisors, these experts may be centralised into an advisory group at the highest activated response level. This ensures their expertise can be assigned to where it is most needed or will have the most effect.

Risk and Legal Advisors

A Risk Advisor monitors and advises the Controller on wider risk considerations related to the response, i.e. political, reputational and strategic considerations.

A Legal Advisor may be required to identify, advise on and manage legal issues.

Iwi/Māori Representation

Iwi/Māori representation provides cultural advice to the Controller and ensures iwi/ Māori interests are represented. Being part of the IMT, the representation also ensures that connections to the various functions are established and maintained, iwi and Māori media channels are informed about the response objectives and progress, and that the welfare of the wider Māori community and whānau is captured in response planning. When more than one iwi is involved, representation from all iwi should be

accommodated to ensure a consistent and shared cultural consideration. The nature of representation will vary from region to region and should be determined by the Controller, working with local iwi/ Māori to ensure appropriate mandates.

Iwi/Māori representation should understand local resources that might be able to be mobilised, ensure interactions with and between iwi/Māori networks are managed appropriately, and provide advice on tikanga and local topography e.g. wāhi tapu.

4.5 Safety

The Safety function supports the Controller to ensure that all those involved in the response are kept safe in accordance with the requirements of the Health and Safety at Work Act 2015. The Safety Manager will have a close relationship with other CIMS functions and other organisations connected with the response, and may be supported by Risk Advisors (Control), and Administration and Health and Wellbeing staff (Logistics).

The Safety function provides expert advice and oversight on issues relating to safety, health and wellbeing within a response. It does not remove the responsibility on individual organisations for the health and safety of their staff.

4.5.1 Responsibilities

Safety is responsible for:

- collecting, collating and analysing safety, health and wellbeing information based on risks posed by an incident and its management;
- working with the Risk Advisor to ensure that the response risk registers are addressing safety, health and wellbeing matters so that the risks are understood and controlled, and that controls are checked to ensure that they are working;
- establishing arrangements for the control, monitoring and reporting of safety, health and wellbeing issues by the CIMS functions;
- ensuring that dynamic safety risk assessments are being completed and documented, as appropriate;
- ensuring continuity of Safety activities across shift changes;
- working with Health and Safety teams to establish and consult on the nature of safety at the front line of the operations;
- maintaining a log and record of incidents, near misses and activities pertaining to Health and Safety;
- providing safety, health and wellbeing advice and recommendations for the Situation Reports (SitReps), Action Plans and other response plans;
- determining staffing requirements and any Health and Safety Technical Advisors required, and reviewing these as required during the response;
- establishing Safety Liaison Officers, or Safety sub-managers, if required within other CIMS functions; and
- attending Incident Management Team (IMT) meetings and keep the Controller and wider IMT informed of the Health and Safety aspects of the response.

4.6 Intelligence

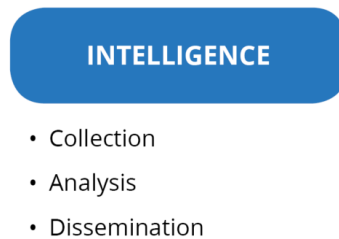


Figure 8: Intelligence

Intelligence is the function that provides the other CIMS functions with a detailed understanding of the incident and the ways in which the incident could potentially develop. It provides situational awareness and understanding for immediate action and forecasting and identification of emerging risks to assist planning.

The Intelligence function is performed through the application of the Intelligence Cycle (see Appendix B). Through this process, incident information is collected, analysed and intelligence products are produced and disseminated.

Intelligence has four key questions to answer:

- What is happening now?
- Why is it happening?
- So what, i.e. what does it mean?
- What may happen next / in the future?

While the first two questions require accurate and timely information on what is actually occurring now, the third requires analysis of the information against the wider context, and the fourth is usually described through at least two scenarios: the most likely way the incident will develop and the most dangerous/worst case. This is so that Planning can address the worst case scenario as well as the most likely (via Action and Contingency Plans). A plan that covers both of these scenarios will generally be robust enough to cover the actual progression of the incident. If time and circumstances permit, other scenarios can also be developed to assist the development of Contingency Plans.

4.6.1 Responsibilities

Intelligence is responsible for:

- identifying and receiving the intelligence requirements of key decision makers (e.g. the Controller and function managers);
- overseeing the collection of information that will help meet those requirements;
- collating and managing collected information;
- evaluating the reliability of the information and recording this appropriately;
- processing the information in preparation for analysis;

- analysing the information and creating intelligence products (e.g. Situation Reports (SitReps), profiles, intelligence summaries, oral briefings, etc.);
- producing and disseminating intelligence to decision makers and others who need to know;
- managing documents of products created by Intelligence;
- gathering feedback about how the products were used and identify any remaining (or new) intelligence requirements that still need to be met;
- contributing to the planning process, including the development of the Action Plan; and
- attending Incident Management Team (IMT) meetings and keeping the Controller and wider IMT informed of the Intelligence aspects of the response

Intelligence provides (in documented and/or oral format):

- updates on the situation (e.g. SitReps);
- identification and analysis of key issues;
- forecasts (scenarios) and identification of emerging risks (including their probability and impact); and
- implications of key decisions for the attention or action of decision makers.

4.6.2 Sub-functions

Intelligence delivers its responsibilities by applying an Intelligence Cycle that groups its steps under three sub-functions.

Collection

Collection is responsible for:

- confirming intelligence requirements;
- identifying the information and sources that will best meet requirements;
- establishing and managing the information collection plan;
- collecting individual pieces of information;
- receiving, logging, and storing the collected information; and
- noting any caveats that may be associated with the information (e.g. confidentiality).

Analysis

Analysis is responsible for analysing the collected and processed information. Analysts should be able to apply a range of analytical tools, techniques and critical thinking skills to develop insights and judgements. The most fundamental interpretation method is to ask the “5WHs” interrogatives: who, what, when, where, why and how? Application of the questions ‘so what?’ and/or ‘what does this mean?’ allows analysts to consider and advise on possible implications for response (and potentially recovery). Such methods help analysts avoid common pitfalls of simply restating the facts or describing collated information. Analysis should have an emphasis on forecasting and identifying emerging risks and potential consequences.

Dissemination is responsible for the production of intelligence products and for delivering these (whether written, oral or pictorial) in a format and timeframe that meets the stakeholders' needs. Products should focus on those key issues that decision makers need to be aware of before making important decisions. The information context may include:

- hazards (natural or man-made);
- community, demographic, cultural and human factors;
- actual or potential impacts on people and animals;
- terrain (geology, topography, vegetation and hydrology);
- climate and weather;
- infrastructure; and
- economic factors.

Products may be a formal written report, a briefing, a meeting or an informal discussion. Decision makers are rarely intelligence professionals. To be useful, intelligence products should be written for decision makers, not for other intelligence professionals. This means that intelligence products need to be clear, concise and simple, and have no jargon. Successful dissemination requires a good understanding of the stakeholders' needs, and the ability to tailor products accordingly.

4.6.3 Geospatial Support and Coordination

Geospatial Support and Coordination is responsible for providing geospatial support, coordination, and services to the Intelligence sub-functions. This involves the collection, processing, analysis, and dissemination of geospatial intelligence products. Geospatial intelligence products should enhance situational awareness of where things are happening, and how they relate, connect and evolve.

There needs to be coordination between agencies and organisations with geospatial capability to enable geospatial information sharing across systems. Working to agreed standards is essential to enable interoperable and consistent geospatial information sharing.

To ensure geospatial services are utilised to the fullest extent possible, geospatial specialists should be able to communicate to others the meaning and limitations of technical products. Graphics should be accompanied with text explanations with no jargon. Geospatial coordinators and specialists should assist other personnel in Intelligence and other functions to become geospatial generalists who can identify possible tasks.

Geospatial technologies can enable some tasks to be completed remotely, but only if tasks are appropriately scoped and communicated effectively with those supporting remotely. Geospatial outputs can include printed maps, web maps, images, infographics, tables and reports.

4.7 Planning

PLANNING

- Action Planning
- Long-term Planning
- Contingency Planning
- Transition Planning

Figure 9: Planning

Planning is the function responsible for overseeing the development of response plans, e.g. Action, Long-term, Contingency and Transition Plans. The Controller has ultimate responsibility for these plans; Planning is responsible for carrying out the planning process on the Controller's behalf.

The Planning function must utilise the "Planning P" as described in Appendix C to ensure that planning is effective. The planning process should be collaborative across all functions and key stakeholders.

Successful planning depends on the following inputs:

- The Controller's intent for the response (this may be informed or influenced by Governance in the form of a Delegation of Authority, Terms of Reference, or Task Assignment);
- The Controller's response objectives, which are the outcomes that a response is aiming to achieve;
- Impact and context analysis from Intelligence outputs. These are used by Planning when developing and analysing options;
- Information and ongoing engagement in the planning process from Control, Operations, Logistics, Public Information Management (PIM), Welfare, Safety, Recovery, support agencies and other Incident Management Team members, e.g. lifeline utilities and iwi/Māori representation; and
- Information on available response resources (immediately available and en-route) from Logistics, Operations and/or support agencies.

Without accurate information on the current state, predicted or forecast situation, and resource availability, planning cannot be effective.

4.7.1 Responsibilities

Planning is responsible for the planning process, including:

- translating the Controller's intent and objectives into an Action Plan;
- convening and facilitating planning meetings for Action Planning, Long-term Planning, Contingency Planning and Transition Planning;

- developing other specific plans, e.g. Communications, Handover, and Demobilisation Plans;
- forecasting medium- to long-term resourcing requirements;
- translating the Recovery Manager's intent and objectives into a transition plan for moving from response to recovery; and
- attending Incident Management Team meetings and keeping the Controller and wider IMT informed of the Planning aspects of the response.

4.7.2 Sub-functions

Action Planning

Action Planning involves developing a plan (or plans) that describe how response objectives will be achieved.

Some responses may require a single Action Plan to be developed that encompasses the entire response. However, planning in complex or larger responses may need to be approached through operational periods with multiple planning cycles being undertaken and multiple Action Plans being developed. In these cases, the Controller will determine which response objectives will be prioritised during each operational period.

Key components of the Action Planning process include:

- developing Specific, Measurable, Achievable, Relevant, and Time-bound (SMART) objectives for the operational period that meet or contribute to the overall response objectives;
- developing the options for achieving these objectives, and selecting a preferred option as the basis for the Action Plan;
- identifying the resource requirements for the options and contingencies;
- monitoring progress towards achieving the planning objectives and response objectives (with Operations); and
- contributing strategic information and risks to Governance reporting.

Long-term Planning

Long-term Planning involves the scoping and developing of plans for response activities beyond the current and subsequent operational period. Long-term Planning may apply to hours, days, weeks or even months, depending on the response level and the scale of the incident. These plans are likely to be less developed than Action Plans, due to less reliable information about the future development of the situation and a greater reliance on assumptions. Long-term Planning delivers:

- plans to address the anticipated development of the situation and how it could be managed;
and
- plans for managing resources.

Contingency Planning

Contingency Planning involves developing plans for a particular situation or scenario that has not, but may occur. It addresses the what-if scenarios, both positive and negative, that the Controller, Intelligence and Planning teams believe deserve particular attention. Contingency Plans are often completed with less detail because of information gaps, personnel, and time constraints and because they cover situations that may occur and are based on assumptions and estimates.

Contingency Plans may be developed after an Action Plan has been completed or may be developed in parallel. The need for a Contingency Plan is often identified during the development of the Action Plan. Contingency Plans are often developed during business-as-usual activities.

Long-term and Contingency Planning use the same processes, inputs, and personnel as Action Planning.

Long-term Planning addresses response objectives that are not being completed in the current or subsequent operational period, but which may require planning to start now (e.g. transition to recovery).

Transition [to Recovery] Planning

Transition Planning involves developing plans for moving from response to recovery. This planning covers how coordination and accountability formally transitions to recovery and how the response phase will be wrapped up. Transition Planning is scalable in the same way that Action, Long-term and Contingency Planning are. A Transition Plan should be based on the Recovery Manager's intent, objectives and outcomes for the recovery phase and include input from the IMT and the Controller.

Both the Controller and Recovery Manager must sign off the Transition Plan.

4.8 Operations



Figure 10: Operations

The Operations function is responsible for the day-to-day coordination of response actions, stakeholder groups, and detailed tasking that follows the Action Plan.

This function has an overview of all the actions within the response, including those of support agencies, community groups and volunteers, and resolves any operational problems that do not need to be escalated to the Controller. To ensure this overview and coordination, Operations must have representation of, or be connected with, the other CIMS functions, key support agencies, and community and volunteer groups that play a role in the response (as appropriate for the response level).

4.8.1 Responsibilities

Operations is responsible for:

- coordinating day-to-day response activities on behalf of the Controller;
- integrating all stakeholders into the response;
- supporting the Welfare function or welfare organisations to deliver welfare services;
- implementing operational aspects of the Action Plan, including coordinating all tasks within the Coordination Centre (this includes tasking actions to appropriate functions, organisations, or other response elements, monitoring the progress of those tasks), and advising or forecasting resource needs);
- coordinating volunteer (including spontaneous volunteers and emerging groups) activities in conjunction with the Safety function to ensure that volunteers are safe and that all accountabilities are considered;
- managing field staff;
- contributing to the collection of information from the field or organisations for the Intelligence function;

- maintaining a log to record function-related activity;
- contributing to the planning process, including the development of the Action Plan; and
- attending Incident Management Team (IMT) meetings and keeping the Controller and wider IMT informed of the operational aspects of response.

4.8.2 Sub-functions

The specific sub-functions of Operations will depend on the type and scale of the incident and the objectives of the Controller. It is essential that the Operations function remains flexible and adaptable to the needs of the response. To ensure this adaptability, Operations should consider a number of potential sub-functions and work with the Controller to determine the most appropriate way to establish and maintain a functional structure. This may involve organising the function along thematic (e.g. Public Health for an infectious disease response, or Investigations for a terrorism response) and/or spatial boundaries (e.g. divisions or zones, as determined by agency procedures and arrangements).

Action Plan Execution

Action Plan execution coordinates the implementation of the Action Plan by ensuring effective planning and assignment of tasks to the respective response elements (within delegation of authority).

Action Plan Execution is responsible for:

- maintaining a register that specifies detailed tasking, and making arrangements to monitor and ensure execution of the requested tasking outcomes;
- consulting and coordinating with the Logistics function and support agencies to identify and prioritise available resources and maintain optimum resource levels;
- receiving resource requests from other organisations or functions, comparing these against available resources and Action Plan objectives and either releasing an available resource or passing the request to Logistics;
- escalating prioritisation and critical resource decisions to the Control function as required; and
- actively executing, managing and overseeing the Action Plan.

Field Staff Management

The Field Staff Management sub-function provides a conduit between the Coordination Centre and any field staff and maintains oversight of field staff's needs and ensures they are being met.

Working directly with field staff, Field Staff Management ensures that effective and regular communications are maintained between the deploying Coordination Centre and field staff. During these communications, the Field Staff Management sub-function should ensure that:

- any field staff issues are being managed (including health and safety);
- field staff's logistical requirements are being met by the appropriate functions; and
- taskings and responsibilities are appropriate and understood.

Volunteer Coordination

Volunteer Coordination is responsible for establishing a connection with established and spontaneous volunteer and emerging groups, to ensure that their efforts and contributions are effectively targeted, utilised and coordinated with the rest of the response. Key activities may include travelling to volunteer bases in the community to determine needs, goals and capabilities, and communicating these to Planning and other functions as required. Volunteer Coordination must work closely with the Safety function to ensure that the risks associated with volunteer participation in a response are understood, integrated into decision making, and mitigated.

Investigations

This sub-function applies in incidents when investigations are required. Investigations are processes that are undertaken to establish avenues of inquiry, collect evidence, use intelligence and require the management of people involved in the investigation. Controllers should consider early which organisation is best placed to undertake any required investigations, liaise with that organisation promptly and establish the Investigations sub-function. For example, if a criminal act is suspected, ensure prompt liaison with New Zealand Police, whose role it is to determine any criminal liability. Usually the investigation will continue after the response phase is completed. In incidents requiring complex investigations, the Controller may determine that Investigations needs to be a standalone function with its own IMT representative.

Lifeline Utilities Coordination

Lifeline Utilities Coordination is responsible for communicating with lifeline utilities to ensure that the status of impacted services, and the support required by lifeline utilities for infrastructure recovery, is communicated to the other functions. This sub-function also ensures that lifeline utilities are aware of response priorities for service restorations.

Key activities may include:

- regular contact with lifeline utilities to receive reports and status updates;
- assessing the impacts due to loss of service/infrastructure; and
- communicating Action Plans and the Controller's priorities to lifeline utilities.

In more complex incidents, the Controller may determine that Lifeline Utilities Coordination needs to be a standalone function with its own IMT representative. In smaller incidents, relevant lifeline utilities may be represented by a Liaison Officers or a single Lifeline Utilities Coordinator representing one or more clusters.

Lifeline Utilities Coordination is the responsibility of civil defence emergency management (CDEM) at the local, regional and national levels. The lead agency Controller may access lifeline utilities coordination arrangements through CDEM.

Support Agency Representatives Coordination

Support Agency Representatives Coordination supports communication between the lead agency, support agencies and Sector Coordinating Entities (SCEs). Staff assigned with Support Agency

Representation Coordination are referred to as Liaison officers. They ensure support agency representatives are accommodated, coordinated, and integrated.

Support agency representatives

Support agency representatives need workable communications with their own organisations, preferably telephone or email, or any other relevant information management system. They must be familiar with the Action Plan and the key appointments and functions within the response structure.

Support agency representatives pass information and tasks between the lead Coordination Centre and support agencies. They provide advice on their organisation's capabilities and intentions, contribute to the action planning process, ensure progress of tasks and help to resolve problems. They do not usually have authority to make decisions or commit resources, but have access to personnel at their organisation with this authority.

Support agency representatives may be representatives from government agencies, the private sector such as lifeline utilities, NGOs and community/volunteer organisations. They can either be based at the lead Coordination Centre or at the support agency. In the latter case, they should attend the lead Coordination Centre for the purpose of meetings and briefings. At the incident level, support agency representatives usually report directly to the Controller.

When appropriate, the lead agency may also establish a representative at key support agencies' Coordination Centres.

International Assistance

This sub-function only applies in large-scale incidents when international assistance is involved. It is always managed at the national level and is responsible for the coordination, integration and management of international support to a response. It also maintains a view over individual organisations' direct connections with international partner agencies in supporting their response efforts, to ensure a holistic and system-wide approach to international assistance.

4.9 Logistics

LOGISTICS

- Supply
- Transport
- Finance
- Information Technology (IT)
- Communications
- Facilities
- Catering
- Personnel
- Administration and Document Registration
- Health and Wellbeing

Figure 11: Logistics

Logistics provides and tracks resources to support the response and the affected communities, and provides resource advice to other CIMS functions. Resources may include personnel, equipment, supplies, services, facilities, and finances.

4.9.1 Responsibilities

Logistics is responsible for:

- setting up and maintaining the Coordination Centre;
- receiving authorised resource requests and requesting or procuring the resources and facilities; receiving, storing, maintaining and issuing resources; and collating and matching offers of assistance;
- notifying response elements of available resources;
- identifying and managing critical resources;
- tracking resource use and financial expenditure;
- activating and operating any required Assembly Areas;
- arranging transport;
- arranging catering, goods and accommodation for both response staff (in coordination with the Operations function) and for affected people, communities, and animals, including animals (in cooperation with the Welfare function);
- establishing and maintaining communications;
- establishing and maintaining information technology networks;
- providing record-keeping and administrative support;
- advising the Controller and the IMT of logistics issues and critical resource levels;

- contributing to the planning process, including the development of the Action Plan; and
- attending Incident Management Team (IMT) meetings and keeping the Controller and wider IMT informed of the Logistics aspects of the response.

4.9.2 Financial delegations

It is important that the Logistics Manager has appropriate financial delegation to be able to keep the operation going. This pertains in particular to expenses related to the Coordination Centre and response staff (i.e. catering and travel), but it is appropriate that the Controller approves expenses related to new or unusual resources.

4.9.3 Sub-functions

All other CIMS functions are generally dependent on Logistics in order to perform their activities, which will normally rely on the ready availability and pre-positioning of resources. Therefore, Logistics must normally operate in advance of the other functions to ensure that those functions can perform their roles unhindered by resource challenges.

Depending on the scale and complexity of the incident, Logistics may arrange its responsibilities into the following sub-functions:

Supply

Supply is responsible for receiving and recording the resource requests from Operations, procuring resources, tracking offers of assistance, and providing supply information to Planning. Supply at an Assembly Area is responsible for receipt, storage, inventory tracking and loading of supplies and equipment.

Transport

Transport is responsible for arranging or providing transport and, where applicable, for equipment maintenance. Transport works with Supply to transport resources, including people, to where they are needed.

Finance

Finance tracks costs, pays accounts and invoices, provides authorised cash advances, and reconciles costs and expenditure. The lead agency's business-as-usual finance systems should be used as much as possible. This is separate to the financial assistance required to meet the needs of affected communities (see Section 4.11).

Information Technology (IT)

Information Technology (IT) is responsible for establishing and maintaining the equipment and information technology networks at the Coordination Centre.

Communications

Communications is responsible for providing input in areas of acquisition, installation and maintenance of communications equipment and the development of the Operational Communications Plan. Communications also receives radio and other messages, logs them and then distributes them to Operations (or if agreed, directly to relevant functions) and sends radio or courier messages on behalf of other functions. Some situations may warrant this sub-function to be part of the Operations function instead of Logistics or, if the event is large enough, it could be a separate function in its own right, documenting incoming and outgoing messages.

Facilities

Facilities is responsible for securing buildings and land for use by response personnel and managing these throughout the response. Facilities assists the Welfare function with securing facilities and accommodation for affected people and animals. Facilities arranges contracts to procure the use of facilities and Supply provides procurement advice and input.

Catering

Catering arranges meals and drinks for response personnel (foodstuffs are ordered by Supply). Catering must be arranged when a response lasts more than six hours or responders are not self-supporting. Catering also works with the Welfare function to arrange catering support for affected people and animals.

Personnel

The Personnel sub-function secures and manages human resources for the Coordination Centre, including rostering, registering, inducting, and training response staff and volunteers.

If the Coordination Centre receives field staff from other organisations / Coordination Centres, the receiving Coordination Centre's Personnel sub-function is responsible for:

- communicating and managing deployment, travel and accommodation arrangements and requesting relevant records (e.g. medical conditions and next of kin), in consultation with the deploying Coordination Centre's Field Staff Management sub-function (in Operations);
- registering field staff on arrival and ensuring they attend any orientation briefings or inductions;
- tasking field staff to their assigned function; and
- ensuring handover, demobilisation (see Appendix E and Appendix F) and return travel arrangements, are completed

If a request for staff is received from another Coordination Centre, the Personnel sub-function may also need to source these staff. If staff are deployed, Personnel will notify the Field Staff Management sub-function (in Operations), who will be the field staff's primary point of contact while deployed. On return from their deployment, Personnel should also complete a follow-up to ensure there are no health and wellbeing issues.

Administration and Document Registration

Administration is responsible for arranging and managing clerical support, cleaning, maintenance, pool vehicles, and record-keeping of key response documents. Administration may also be required at other locations during the response such as at Assembly and Staging Areas.

Document Registration establishes and maintains a coordination point for incoming and outgoing formal documents such as Action Plans, Situation Reports (SitReps) and Minutes. This ensures that:

- incoming formal documents are appropriately registered, noted and distributed across the response structure; and
- outgoing formal documents are appropriately registered and disseminated internally and externally.

Document Registration is also the central coordination point for contact information, e.g. names of key agency personnel, telephone numbers, email addresses, radio channels and call signs, and location addresses and coordinates.

Other functions and sub-functions can still directly receive, send and register operational documents and information that relate to their specific functions.

Health and Wellbeing

Health and Wellbeing is responsible for the planning and provision of health and wellbeing support for response staff. This is separate to the health needs of the affected people and animals, which falls under the Welfare function. Health and wellbeing collaborates closely with the Safety function of the response and may be combined with it.

The structure of the Logistics function should be determined depending on the resource demands of the response. If the response is complex and/or sizeable, it may be useful to split the Logistics team into two smaller groups, one with an internal focus on the Coordination Centre, the other with an external focus on the response elements outside the Coordination Centre. The Logistics Manager would supervise both teams.

The maintenance of vehicles and equipment is not included as a sub-function as it is usually addressed directly by the agency responsible for the equipment. Planning and provision of maintenance support is usually done by Supply (for stores and equipment), Transport (for vehicles) and Facilities (for buildings).

4.10 Public Information Management

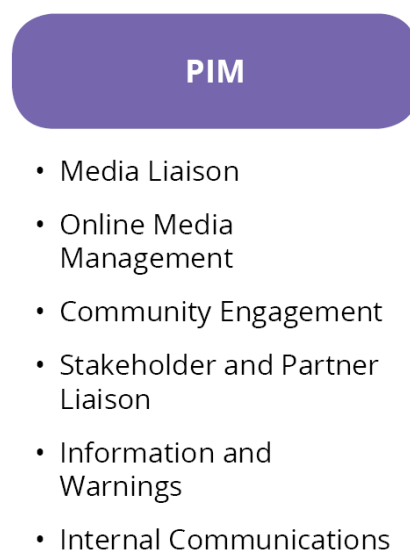


Figure 12: Public Information Management

Public Information Management (PIM) primarily provides information and safety messages to the public. PIM is responsible for informing the public about the incident and the response (including actions they need to take), media liaison and monitoring, community engagement, stakeholder liaison, giving and receiving information via social media channels, and internal communication. On the Controller's direction, PIM also issues warnings and advisories.

PIM personnel have a close link with Strategic Communication personnel (when activated) to help ensure Governance and elected officials are appropriately supported. They also ensure that messages are consistent and that priorities are aligned across all levels of response.

4.10.1 Responsibilities

PIM is responsible for:

- preparing and sharing clear, accurate, frequent, relevant, and timely information directly with the impacted communities and the wider public (via social media, public meetings, handouts, etc.) or via the media and trusted third parties — the content of official information is generated by official processes and approved by the Controller;
- identifying key partners, including iwi and key stakeholders such as elected officials and the business community, and ensuring they are briefed and provided with up-to-date, relevant information, as well as providing a consistent point of contact within the Coordination Centre;
- liaising with the community, including arranging regular community meetings and information sessions and providing supporting material (e.g. handouts, visual aids);
- ensuring online channels, community-led centres, i-Sites, call centres, helplines, reception personnel and Civil Defence Centres (when activated) are updated frequently to have current public information and key messages;

- monitoring the public and media reactions and passing information to Intelligence and other relevant CIMS functions;
- coordinating with other organisations' PIM functions to ensure consistent and coordinated messages and to avoid duplication;
- working with the media, including arrangements for media visits, media conferences and accreditation;
- liaising with VIPs and their personnel about site visits;
- supporting other functions — particularly Welfare and Operations — to ensure that all staff involved in public-facing activities (e.g. those working at cordons, in Civil Defence Centres or in community-led centres) have up-to-date, relevant information to share with the public and that information related to the welfare of affected individuals, families/whānau and communities, including animals, is up to date and accurate;
- providing photography/videography to assist with communicating what has happened and what is being done in the response to assist impacted communities and why. Images and footage are used in online channels, provided to news media and illustrate community and stakeholder briefings;
- preparing speaking points and preparing interview locations;
- liaising with Strategic Communications to ensure consistent public information is given at all levels of the response and Governance;
- contributing to the planning process, including the development of the Action Plan; and
- attending Incident Management Team (IMT) meetings and keeping the Controller and wider IMT informed of the PIM aspects of the response.

The lead agency is responsible for developing key messages and coordinating with other organisations' PIM functions to ensure consistency. A multi-organisation PIM group may be required to coordinate public information during an extensive or extended response.

PIM priorities and intended actions need to be outlined in all Action Plans. A PIM response plan (or appendix to the Action Plan) is usually required to ensure that PIM activity is coordinated.

Support agencies' PIM personnel must support the lead agency by:

- aligning their messages with the lead agency's;
- sharing the lead agency's messages;
- restricting their own messages to their field of expertise;
- referring important or potentially controversial media inquiries to the lead agency PIM;
- relaying emerging themes or reoccurring media inquiries to the lead agency PIM; and
- directing spokespeople to the lead agency.

PIM is also responsible for briefing and preparing spokespeople before they engage in media interviews or community and stakeholder meetings. PIM ensures the spokesperson is informed about:

- the audience, including its likely mood;
- key messages to communicate;
- questions they can expect; and
- what the audience already knows.

4.10.2 Sub-functions

Any response triggers a public interest. In the first instance, affected people want to understand the personal impacts, what is being done and what to do in relation to the impact on themselves, and what not to do. In the second instance, those not directly affected will be interested in the response and will want to be informed by news media and other channels. Depending on the scale of the response, PIM must consider and arrange itself to cater for the following sub-functions:

Media Liaison

Media Liaison works with media organisations to distribute key messages through interviews, media releases and media conferences, and monitors media outputs — broadcast, online and print. Media Liaison is responsible for:

- facilitating media access to response sites and personnel, including negotiating pool arrangements where necessary;
- arranging accreditation where there are access restrictions to impacted areas;
- fielding and responding to media requests for information and interviews;
- producing updates and releasing authorised, authenticated information to media;
- briefing spokespeople for media interviews, stand-ups and press conferences, ensuring that the appropriate people are available and that each understands their role and share of messages during the interview/event; and
- logging all media activity including queries, responses, interviews and updates / media releases.

Online Media Management

Online Media Management proactively shares information via social media channels and websites. Online Media Management is responsible for:

- posting information and updates that have been authenticated and authorised for release;
- responding to queries;
- correcting misinformation by pointing back to official sources of information such as websites;
- identifying emerging issues and ‘taking the temperature’ of the community by monitoring threads on both official social media sites and community networks, liaising closely with the Intelligence function to share this information;
- taking or sourcing photographs and video footage to use across all public communications and share with media;

- updating and maintaining websites with current information to create a 'single source of truth' for the emergency response;
- livestreaming media conferences and other events; and
- interviewing response personnel and partners to highlight activities that will increase public confidence in the response.

Community Engagement

Community Engagement carries out two-way communication directly with affected communities in consultation with other functions such as Operations and Welfare. This ensures that those directly impacted by the emergency have clear, accurate, relevant and timely information and enables the Coordination Centre to obtain local knowledge, needs, and intentions so that these are reflected in response and recovery. Community Engagement is responsible for:

- developing a community engagement strategy, determining when, where, who and how to engage;
- scheduling and facilitating community meetings, working with the Logistics function;
- producing collateral for the community such as newsletters, posters and handouts, as well as advertising in media that will reach the impacted community;
- logging issues raised by community members and obtaining responses; and
- advising and working with the Welfare function regarding the needs of affected people and animals, including the development of factsheets to meet information needs.

Stakeholder and Partner Liaison

Stakeholder and Partner Liaison identifies key stakeholders and partners, including local and national elected officials, executives, iwi, businesses and other lead agency staff who aren't directly involved in the response; and ensures they are briefed and provided with up-to-date, relevant information through channels that are appropriate for each stakeholder and partner. Stakeholder and Partner Liaison is responsible for:

- sharing regular updates of authorised, authenticated information, which may be both general in nature and/or tailored to the stakeholder or partner's area of interest;
- facilitating VIP visits by liaising with VIP's staff and other CIMS functions, including the Controller, to ensure appropriate arrangements are made to support the requested itinerary and that all personnel are briefed;
- providing a consistent point of contact within the Coordination Centre and appropriate two-way channels of communication; and
- identifying emerging issues and advising the Controller and other functions about stakeholder and partner needs.

Information and Warnings

Information and Warnings gathers information from other functions to provide tailored information, warnings and advisories (approved by the Controller) to the public. Key sources are the Intelligence, Operations and Welfare functions. These are then normally distributed through Media Liaison, Online Media Management and Community Engagement. Information and Warnings is responsible for creating clear and timely warnings to be issued to target audiences by all available channels.

Internal Communications

Internal Communications ensures that every individual and organisation involved in a response is well-informed of the progress of the response, the Controller's priorities and how they are being given effect, and critical milestones. Internal Communications is responsible for:

- sharing all external communications products with staff and support agencies;
- ensuring copies of all external communications (media releases, stakeholder updates, etc.) are available within the Coordination Centre and are copied to support agencies for their own internal distribution; and
- supporting the Controller with notes for Coordination Centre briefings.

4.11 Welfare

WELFARE

- Needs Assessment
- Welfare Delivery
Coordination

Figure 13: Welfare

The Welfare function is responsible for ensuring planned, coordinated, and effective delivery of welfare services to affected individuals, families/whānau and communities, including animals² (hereafter people and animals) affected by an incident. The welfare of responders is a responsibility of the Logistics function.

The scale, complexity and consequences of an incident dictate the extent of welfare services required.

- At the incident level, these services relate to meeting the immediate needs of the affected people and animals (e.g. providing shelter in a safe place and information about available services).
- In a response where delivery of welfare services requires more significant coordination (e.g. a flood event), the welfare services arrangements in the National Civil Defence Emergency Management Plan Order 2015 may need to be activated in coordination with Civil Defence Emergency Management (CDEM) Groups.

During response, immediate welfare needs should be met as soon as possible. Ongoing and future needs should be identified, assessed, coordinated and met.

Needs may include (but are not limited to):

- food, water, hygiene and clothing;
- medication and other health needs;
- shelter or accommodation;
- psychological first aid and psychosocial³ support;
- care and support for vulnerable people and communities;
- financial assistance (e.g. tax relief or business support);
- veterinary assistance, food, water, rescue, evacuation and/or shelter for affected animals;
- assistance with contacting family/whānau or significant others; and
- timely information about available services.

² Animals are generally considered to be a part of Welfare, especially in relation to companion animals and livestock. However, animals may also be considered to be under Operations during evacuations or in an incident that impacts wildlife, e.g. an oil spill.

³ Psychosocial support involves focusing on physical, psychological and social interventions, as well as enhancing wellbeing and supporting recovery.

Meeting these needs will depend on a variety of influencing factors, including:

- the type, scale and complexity of the incident;
- the location;
- the number of welfare services organisations involved;
- timeframes (from immediate needs to ongoing needs, including into recovery); and
- available resources.

All lead agencies need to consider the consequences of an incident on people and animals and plan accordingly. Because they have established welfare arrangements, this should include engaging with CDEM Groups but may also involve:

- support agencies;
- welfare services organisations (including animal welfare organisations);
- iwi/Māori
- culturally and linguistically diverse (CALD) communities;
- faith-based communities;
- rural communities and primary industry sectors;
- tourism and business sectors;
- embassies and consulates responsible for impacted foreign nationals;
- insurance and financial sectors; and
- relevant community and volunteer groups.

4.11.1 Responsibilities

Welfare is responsible for:

- ensuring the welfare needs of affected people and animals are identified and met through response and into recovery, as appropriate;
- coordinating with other organisations on the provision of welfare services to ensure delivery is integrated, timely and aligned to the needs of people and animals;
- planning, coordinating and integrating welfare activities with other CIMS functions and activities, including Logistics for the establishment of facilities to support affected communities (e.g. Civil Defence Centres and animal welfare shelters);
- providing timely and accurate welfare services information, through Public Information Management (PIM), to affected individuals, families/whānau and communities;
- identifying welfare priorities and providing strategic and operational advice to the Controller;
- contributing to the planning process, including the development of the Action Plan; and

- attending Incident Management Team (IMT) meetings and keeping the Controller and wider IMT informed of the Welfare aspects of the response.

4.11.2 Sub-functions

The specific sub-functions of Welfare will depend on the type, scale and complexity of the incident and the objectives of the Controller. It is essential that the Welfare function remains flexible and adaptable to the needs of the response and provides continuity of care into recovery, in conjunction with other CIMS functions. To ensure adaptability a number of potential sub-functions should be considered and the Welfare Manager should work with the Controller to determine the most appropriate functional structure.

Depending on the type, scale and complexity of the incident, Welfare may arrange its sub-functions into dedicated or combined functions, including (but not limited to):

- Needs Assessment; and
- Welfare Delivery Coordination.

Needs Assessment

Needs assessment is the systematic process of analysing, prioritising and understanding the interdependencies of the identified needs of affected people and animals.

Before welfare services can be delivered, the needs of affected people and animal must be identified and assessed in a timely and coordinated way.

Needs identification involves identifying the immediate and ongoing needs of people and animals affected by an incident to inform response and recovery activities.

Identification of immediate needs can come from:

- requests for assistance or advice on available support for people and animals;
- information received from the Operations function (e.g. during evacuations);
- information gathered by the PIM function (e.g. on social media or through community engagement);
- requests received by call centres and through welfare facilities;
- coordinated community outreach activities;
- knowledge and experience from previous events;
- information received from welfare services organisations; and
- the Intelligence function to analyse ongoing and emerging needs and trends based on community, demographic, cultural and human factors, response decisions, or changing hazards circumstances.

When assessing needs, it is important that the Welfare function understands the diverse nature and vulnerabilities of individuals, families/whānau and communities, and their animals.

Welfare Delivery Coordination

This sub-function ensures appropriate welfare services organisations and community groups have the capability and capacity to address the specific welfare needs. Welfare Delivery Coordination works with the other CIMS functions, welfare services organisations and communities to ensure that welfare activities and services are appropriate, timely, coordinated, and integrated to achieve maximum effectiveness and efficiency.

Welfare Delivery Coordination determines options to deliver prioritised and accessible welfare services that meet assessed needs. Welfare Delivery Coordination is responsible for:

- ensuring effective planning, coordination, delivery and monitoring of required welfare services between all functions and welfare services organisations;
- coordinating with the Operations function for delivery of welfare support or provision of support to welfare organisations;
- coordinating with the Logistics function to source welfare goods and resources, and to establish response facilities for the community, including animals;
- coordinating with welfare services organisations and Public Information Management (PIM) to provide information to affected individuals, families/whānau and communities;
- coordinating with Operations (Volunteer Coordination sub-function) and PIM (Community Engagement sub-function) to understand, integrate and align with the community response; and
- ensuring the needs of affected people and animals have been met appropriately.

In a larger response where comprehensive welfare services delivery is required, such as establishing welfare facilities, provision of welfare support for people sheltering in place, welfare support at community-led centres, or providing welfare support for people evacuated from another area, the Welfare Manager may determine that a Welfare Facility sub-function is required to manage and coordinate the delivery of welfare services.

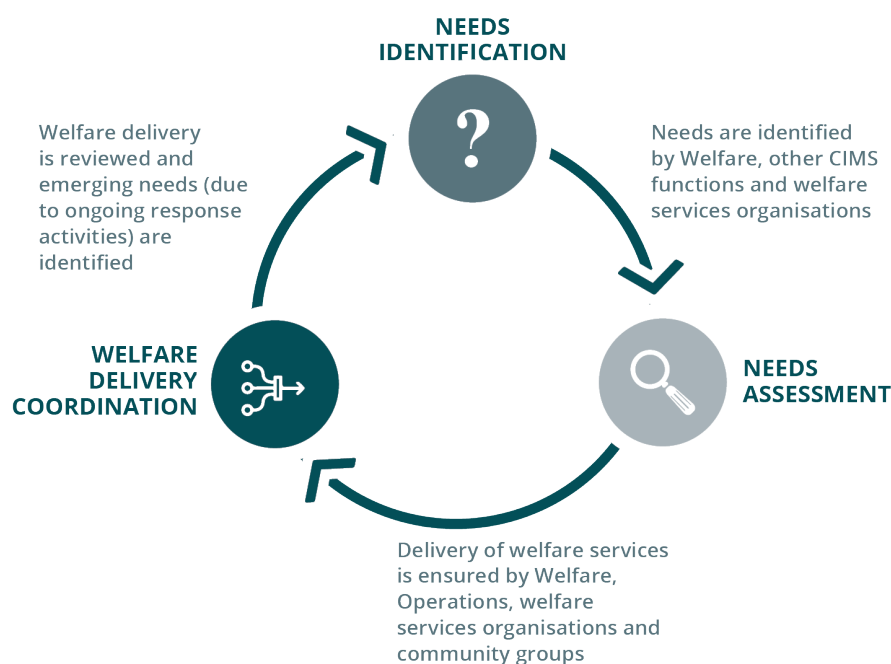


Figure 14: The Welfare cycle

A holistic and coordinated approach

Meeting the needs of affected people and animals requires a holistic approach and the recognition that their needs may be met through services provided by a number of different welfare services organisations and community groups.

In larger responses, the Welfare function involves a number of welfare services organisations, which will require strong coordination to avoid duplications and overlaps in the identification, assessment and delivery of welfare services.

The Welfare function may need to form clusters to ensure there is a manageable span of control. Each cluster will have a lead that is responsible for that cluster and reports to the Welfare Manager.

Clusters may include the welfare services arrangements that are articulated in the National Civil Defence Emergency Management Plan Order 2015 and that are coordinated by the National Welfare Coordination Group and Welfare Coordination Groups. These services include:

- registration and needs assessment;
- inquiry;
- care and protection services for children and young people;
- psychosocial support;
- household goods and services;
- financial assistance;
- shelter and accommodation; and
- animal welfare.

The lead agency Controller may access pre-arranged emergency welfare services. Emergency welfare services arrangements are coordinated by CDEM Groups and/or the Ministry of Civil Defence & Emergency Management (MCDEM).

4.12 Recovery (in Response)

For affected communities, the process of recovering and regaining a sense of usual daily functioning starts at the beginning of a response.

Like response, recovery is scalable. Coordination arrangements for recovery are not one-size-fits-all, as they need to be based on the actual consequences of the relevant incident. Organisations should consider possible consequences that may need to be addressed in recovery, and define scalable and adaptable coordination arrangements needed. The arrangements and scale of recovery need to be built on the needs of the affected people and animals. These needs will change over time, so the recovery approach needs to be able to change, downsize, merge, grow, and be reorganised when and where needed.

Recovery is activated in response to consider consequences of the incident on communities. Efforts are made to anticipate, plan and prepare for addressing consequences of the incident on a community or part of a community — whether a geographical community or a community of interest.

4.12.1 Objectives

Recovery ensures that the affected communities, and how they can be supported to recover from an incident, are considered and incorporated in response. It also ensures that decisions or actions (or lack there-of) made during response consider any implications for recovery.

Coordinating and integrating recovery with response means that:

- the consequences for people and animals in the short-, medium- and long-term will be better understood;
- recovery management considerations will be integrated in response decisions and actions will minimise the negative impact the response can have on recovery;
- staff resources can be managed and allocated as effectively and efficiently as possible;
- there will be a planned, managed, and coordinated transition from response to recovery management arrangements;
- recovery activities and priorities will be identified and aligned with response priorities;
- recovery planning and coordination will be initiated as early as possible and response and recovery organisational structures will be aligned where possible; and
- engagement with key stakeholders and partners across the affected area will be initiated as early as possible.

4.12.2 Responsibilities

Recovery is responsible for:

- if appropriate, appointing a Recovery Manager and establishing core recovery team resources;
- maintaining situational awareness and understanding from a Recovery perspective;
- beginning initial recovery planning, including identifying what information gaps exist, and ongoing recovery arrangements including the recovery team and office (if necessary), financial arrangements, and other resources and facilities;

- discussing outstanding and ongoing needs of people and animals with the Welfare function;
- discussing key recovery messages with Public Information Management (PIM) to ensure that messages are consistent priorities are aligned across all levels of response and into recovery, ensuring that PIM are aware that public information management will need to continue into recovery;
- establishing and maintaining liaison and communications with key organisations and community leaders in affected areas, drawing on existing relationships and plans developed prior to the emergency and leveraging or aligning with the Operations and PIM functions. Establishing a key contact list for ongoing liaison with those involved in response in recovery;
- communicating with Governance (on recovery matters);
- holding briefings with the core recovery team (if established) to discuss consequences, new information and gaps, risks, response decisions and activities and recovery tasks;
- working with the Controller and Planning to plan and manage the transition from response to recovery; and
- attending Incident Management Team (IMT) meetings and keeping the Controller and wider IMT informed of the Recovery aspects of the response.

4.12.3 Transitioning to recovery

Moving from response to recovery signals a shift in intent, objectives and priorities, including considering medium- and long-term priorities. The move must be carefully planned during response, managed and communicated as it formally transitions coordination and accountability from response to recovery leadership and wraps up the response phase. Both the Controller and Recovery Manager have leadership responsibilities during the shift from response to recovery to ensure that the process is seamless both from an internal organisational and community perspective and communicated. Using the holistic and integrated response and recovery approach (see Section 2.8) will assist integrated response and recovery planning and a seamless transition. The actions to move from response to recovery are given in Table 9.

Action required	Lead	Support
Complete a Response to Recovery Transition Report	Controller	Recovery Manager
Ensure that agencies, organisations and groups with a role in recovery are committed to their continuing role.	Recovery Manager	Controller
Prepare a Recovery Action Plan	Recovery Manager	Controller
Prepare for and conduct a Transition Briefing	Controller	Recovery Manager
Work with PIM and Strategic Communications to prepare and hold media briefings and communications, and ensure messages are consistent and accurate across all agencies.	Controller	Recovery Manager

Table 9: Actions required to move from response to recovery

Section 5 Application of CIMS

CIMS can be scaled to manage any type or size of incident. Controllers may delegate functions to individual personnel or teams on a scale that reflects the requirements of the incident. A protracted response may scale up and down several times depending on the nature of the incident and the required response.

Decisions to scale the response are based on the following considerations (not exhaustive):

- Safety of response personnel, the affected people and communities, animals and property;
- Size and complexity of the incident;
- Span of control;
- Recommendation or agreement among the Incident Management Team (IMT);
- Achieving the response objectives; or
- Legislative provisions.

5.1 Incident level response

5.1.1 Incident level response: Single agency

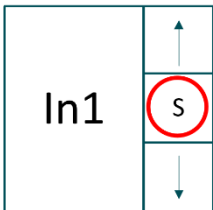
In a single agency response at the Incident level, the personnel and resources come from one agency, so command and control are relatively simple — there is one line of command. Minimal facilities are needed, and the Incident Control Point (ICP) could just be a single vehicle.

In this response, the most senior responder first on the scene is the Incident Controller. They have responsibility for all the CIMS functions required for the response. If the lead agency deems it appropriate, this initial Incident Controller may be replaced later by a more senior, experienced or qualified officer.

The Incident Controller must consider all of the CIMS functions and perform those that apply. For example, there may be people requiring assistance, media present or hazards to manage.

As more personnel become available, the Incident Controller may delegate CIMS functions and establish an Incident Management Team (IMT), while usually retaining responsibility for the Public Information Management and Safety functions. Some functions may be combined, such as Planning and Intelligence, and Operations and Welfare. The combined functions may separate as the incident progresses.

Example: Incident level response involving a single organisation (vehicle accident)

Situation	An accident involving four vehicles has occurred on an urban highway during a peak-traffic period.
Consequences and impacts	- There are no injuries or fire. - One lane is blocked — traffic is congesting fast and requires direction.
Resources	- Two police vehicles have been deployed to manage the incident. - A tow truck is required.
Public, political and media interest	- Public notices to expect delays have been published on social media and overhead road signs. - A television crew have arrived on the scene and wants an interview about the congestion for the early evening news. - Political interest is unlikely.
Response and recovery characteristics	- The response is considered routine police work and is managed in accordance with standard procedures. - The Incident Controller reports back to the Police communications centre, which performs a Governance role.
Incident classification	The incident is classified In1 and stable. 

In this example, New Zealand Police is the lead agency and they manage the incident without support from other emergency services or organisations. The first police officer to arrive assumes the roles of Incident Controller and manages all the relevant CIMS functions. Following assessment of the situation, the Incident Controller requests that the Police communications centre dispatch another unit as three staff are required to manage the incident. The Incident Controller retains the roles of Operations, Intelligence, Planning and PIM, while delegating the Safety function to another officer, who is responsible for securing the scene and directing traffic flow, and the Logistics function to a third officer, who is responsible for clearing the affected vehicles. Although there are welfare considerations, there is no need to activate the Welfare function.

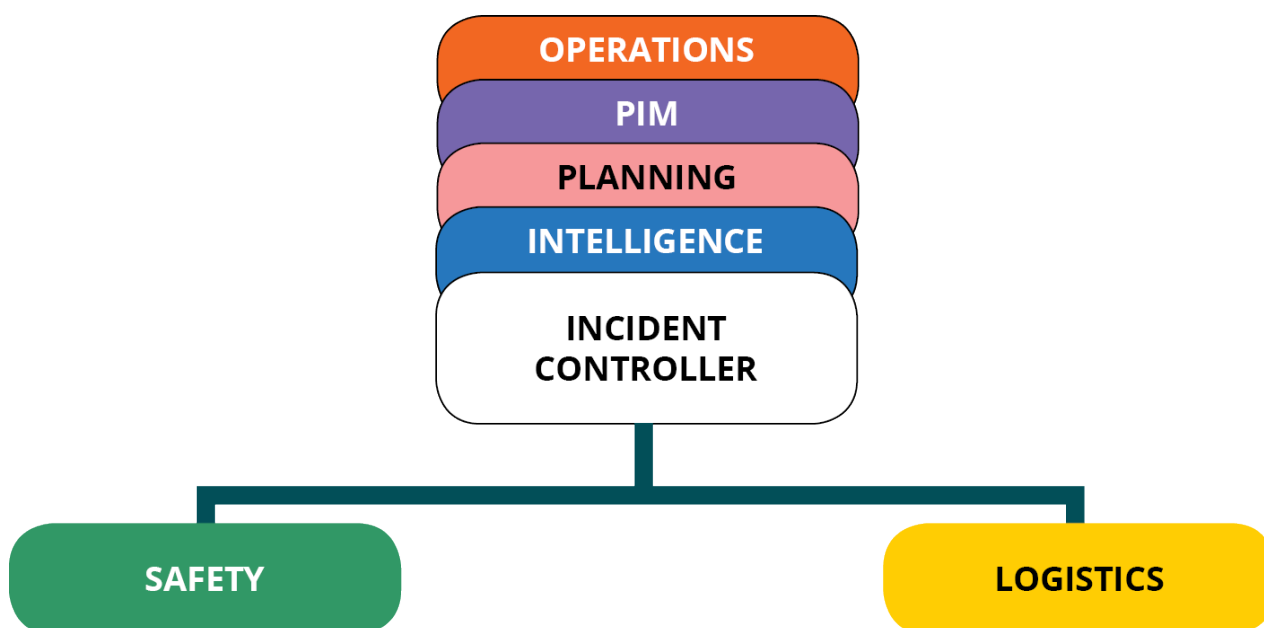
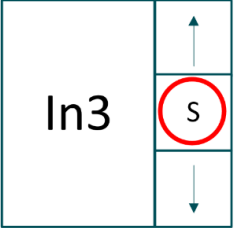


Figure 15: Incident level response — single agency (vehicle accident)

Example: Incident level response involving a single organisation (business disruption)

Situation	- An organisation's servers and networked computers have been hacked and the data has been encrypted and is inaccessible. - Programmes and systems that rely on the internal network or internet are impacted. - A weekly offsite backup will need to be restored, but this will take 2–3 days, and then another 1–2 days to check the backup.
Consequences and impacts	- Customer/stakeholder information is inaccessible. Customers/stakeholders cannot be contacted directly and all outstanding deadlines are impacted. - Communication is limited as email and landline calls are not available. - There will be loss of revenue and a potential risk to the organisation's reputation. - The payroll system is affected as electronic personnel files are inaccessible.
Resources	- Normal staffing levels are available. - Third-party IT contractors are assisting with diagnosis and recovery. CERT NZ has been contacted for advice and support. - Additional equipment, systems and personnel need to be procured.

Public, political and media interest	• The organisation's Board has been notified. • Media interest is likely and is being prepared for. • Political interest is possible.
Response and recovery characteristics	• The entire organisation is impacted. • All business units have activated their business continuity plans and are using workarounds to limit the impacts and consequences on work and staff. • An Incident Management Team is coordinating the response.
Incident classification	• The incident is classified In3 and stable. 

Given the severity of the incident to the organisation (e.g. impact to customers/stakeholders, loss of revenue, reputation risk, and potential duration), an Incident Management Team has been activated with a senior manager as the Controller. The Controller will provide direction across the organisation and business units / teams.

All business units / teams contribute to the planning process to ensure the consequences of response decisions and tasks in the Action Plan are understood and considered.

The Operations function is managed by the IT department. The Intelligence function and Technical Advisors are combined with Operations as their information would be relayed to IT anyway in this situation.

The Personnel sub-function of Logistics needs to engage with the union as payroll is impacted. The Health and Wellbeing sub-function will also work closely with the union as work hours are also affected and the incident may cause anxiety for staff.

The Public Information Management (PIM) function is coordinating communications with both external stakeholders (such as customers and the media) and staff. Strategic Communications complements the PIM function through communications support for senior management and the Board.

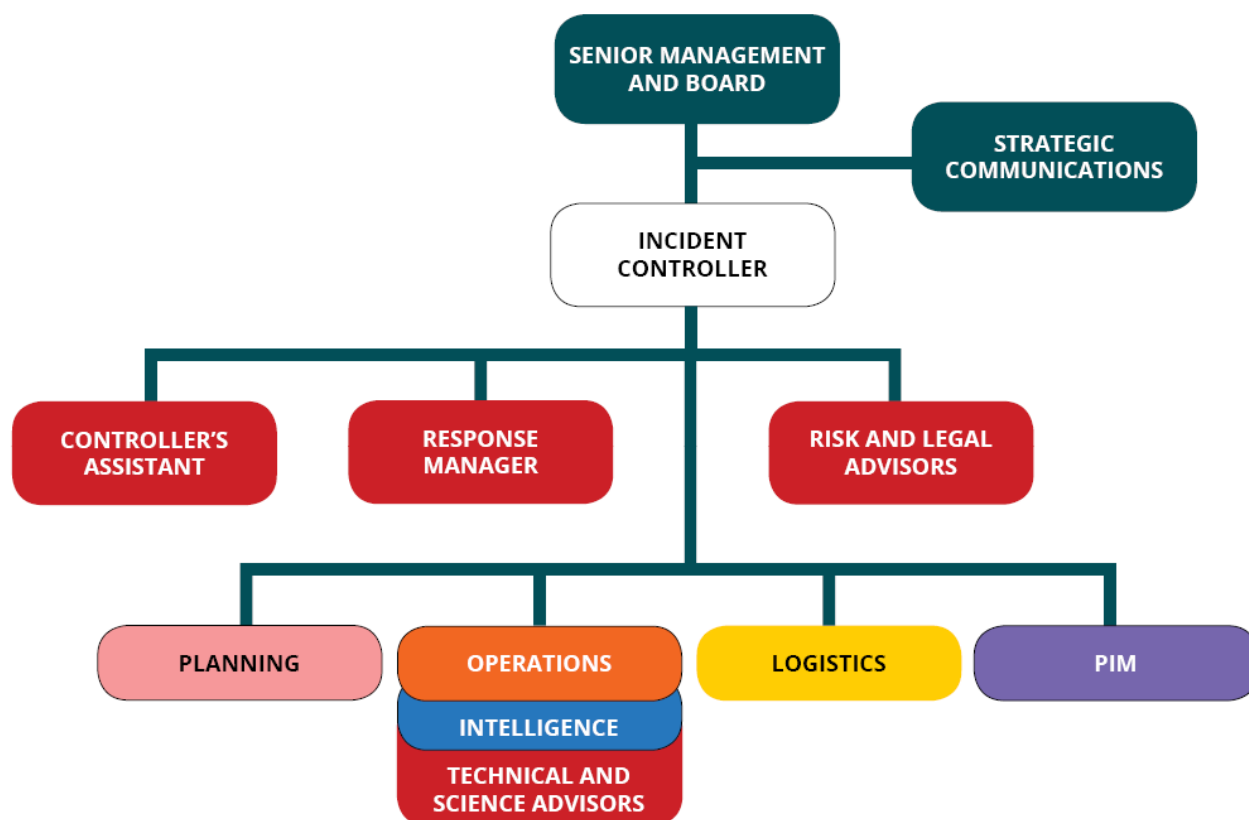


Figure 16: Incident level response — single agency (business disruption)

5.1.2 Incident level response: Multiple organisations

In a multi-agency response at the incident level, the management structure expands in relation to the scale and complexity of the response. Incident Control is likely to change from the most senior person on the scene to a more senior official, or to the lead agency — taking into account legislative mandates and experience.

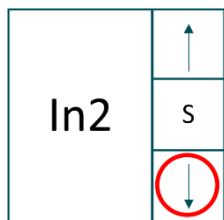
The Incident Controller is likely to delegate most or all of the CIMS functions — some functions may be combined depending on the scale and complexity of the event.

The Incident Controller, supported by the Incident Management Team (IMT), is responsible for directing the overall response activities across all responding organisations. This includes tasking and coordinating support agencies, who action those tasks within their own command structures.

The Incident Controller confirms their authority over support agency response elements if there is no pre-existing understanding.

Support agency representatives should be present at the Incident Control Point (ICP) so that their specialist knowledge is accessible and their organisations' requirements and resources can be incorporated on an ongoing basis. This also gives the ICP more capacity to cope with the expanded scope and workload. These (or more senior) support agency representatives should be part of the IMT.

Example: Incident level response involving multiple organisations

Situation	A 111 call has been made from an industrial complex where people have complained of a strong odour coming from a tank.
Consequences and impacts	- Around 20 people are complaining of coughing and feeling short of breath. - Potential downwind risks have been eliminated.
Resources	- Emergency services involved in the response are: - Fire and Emergency New Zealand, and for the hazardous material response, HAZMAT - Ambulance/District Health Board (DHB) service to treat casualties, and - New Zealand Police to help cordon and contain the incident site and manage any potential crime scene concerns. - The Institute of Environmental Science and Research (ESR) and Public Health teams may also be involved.
Public, political and media interest	- There is local and regional media coverage. - Media have requested an interview with the Incident Controller.
Response and recovery characteristics	- The potential health risk is considered serious, so containment is urgent. - A number of organisations are involved and more may become involved. They are considered familiar with tasks, procedures and each other. - The area of impact is relatively small and there is no downwind risk. However, the community in the immediate vicinity will likely have to be evacuated resulting in limited welfare needs. - Minimal recovery effort will be needed.
Incident classification	The incident is classified In2 de-escalating to In1. 

In this example, the incident is managed at the incident level and no other response levels are involved. The Incident Controller operates from the ICP that is established near the scene. Initial control of the incident falls to Fire and Emergency New Zealand, as the lead agency, until the potential HAZMAT incident is isolated and contained.

The Ambulance team, in conjunction with Fire and Emergency New Zealand, is tasked with triaging/caring for victims and Ambulance will transport those exposed to the unknown substance to hospital. The staff involved are under the command of their own managers, albeit working with Fire and Emergency New

Zealand to achieve the Incident Controller's response objectives. Ambulance reports back to the Incident Controller.

The New Zealand Police, in consultation with Fire and Emergency New Zealand and Ambulance, is tasked with cordoning and containing the affected area. Police staff tasked with executing this are under the command of their own managers and the method for achieving the task is at their discretion. New Zealand Police reports back to the Incident Controller on the nature and management of the cordon.

Considering the scale and complexity of the incident, the Planning and the Intelligence functions are likely to be structured as a combined function, while the extent of the Welfare dimension is such that it can be managed by Operations.

Once the HAZMAT incident has been contained and/or the hazard eliminated, the scene transitions to a crime scene. As the new lead agency, control then transitions to the New Zealand Police, while the original Fire and Emergency New Zealand Controller ensures recovery arrangements are in place.

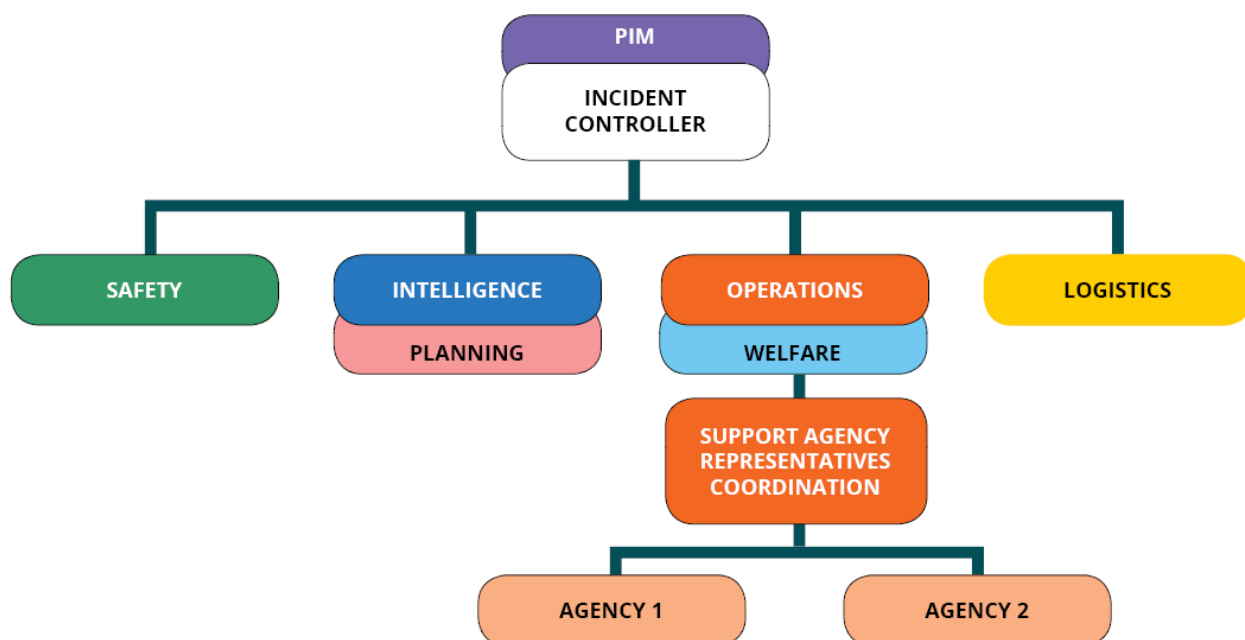


Figure 17: Incident level response — multi-organisation

The structure is similar to the one for a single agency incident level response, except that Operations is likely to be tasking support agencies and the Support Agency Representatives Coordination sub-function is activated.

5.2 Local or regional level response

A local or regional level response is typically activated when one or more of the following conditions are met:

- offsite coordination and support is required;
- there are several incident level responses at different sites and local or regional level coordination is necessary;
- there is a significant community impact;
- it is requested by the emergency services because the level of coordination or resources required is best managed from a higher level; or
- a state of local emergency has been declared.

At the local level, the Local Controller operates from a local Emergency Operations Centre (EOC) and needs to:

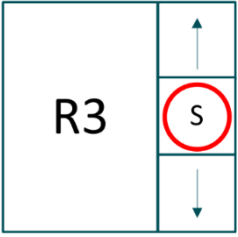
- define their command and control relationship with the Controllers at each Incident Control Point (ICP) (where there is no pre-existing agreement);
- receive a detailed briefing from the Incident Controller(s);
- provide coordination between the ICPs;
- inform ICPs of resources available;
- consider the allocation of resources across ICPs and response elements; and
- ensure communications and support arrangements are activated and communicated across ICPs and support agencies.

At the regional level, the Regional Controller operates from a regional Emergency Coordination Centre (ECC) and needs to do the same as the Local Controller when no local level EOCs are involved, or if EOCs are involved, in relation to Local Controllers and EOCs.

It is likely that all the CIMS functions will be established and that several support agencies will be involved and represented in the IMT. Iwi/Māori representation becomes essential.

Example: Local/regional level response

Situation	• A major rural fire has spread quickly to a 30km perimeter of mainly forest and farmland. • Fire and Emergency New Zealand were initially the lead agency, but a state of local emergency was declared and the regional Civil Defence Emergency Management (CDEM) Group is now the lead agency. • Fire and Emergency New Zealand remain responsible for managing the fire response.
Consequences and impacts	• The areas closest to the fires need to be evacuated and more evacuations will need to take place if the fire spreads further. • Several roads and a state highway are closed. • It is likely that a number of business will have to close down temporarily, which will cause economic impacts. • Consequences will likely include destruction of forestry, pasture and fencing; loss of income; evacuation and stock expenses; animal losses; and ongoing stress and anxiety for people and animals. • There will be impacts on/from waterways; earth works; sediment, smoke and ash impacts on air and water quality; and welfare.
Resources	• There are not enough local resources and all organisations will need additional support. • The response will likely need to be supported by an NCC, which will provide updates to the Minister, national agencies and CDEM Groups and facilitate/coordinate resource requests from the ECC. • Fire and Emergency New Zealand, New Zealand Police, New Zealand Defence Force, Ambulance, Public Health and volunteer response teams are all involved in the response. • The volume of social media will require the ECC to establish a multi-organisation social media team. • A Strategic Communications advisor will need to be appointed to support the Mayor. • The CDEM Group Recovery Manager will need to establish a recovery plan and team, and will work with the Lead Controller to develop a Response to Recovery Transition Report.
Public, political and media interest	• There is significant local and regional media interest expected. • Regular community meetings for the Mayor, Lead Controller and senior agency commanders are being planned for. • Due to the size and location of the fire, significant political interest is expected. • Ministers and other VIPs will likely visit and appropriate planning is required to manage this.

Response and recovery characteristics	• All the emergency services, New Zealand Defence Force, Ministry for Primary Industries, Public Health, Inland Revenue and lifeline utilities are represented with the CDEM Group staff in the ECC. • Fire and Emergency New Zealand, New Zealand Police and the Ministry for Primary Industries have all established Coordination Centres. • The regional Iwi Chairs Group has appointed representatives to the ECC to represent iwi in the area. They attend all IMT meetings and media briefings. • The regional Welfare Coordination Group has been activated to coordinate Welfare activities.
Incident classification	• The incident is classified R3 and stable 

In this example, the incident has become an emergency under the Civil Defence Emergency Management Act and is managed at the regional level from a regional ECC. As there is a local state of emergency, the Regional Controller is the Lead Controller. The Controllers of all the other Coordination Centres as well as the iwi representative meet daily to ensure a coordinated response and to front the media and community meetings jointly. The National Controller is based in Wellington at the NCC and acts in support of the Lead Controller.

A comprehensive CIMS structure is established at the ECC — this includes the activation of the Lifelines Utilities Coordination function due to the roading and potential other lifeline consequences. CIMS structures also support the agency Coordination Centres, and interact with their equivalents at the ECC.

As the fire gets contained and the response scales down after a number of days, the state of local emergency for the region is terminated and a notice of a local transition period is given for the region under the Civil Defence Emergency Management Act 2002. This gives the Recovery Manager the ability to exercise special powers and ensures that the termination of the state of emergency does not leave any gaps in ongoing remedial work and safety activities.

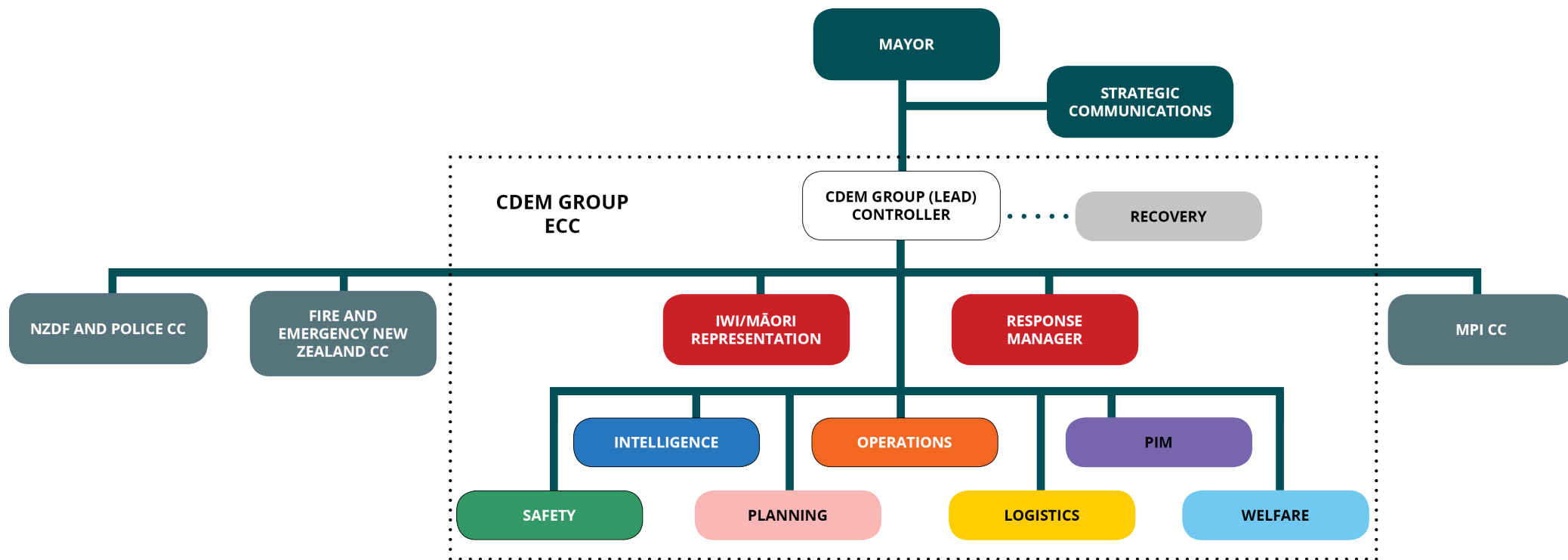


Figure 18: A local/regional level response

5.3 National level response

A national level response provides direction or support for regional levels, while a regional level response provides advice, resource requests and situation updates to the national level to inform national level decision making and other outputs.

National agencies

At the national level, the [Agency] National Controller operates from a National Coordination Centre (NCC) to support or provide direction to an agency's regional response activities, mobilise agency resources and manages the flow of information to and from the National Security System, if activated. When a regional Emergency Coordination Centre (ECC) is activated, the related agency NCC usually also activates. In some cases, national agencies may carry out the coordination and direction at the national level by using business-as-usual arrangements.

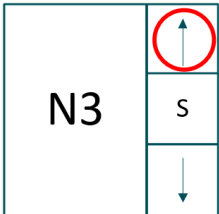
Support agency NCCs command their own resources, inform their own Chief Executives and Ministers, and contribute to the response in line with requests and tasks from the lead agency. Support agencies are normally represented in the lead agency NCC.

All-of-government coordination

To support the National Security System with all-of-government and international response coordination, the government maintains the National Crisis Management Centre (NCMC), a facility to coordinate the all-of-government response, including all-of-government strategic communications and collating information for all-of-government use. The lead agency usually supplies the key appointments for the NCMC, based on CIMS. The lead agency is supported by other relevant support agencies, some of whom may also have suitable personnel for specific appointments in the NCMC. Relevant industry groups and NGOs may also be represented in the NCMC.

Example: National level response

Situation	• A series of threats have been received against the dairy industry. The threats imply that cows will be poisoned with a dangerous strain of anthrax. • Unexpected cow deaths have occurred at a number of dairy farms across New Zealand. Initial tests indicate anthrax as the cause and investigation indicates the anthrax was maliciously introduced into the cattle water supply. There are no human cases. • A State of Biosecurity Emergency has been declared under the Biosecurity Act 1993 and response plans have been activated.
-----------	---

Consequences and impacts	- Because the dairy industry is New Zealand's single largest export industry, communities; businesses; the economy; and most New Zealanders will be directly or indirectly affected. - Overseas markets have closed to New Zealand dairy products, impacting the country's reputation and other exports. - Some farmland will remain contaminated for many years.
Resources	- The Ministry for Primary Industries (MPI) is the lead agency and a number of support agencies are also involved. - Many government agencies have activated their NCCs. Regional ECCs and local EOCs are also activated. - The National Security System and the NCMC are activated to coordinate the all-of-government response. - The response is also supported by industry, international assistance and community-led action.
Public, political and media interest	- There is major public and political interest in the event, including international interest. - The MPI National Controller, Chief Executive, Ministers and the Prime Minister have all had interview requests.
Response and recovery characteristics	- The response and recovery effort will require significant and long-term resourcing that is beyond the capacity of current government structures. - The event will have a significant impact on trade and the economy, as well as on welfare, for many years.
Incident classification	The incident is classified N3 escalating to N4.  The diagram shows a large box labeled 'N3' on the left. To its right is a vertical stack of three boxes. The top box contains an upward-pointing arrow and is circled in red. The middle box contains the letter 'S'. The bottom box contains a downward-pointing arrow.

In this example, the response is managed at the community, incident, local, regional and national levels. The scale of the incident dictates that it is necessary to have Control functions established at all levels of response. The MPI National Controller is the Lead Controller and reports to ODESC and relevant Cabinet committees as required.

The response involves multiple agencies and stakeholders at all levels, including emergency services, government departments, lifeline utilities, business groups, stock and landowners.

Strategic Communications is critical given the economic and international consequences. This is coordinated from the NCMC in close association with all functions and agencies/organisations to ensure consistent messaging. Similarly, the Government will require a dedicated and coordinated Policy approach. This will also likely be established in the NCMC.

If the powers in the Biosecurity Act 1993 are insufficient to manage all consequences, the Government may decide to declare a state of national emergency under the Civil Defence Emergency Management Act 2002 so that maximum powers and resources can be used. In that case the Ministry of Civil Defence & Emergency Management (MCDEM) would become the lead agency.

In a response of this extent, additional structures may be necessary to manage the scale of activities required. The potential structure outlined here includes work streams to achieve manageable units, according to logical groupings of responsibilities and activities. CIMS is applied within and across these work streams.

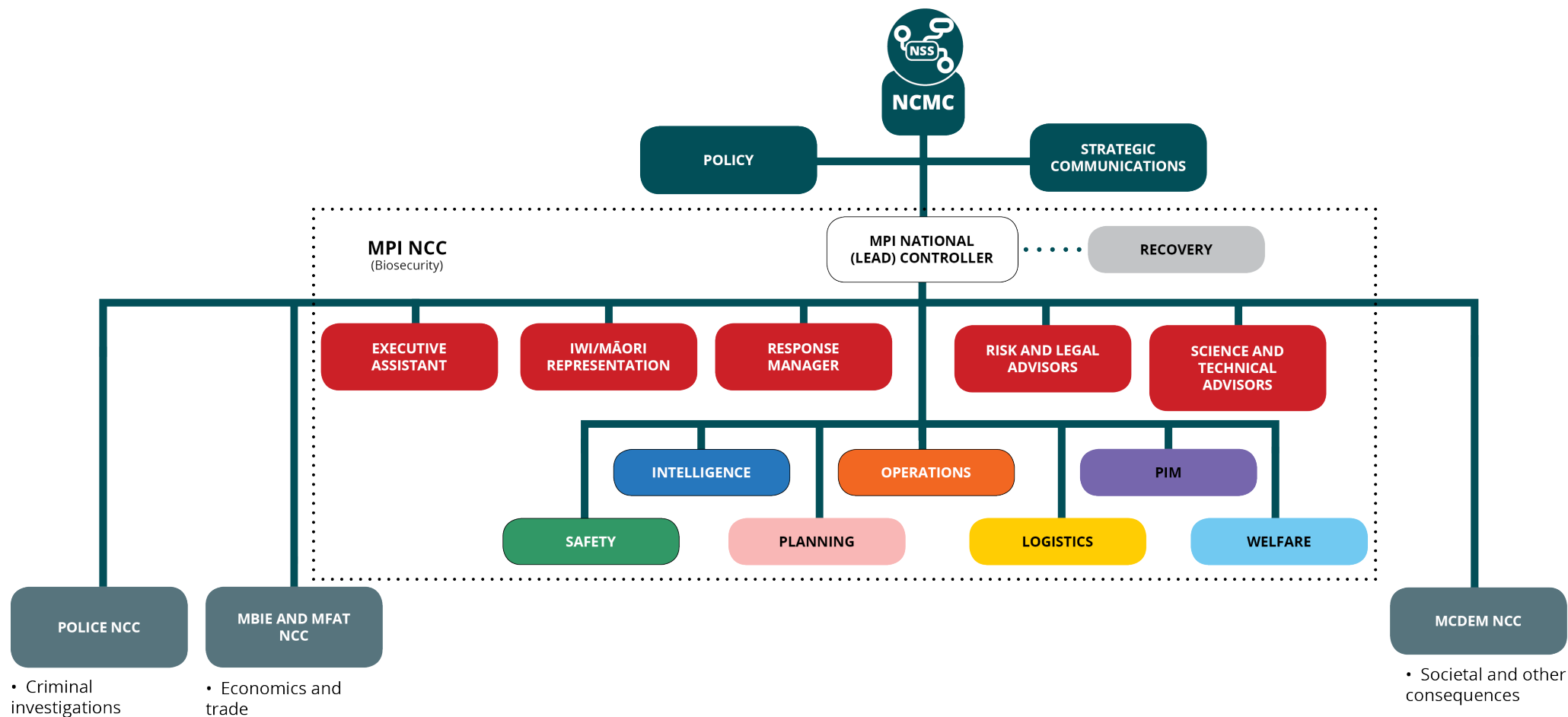


Figure 19: A national level response

Appendix A The full CIMS Hierarchy

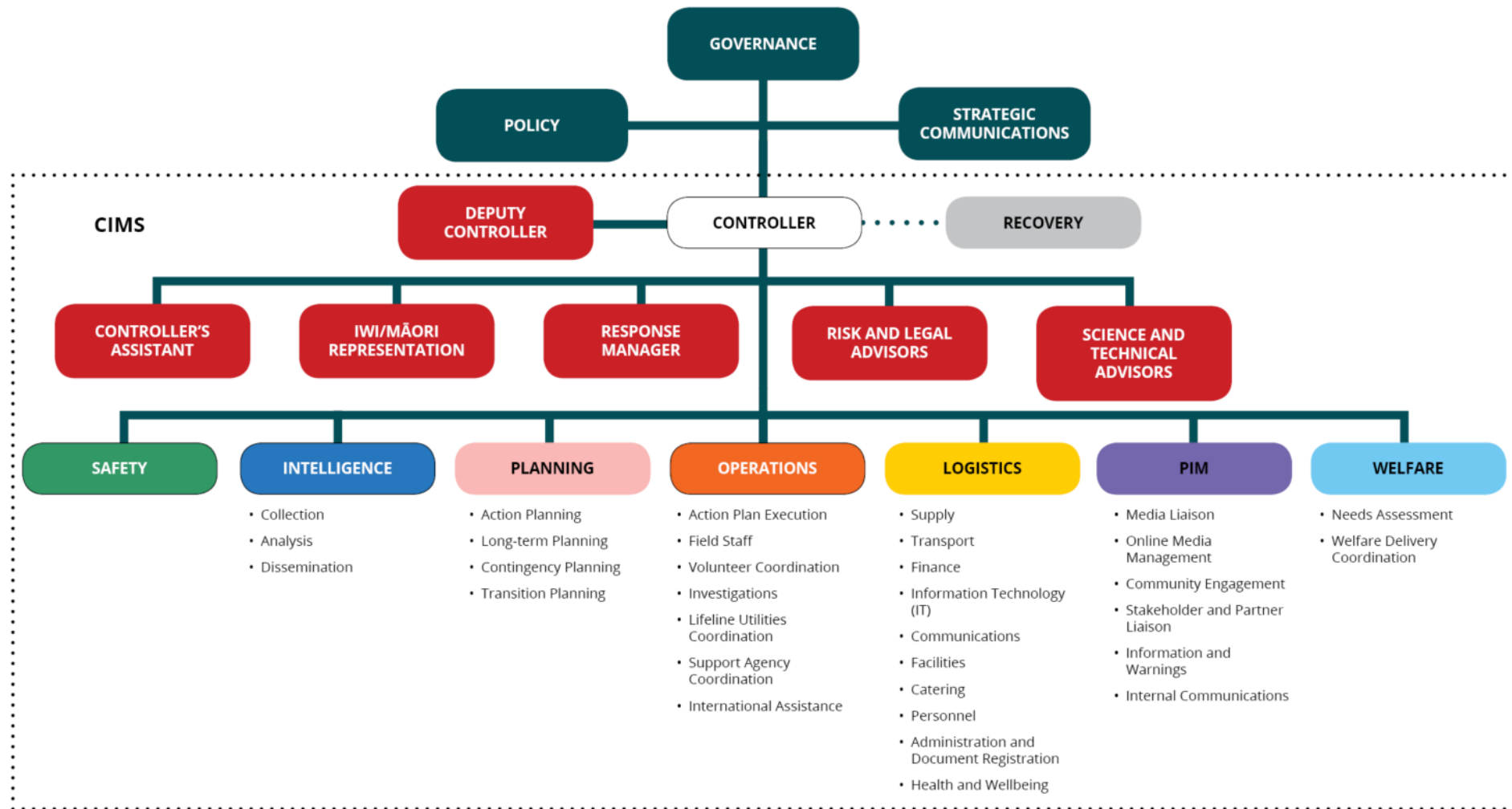


Figure 20: A full CIMS hierarchy

Appendix B The Intelligence Cycle

Intelligence delivers its responsibilities by applying an Intelligence Cycle, such as the one shown in Figure 21. The cycle comprises six steps, which are grouped under the three main sub-functions.

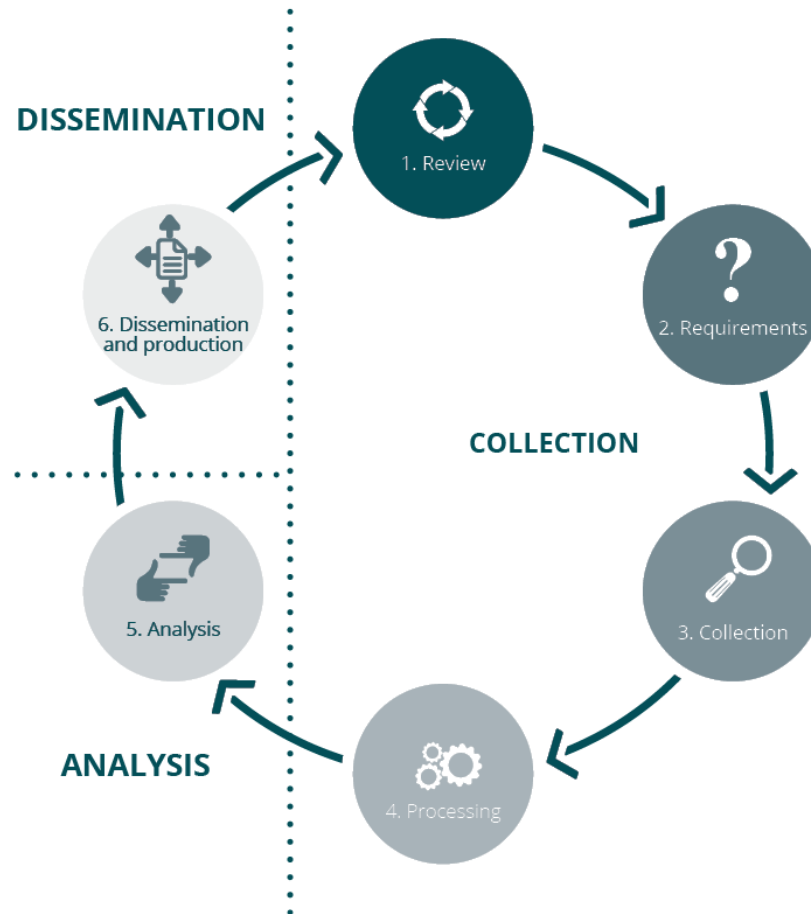


Figure 21: The Intelligence Cycle

1. Review

This step reviews the current situation and begins the Intelligence Cycle. At the end of the Intelligence Cycle, it assesses whether or not the completed intelligence products are meeting intelligence needs and identifies any areas for possible improvement. The Intelligence Manager is usually responsible for reviewing the current situation at the start of a response and for gathering feedback from other functions and support agencies once a response is underway.

2. Requirements

While various stakeholders may have intelligence requirements — things they would like to know from the Intelligence function — the Intelligence Manager is responsible for identifying the Priority Intelligence Requirements. These requirements should be relevant to the objectives of the response and take priority if time or resources are tight.

Intelligence requirements are the key questions that other functions and support agencies would like answered. They are not random and are confirmed and prioritised by the Intelligence Manager. The

purpose of these requirements is to focus the collective effort of the Intelligence function on these topics. The questions will usually relate to matters that will affect the ability of responders to respond to and/or recover from the incident. These might include (but are not limited to):

- the status of the incident;
- impacts of the incident on people and animals, infrastructure, lifeline utilities, etc;
- impacts on and from the environment (e.g. terrain, natural and/or human hazards, weather, etc.);key decisions that will need to be made by function managers in the short to medium term — with an assessment of priority and/or interdependencies across all CIMS functions; and
- any emerging issues related to the incident response capacity (e.g. staffing pressure) or the coping capacity of communities.

3. Collection

Ideally, collection should be undertaken by an assigned Collection Officer. If this is not possible, the collection phase can be planned by the Intelligence Manager, with input from other staff as needed.

Intelligence requirements are recorded in an Intelligence Collection Plan, ensuring that the associated questions are properly defined as intelligence or information requirements and are assigned to a function or organisation for answering. Information sources and contact details should be recorded for future use.

Each intelligence or information requirement is numbered, dated, prioritised and then assigned to an individual or organisation to answer. Once an answer is received, the intelligence or information requirement is closed (but not deleted).

The following example might be for the initial stages of an earthquake response.

Number	Date/Time	Intelligence requirement	Assigned	Status
001	12/3, 2145	What is the casualty status as at 1800 hours 12/3?	Ambulance, Police	Closed
002	12/3, 2200	Is the bridge on SH9 over White River open?	Police, Rooding	Closed
003	12/3, 2245	What is the operational status of the Greyville Hospital?	DHB	Open
004	12/3, 2315	What welfare support can be provided from regional and national?	ECC	Closed
005	13/3, 0100	What is the forecast rainfall in the White River catchment for the next two days?	Intelligence	Closed

Table 10: Example of an Intelligence Collection Plan

The Intelligence Collection Plan assists with prioritising and targeting the collection of information and helps to prevent duplication of effort. Information must be systematically acquired throughout the response, and information needs and sources should be continually reviewed.

4. Processing

Processing involves the logging of all information received; evaluating its credibility/reliability, relevance and accuracy; and the systematic storage of the information so that it can be easily accessed and analysed. Processing also involves combining the collected information (as graphs, maps, timelines and network charts) with other similar information to prepare it for analysis.

5. Analysis

Analysis involves interpreting the processed information and drawing conclusions. It should be provided in a timely manner so that it can be used in decision making. It transforms information from various sources into judgement and insight.

A good intelligence analyst will be curious, a critical thinker, tenacious and able to identify and challenge their own assumptions and biases. They should not take any information at face value. Ideally, the analysis step of the Intelligence Cycle should be undertaken by a person, or persons, with training and/or experience using analytical tools and methodologies. If this is not possible, a person or persons with experience producing briefings and/or policy advice is the next best choice.

Where possible, functions should be encouraged to analyse their own information and provide this analysis to Intelligence along with the information. This will allow the Intelligence function to gain insight from subject matter experts and allow Intelligence staff to look across the response at the interdependencies and risks.

For example, Lifeline Utilities Coordination can provide the Intelligence function with a list of closed and at-risk roads, or they could provide this list along with an analysis of communities that are isolated or at risk of becoming isolated.

Analysis does not involve collating or summarising existing information from other sources (sometimes referred to as “news and weather” reporting).

6. Production and dissemination

Production is how analysis is presented. The product format should be determined by the requirements of other functions and support agencies. Intelligence products may include (but are not limited to):

- written reports or briefings;
- profiles;
- single page snapshots or warning documents;
- annotated maps or charts; and/or
- verbal presentations (potentially supported by slides).

Some other functions and support agencies may have particular product preferences, or may require analysts to give particular consideration to certain aspects of the incident. It is helpful to identify these at the requirements stage.

Above all, intelligence products must make an assessment of the available information and identify the implications for other functions and support agencies. It is good practice for analysts to include an indication of confidence in the assessment, or assessments, made to help other functions and support agencies determine how much decision-making weight to give to each product.

Dissemination is the act of providing the finished intelligence product or products to other functions and support agencies. Records should identify the recipients of each product.

The dissemination of intelligence products should comply with privacy and security requirements as appropriate, for example:

- the Privacy Act 1993
- the Official Information Act 1982
- the Local Government Official Information and Meetings Act 1987
- the New Zealand Government Security Classification System, and/or
- Handling Requirements for Protectively-marked Information and Equipment.

These documents are provided in the Information Security section of the Protective Security Requirements website.

Appendix C The Planning Process

Planning provides the foundation for effective incident management. The planning process may begin when scheduling a planned event, when identifying a credible threat, or during the initial response to an actual or impending incident.

The planning process described in this appendix represents the underlying process for all planning, including Action, Contingency, Long-term and Transition planning, at any response level and the development of function plans at any Coordination Centre.

Planning fundamentals

The Controller is responsible for planning, and while they may delegate the planning process, all planning outputs remain their responsibility. The Controller must therefore provide their intent to planners and must be engaged at key points in the planning process.

The planning team must include appropriate representation from key stakeholders. These stakeholders will differ depending on the plan being developed. A planning team, for example, must include representation from all CIMS functions (including Recovery), support agencies and relevant industry and community representation (including iwi/Māori) to ensure all perspectives are captured. This will help to develop a plan that has the best possible outcome and that considers all impacted communities and infrastructure. Each member of the Incident Management Team (IMT), or their representatives, are responsible for gathering and bringing information that will support the development and execution of the plan.

Plans must provide clear direction; include a list of the critical or key tasks, response structure, responsibilities and deadlines, and identify any resource requirements and support required to accomplish the objectives. Plans are living documents that are based on the best available information at the time they are produced. The operational period for a plan will vary depending on the type or scale of the response, as well as the stage of the response — this may be hours, days, weeks or even months. The operational period and planning cycle may also be influenced when:

- the objectives in the current plan are achieved,
- the situation changes significantly and the current plan objectives cannot be achieved, or
- the response intent or objectives are changed by the Controller.

The Planning 'P'

The "Planning P" (Figure 22) depicts the stages in the Action Planning process. The leg of the "P" includes initial understanding and mobilisation. Although maintaining situational awareness is essential throughout the life cycle of the incident, Phase 1 is completed only once. When this is accomplished, incident management shifts into a cycle of planning and operations. This is informed by ongoing situational awareness that continues and is repeated depending on the nature of the incident.

Five phases are applied to create comprehensive plans.

1. Initial understanding and mobilisation
2. Establish/review planning objectives

3. Develop the plan
4. Prepare and disseminate the plan
5. Execute, evaluate and revise the plan

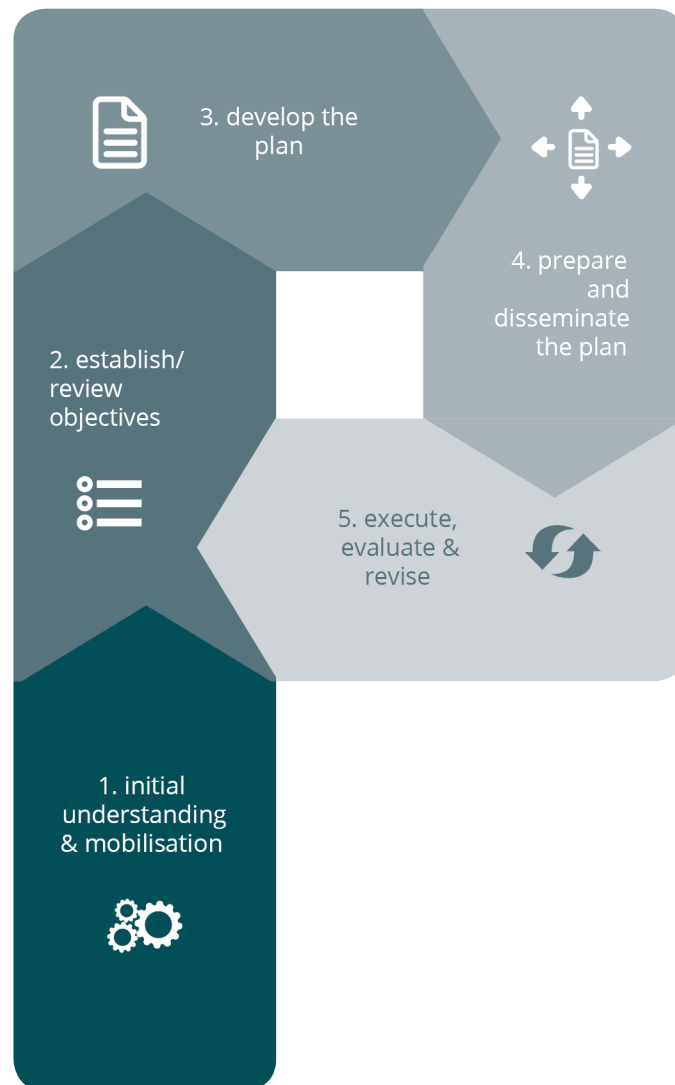


Figure 22: The “Planning P”

Planning process adaptation

More detailed versions of the “Planning P” are available,⁴ and while the underlying phases are the same, these versions are generally more detailed and include additional steps such as signoffs and meetings to suit particular needs. As the underlying phases are the same, New Zealand agencies and organisations who require a more prescriptive approach are able to adopt these planning processes. However, when utilising the more prescribed “Planning Ps”, the underlying phases should be referenced to allow easier collaboration between agencies.

⁴ Including, but not exclusively, National Incident Management System (NIMS), Incident command system (ICS), Australian inter-agency incident management system (AIIMS), Military Appreciation Process (MAP)

The “Planning P” steps

1. Initial understanding and mobilisation (what’s happened / is happening)

- Notification of incident
- Initial response and assessment
- Incident briefing
- Decision point — required planning

This initial phase is done upon notification that an incident has occurred, or is about to occur. This includes gathering information, recording and analysing the initial response and undertaking initial response actions. Through this phase, an increased situational awareness of the magnitude, complexity and potential impact of the incident will inform the decision whether or not to escalate the response. At that point a Situation Report and briefing will need to be prepared on the situation to date. This initial phase occurs once in any incident, at which point the planning cycle continues by repeating phases 2–5. If the incident can be handled with the available resources, the planning team may stand down and no further planning action is required.

2. Establish/review planning objectives (what do we need to achieve)

- Review situation
- Understand operating environments (determine freedoms/constraints)
- Define SMART objectives (for this operational period)
- Analyse objectives
- Identify critical facts and assumptions

Once the decision has been made to move beyond the initial response, the planning cycle begins. This phase includes reviewing the situation and any existing objectives, and then formulating and prioritising measurable objectives for the planning cycle. The plan objectives must conform to the response objectives and legislative obligations of all involved agencies. Objectives should be Specific, Measurable, Achievable, Realistic and Time-bound (SMART), and relevant for the current operational period.

Identification and documentation of the critical facts, constraints, risks, and assumptions is an essential part of reviewing the situation to enable SMART objective setting. Documentation of the timeline of the incident to date and establishing time available for planning will also support effective planning.

3. Develop the Plan (how could/should we achieve the objectives)

- Options development and identification of critical tasks
- Identification of contingencies
- Options analysis
- Option selection/recommendation

The planning team will now consider options to achieve the objectives — the most suitable options are then analysed against the specifics of the scenario and evaluated to determine the most appropriate

option. Evaluation criteria include area of operations; resource availability; hazards forecasts; and climate, political, economic, social, time, legal, environmental and safety considerations.

Options, including recommendations, are then briefed to, and approved by, the Controller. A preferred option is selected and becomes the basis for the plan.

4. Prepare and disseminate the Plan

- Determine appropriate format, or formats, for the plan (formal written plan, verbal brief, etc.)
- Place into appropriate template
- Plan approval (Controller signoff)
- Dissemination
- Hand over to Operations for operationalisation

This phase involves producing the plan in a format that is appropriate for the incident level and its complexity. For the initial response, the format may be an oral briefing. For incidents that will span multiple operational periods, the plan will be developed and delivered in writing. The required contents of the plan are set out in Appendix G.

The plan is authorised by the Controller. Coordination Centre staff, support agencies and subordinate response elements are briefed using a GSMEAC format (see Appendices E and H); and the plan is handed over to the response functions and lower Coordination Centre Controllers to implement. The plan is then disseminated as widely as required. Distribution includes all personnel involved in the lead agency Coordination Centre, support agencies and interconnected Coordination Centres.

This point marks the start of a new operational period.

5. Execute, evaluate and revise the Plan

- Evaluation of plan against response objectives
- Adjustment of plan to evolving situation
- Decision point — is another plan / planning cycle needed
- Debriefing

The ongoing planning process involves evaluating planned activities and checking the accuracy of information to be used in planning. The Controller and Incident Management Team should be able to regularly compare planned progress with actual progress and check if objectives have been met. When deviations occur and new information emerges, it should be used for modifying the current plan or developing the next plan. Debriefing is also an important part of this process to identify relevant issues and information to inform plans for the subsequent operational period.

The planning team will commence development of the plan for the subsequent operational period if required.

Appendix D The National Security System

The National Security System⁵ is activated for events that are nationally significant, or complex enough, to demand a coordinated strategic response at the national level. Criteria and examples are included in the National Security System Handbook available from the DPMC website. These criteria are:

- increasing risk, or a disaster or crisis, **affects New Zealand interests**
- active, or **close coordination**, or **extensive resources** are required
- the crisis might involve risk to New Zealand's **international reputation**
- an issue is of **large scale, high intensity or great complexity**
- multiple smaller, **simultaneous, events** require coordination
- **an emerging issue** might meet the above criteria in the future, and would benefit from proactive management.

The National Security System is the architecture that provides all-of-government support to national security decision makers at the strategic level. It coordinates the activities of central government agencies in support of a lead agency.

In the context of incident classifications (see Section 3.2), activation of the National Security System is most likely to occur at R3&4 and N3&4 incidents. Examples of activation are the March 2019 terror attack in Christchurch, the September 2017 Auckland Fuel Supply Disruption, the November 2016 earthquake and tsunami, and the 2015 threat to contaminate infant and other formula with 1080.

The National Crisis Management Centre (NCMC), which is normally located in the Executive Wing of Parliament (Beehive), is a facility from where the National Security System is supported by all-of-government response and international assistance coordination. It is a permanent, all-hazards, all-risks coordination facility, and a lead agency can use the NCMC as their NCC. The lead agency runs the NCMC and is supported by other relevant support agencies, some of whom may also have specific appointments in the NCMC. Relevant industry groups and NGOs may also be represented in the NCMC.

The National Security System operates at three levels: Watch Group, the Officials' Committee for Domestic and External Security Coordination (ODESC) and Ministers.

Watch Group

The Watch Group comprises senior officials from relevant organisations, including the lead agency's National Controller and, if relevant, local government and the private sector. It focuses on the national interest at a strategic level. Attendees:

- test current arrangements
- check that all strategic risks have been identified and are being managed
- identify gaps and areas of outstanding concern, and

⁵ The National Security System was previously known as the Domestic and External Security Coordination (DESC) system.

- agree on any further action required.

The Watch Group Chair reports the Watch Group's assessments and advice to ODESC.

Officials' Committee for Domestic and External Security Coordination (ODESC)

ODESC is the group of Chief Executives responsible for providing strategic direction and for coordinating the all-of-government response. It:

- provides all-of-government coordination at the Chief Executive level of the issues being dealt with through the response;
- provides strategic advice on priorities and mitigation of risks beyond the lead agency's control;
- ensures that the lead agency and those in support have the resources and capabilities required to bring the response to an effective resolution;
- provides a link to the political level, including supporting Ministers to make decisions about strategic policy, authorise resources or any other decisions that sit within a Ministers' ambit of control; and
- exercises policy oversight and advises the Prime Minister, Cabinet and, when activated, the relevant Cabinet Committee.

Ministers

Depending on the scale of the event, Ministers may have a role in making policy decisions in response and recovery. This includes briefing Cabinet on the impacts and consequences of the event and recommending financial assistance for response and recovery activities. Ministers also provide public assurance and information about the government's level of involvement, as well as reiterating safety messages. Ministers show support for the response operations underway, but generally do not comment on operational issues. Their involvement may be as individual portfolio Ministers, as a Cabinet Committee, or through meetings of relevant Ministers.

Civil Defence Emergency Management (CDEM)

Civil defence emergency management (CDEM) is part of the National Security System. Realisation of CDEM depends on there being an effective partnership between lead agencies and supporting agencies, including emergency services and CDEM agencies (CDEM Groups and the Ministry of Civil Defence & Emergency Management - MCDEM) nationally, regionally, and locally.

The Director of CDEM is a statutory position with specific functions and powers under the Civil Defence Emergency Management Act 2002. The Director of CDEM is supported by a national emergency management agency (currently MCDEM but in 2019 a National Emergency Management Agency (NEMA) will be formed). The national agency enables the Director to meet their functions and exercise their powers, including providing national leadership across central and local government, communities, iwi, and business to ensure emergency management is ready and able to provide an effective and integrated response to, and recovery from, emergencies.

Appendix E Handovers

A handover is a process to hand over the incident to the next shift. It involves the changing of personnel and equipment, and relaying essential information. Poor handovers can impact the effectiveness and cost of the response. The Controller is ultimately responsible for an efficient handover, but all the functions participate and contribute to its effectiveness.

Handovers should be conducted so that operational delivery is not impacted. For field operations, it is normally preferable to hand over in daylight and at a suitable location close to the incident ground. The oncoming shift should be fed before handover and the outgoing shift fed after handover. Specific briefings appropriate to each function should be prepared. The specific functions' briefings should be preceded by a general, all-of-staff handover briefing focusing on the following:

- The current situation, including a high level overview of what has been done and what is currently in progress
- A high level overview of the Action Plan, including objectives and strategies for the incident (what is planned and what is outstanding)
- Critical issues being managed
- Key risk exposures (safety, political, economic, social, public health and environmental)
- Administrative details such as logistics, timings, document systems (i.e. file structure), communication arrangements (including key contacts), map of facilities, etc.

Specific responsibilities

The outgoing team:

- sets the handover time and location
- prepares handover briefings (for each function, detailing actions and processes for a particular function)
- attends handover briefings and briefs replacement staff, and
- conducts a hot debrief after the handover, ensuring critical learning is passed on to the oncoming shift, and then leaves.

Handover briefings for incoming operational staff may follow a G-SMEACS-Q process:

Ground / Situation / Mission / Execution / Administration and Logistics / Command, Control, Communications / Safety – Questions.

Handover briefings for the Incident Management Team can follow the structure of the Action Plan.

The incoming team:

- attends/receives handover briefings (a general all-of-staff briefing and function-specific briefings)
- ensures they are acquainted with the Action Plan, completed and ongoing tasks, critical issues and risks, processes, and document systems
- establishes connections with other functions and response levels, and
- ensures continued response and commences planning for the next handover.

Appendix F Demobilisation

Demobilisation is the planned and coordinated process for releasing and returning resources and for ending processes that are finalised, or no longer required. Demobilisation generally occurs at the end of a response or as part of the transition to recovery. Demobilisation may also occur as the scale of a response decreases, or if the lead agency changes.

The roles of some of the different functions in the demobilisation process are the following:

- Planning develops the demobilisation plan in consultation with the Controller and the IMT
- The Controller approves the demobilisation plan and communicates it with Governance
- Intelligence files and secures collected information and intelligence product
- Operations ensures tasks are completed, advises support agencies and liaison staff and releases resources (including personnel) that are no longer required
- Logistics releases facilities, returns resources, processes outstanding payments, and files documentation. Logistics also ensures personnel have adequate rest before traveling, are debriefed and are signed out. It also ensures records of all financial transactions are passed to the Recovery office
- Public Information Management (PIM) updates social media posts, sends out media releases and updates or removes community notices. PIM also remains available for Recovery messaging
- Welfare ensures outstanding or ongoing community needs have been met or referrals are made to the appropriate organisations. Welfare also remains available for the Recovery team

The Controller should be the last person to remain at the Coordination Centre until either demobilisation or the formal transition to recovery has been completed.

After demobilisation, lead agency, multi-organisation and community debriefs may occur. Lessons that are identified from debriefs (whether formal or informal) should be recorded, analysed, actioned, tracked and shared where appropriate to improve future responses.

In larger responses, the lead agency should formally acknowledge support agencies, individuals and community/volunteer groups.

Appendix G Recommended Template Content

CIMS relies on standardised templates to aid information management, information collation and analysis, planning and decision making. This appendix includes the recommended content for Status Reports, Situation Reports (SitReps), Action Plans, Resource Requests and Response to Recovery Transition Reports.

Consider the following when preparing response documents:

- Use the same layout at the top of similar types of forms or documents so that personnel can scan them quickly;
- Include pagination and the filename in the footers (by inserting the filename field);
- Save documents with filenames that include the:
 - organisation initials
 - place the report is coming from
 - type of report
 - # and sequential reference number, including zeros as place holders; and
 - date in the format yyyy-mm-dd, including zeros as place holders.

Some examples of filenames are:

- Kaipara District Council EOC SitRep #04 2020-04-31
- Police ECC Action Plan #01 2020-09-31
- NCMC SitRep #17 2020-02-29
- USAR ICP SitRep #09 2020-11-31

This means that when files are stored electronically, they sort into a logical sequence that is easy to search through.

Response document types

Document name	Document purpose
Status Report	An internal update on a function or cluster's progress that is created between Situation Reports.
Situation Report (SitRep)	A brief description of an incident and the response, usually updated and distributed at regular intervals.
Action Plan	A description of how the response will be managed and how response agencies will integrate their activities.
Resource Request	A request from one function or organisation for specific resources.
Response to Recovery Transition Report	A description of the end state of a response, including outstanding actions, to provide the basis for further recovery planning.

G.1 Status Report

Recommended content for a Status Report.

Name of field	Comments	Example
Function, cluster or organisation	Function or organisation completing the Status Report	Mackenzie District EOC
Type of report		Status Report
Report number	Include a hash (#) and include enough digits for maximum required	#008
Incident	Type of incident, location and time	Tekapo flood April 2020
Date and time issued		2020-04-30 0600
Period covered	Date/time covered (start and finish)	2020-04-29 0500 to 2020-04-29 1700

Main body

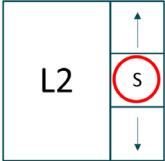
Name of field	Comments
Current status	Current status of function, cluster or organisation (not the incident as a whole), actions taken, current resources, etc
Limiting factors / outstanding issues	Anything that affects, or is likely to affect, the effectiveness of the function, cluster or organisation's ability to carry out its tasks
Anticipated priorities/actions	In the current and subsequent operational period — note any assumption or conditions
Comments	

Approval and distribution

Name of field	Comments
Status Report prepared by	Name (and rank if applicable), response role, signature and contact details
Status Report approved by	Name (and rank if applicable), response role, signature and contact details

G.2 Situation Report

Recommended content for a Situation Report.

Name of field	Comments	Example
Coordination Centre	Coordination Centre issuing the SitRep (include organisation)	Mackenzie District EOC
Type of report		SitRep
Report number	Include a hash (#) and include enough digits for maximum required	#002
Incident	Type of incident, location and time	Tekapo flood April 2020
Date and time issued		2020-04-30 0600
Period covered	Date/time covered (start and finish)	2020-04-29 0500 to 2020-04-29 1700
Incident classification	See Section 3.2	

Main body

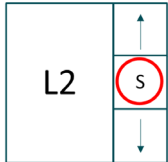
Name of field	Comments
Summary of incident	
Actions carried out	
Predicted incident progression	How this situation is anticipated to evolve — causal factors, consequences and response
Resources in place	
Resources required	These need to be requested on a separate Resource Request form but can be summarised here
Limiting factors	Anything that is currently affecting, or is likely to affect, the effectiveness of the response
Assessment	Any critical issues or assumptions made
Options	Outline major options for action that are being or have been considered
Intended actions	Outline significant actions intended in current and subsequent operations

Approval and distribution

Name of field	Comments
SitRep prepared by	Name (and rank if applicable), response role, signature and contact details
SitRep approved by	Name (and rank if applicable), response role, signature and contact details
Distribution	Include CIMS functions, partner agencies and representatives at the Coordination Centre, and consider including partner agencies not represented at the Coordination Centre and external liaison
Next SitRep due at	Date and time

G.3 Action Plan

Recommended content for an Action Plan.

Name of field	Comments	Example
Coordination Centre	Coordination Centre issuing the Action Plan (include organisation)	Mackenzie District EOC
Type of report		Action Plan
Action Plan number	Include a hash (#) (versions are indicated by adding .1, .2, etc.)	#1, #1.2
Incident	Type of incident, location and time	Tekapo flood April 2020 (R2)
Date and time issued		2020-04-30 0600
Operational period covered	Date/time covered (start and finish)	2020-04-30 0600 to 2020-05-03 1700
Incident classification	See Section 3.2	

Main body

Name of field	Comments
Summary of incident	A summary of the hazard impacts, environment and response actions to date based on issued SitReps.
Intent	A statement that gives clear direction on what the Controller wants to achieve, the response actions to achieve them, and what it will look like when it's done. It may be combined with Objectives and/or with Plan of action/strategy below.
Objectives	Breaking the intent down into specific objectives; best described as Specific, Measurable, Achievable, Relevant and Time-bound (SMART).
Plan of action/strategy	Concept of operations describing the response actions that will be done to achieve the intent and objectives — a broad statement of what must happen and when
Designated tasks	Specific tasks and timings for each organisation under the plan
Limiting factors	Matters that may or will limit options, timeframes and/or outcomes
Coordination measures	Times, locations, boundaries and other measures designed to coordinate the response
Resource needs	Resource requirements — who will provide what and when they will do it
Information flow	Who needs to know and who has the information
Public information plan	Outline of intended public information processes and outputs — this may be an appendix
Communications plan	Frequencies/purpose/coverage, role cellphone numbers, communications schedule, etc.

Name of field	Comments
Organisation	List / organisation chart of key roles, contact details and rosters of people assigned to the roles
Appendices	Specialist functions, lists, tables, maps, etc.

Approval and distribution

Name of field	Comments
Action Plan prepared by	Name (and rank if applicable), response role, signature and contact details
Action Plan approved by	Name (and rank if applicable), response role, signature and contact details
Distribution	Include CIMS functions, all partner agencies' representatives at the Coordination Centre and any other activated outputs

G.4 Request for Assistance / Resource Request

Recommended content for a Resource Request.

Request details

Name of field	Comments	Example
Coordination Centre	Coordination Centre, function or organisation making the Resource Request (include organisation)	Mackenzie District EOC
Contact details	Name, response role, and contact details for the individual who can answer any questions relating to the request	
Request number	Include a hash (#) and include enough digits for maximum required	#013
Incident	Incident name	Tekapo flood April 2020
Importance	High Medium Low (circle as appropriate)	
When request made	Date and time	2020-04-29 0600
Date and time requirements	The length of time the resource is required — give an end date if known	2020-05-10 1500

Main body

Name of field	Comments
Brief description of effect/outcome to be achieved (or problem to be solved)	Describe the effect/outcome to be achieved. Effects must be phrased as outcomes, and not resource requirements (consider the what, where, when and why). <i>For example, request for the movement of portaloos from one location to another (as opposed to requesting an NZDF helicopter to move portaloos).</i> Explain why the task is important to the response and what would occur if the effect/outcome could not be achieved or problem solved.
Specific resource requested (and any supporting requirements)	If known, specify any specific resources, type, standards, capacities and number that could be best utilised to achieve the effect/outcome. For example, if diesel (not petrol) is required for a generator and it requires particular dangerous goods delegations.
Possible substitutes	Alternative options, in case the requested resource is unavailable
Receipt/delivery details	Specify name and location of staging area / final destination, and name, response role, and contact details
Disposal plan required?	Yes / No

Approval to request

Name of field	Comments
Requested by	Name, position or response role, signature and contact details
Request approved by	Name, position or response role, signature and contact details

Approval to supply

(Separate section at end of resource Request Form, completed by resource provider)

Name of field	Name of field
Resource available? Yes / No	Critical resource? Yes / No
Supplier contact details:	
Estimate/actual cost:	Supplier reference:
Payment details:	Date and time resource requested:
Resource processed by: <i>(Name and rank, response role, signature and contact details)</i>	
Supply of resource approved by: <i>(Name and rank, response role, signature and contact details)</i>	
Details of resources supplied (quantity, type, size, etc.):	
Date and time of dispatch:	Estimated date and time of arrival:
Date and time requester notified of approval/rejection:	Date and time requester confirmed receipt of resource:
Comments:	

G.5 Response to Recovery Transition Report

Recommended content for a Resource Transition Report.

Name of field	Comments	Example
Coordination Centre	Coordination Centre issuing the Response to Recovery Transition Report (include agency)	Mackenzie District EOC
Type of report		Response to Recovery Transition Report
Version number	Include a hash (#) (versions are indicated by adding .1, .2, etc.) Draft/final	#1, #1.2 Draft
Incident	Type of incident, location and time	Tekapo flood April 2020
Date issued		2020-04-30

Main body

Name of field	Comments
Handover date	Date of handover from Controller to Recovery Manager
Summary of event	Brief summary of the event, including a summary of emergency powers exercised, open purchase orders, ongoing costs and ongoing funding
Nature and extent of consequences (short-, medium- and long-term)	Condition of community Situations with the potential to re-escalate Consequences on the social environment, including critical issues Consequences on the built environment, including critical issues Consequences on the natural environment, including critical issues Consequences on the economic environment, including critical issues Consequences on other environments, e.g. cultural, rural
Governance arrangements	Details of Recovery Managers and recovery leads Reporting that will be carried over into recovery Meetings and forums that will be carried over into recovery
Engagement and communications	Communications: underway or planned Engagement with key partners, including iwi: underway or planned Community engagement: underway or planned
Short term resource analysis	Analysis of actions required, priority, responsible agency and potential gaps
Risks	Key risks and issues arising because of the emergency and in moving from response to recovery, and actions proposed and underway to reduce the impact
Outstanding actions	Outstanding response actions and agencies and organisations responsible
Source documents	Documents used to develop this Response Transition Report, e.g. Community Engagement Plan, Communications Plan

Approval and distribution

Name of field	Comments
Response to Recovery Transition Report Prepared by	Name (and rank if applicable), response role, signature and contact details
Response to Recovery Transition Report approved by	Controller Recovery Manager
Distribution	Include CIMS functions, all partner agencies' representatives at the Coordination Centre, any other activated sub-functions and any other stakeholders involved in the recovery

Appendix H Glossary and Acronyms

Glossary term	Definition
4Rs	The 4Rs of emergency management are [risk] reduction, readiness, response and recovery. [risk] Reduction involves identifying and analysing risks to life and property from hazards, taking steps to eliminate those risks if practicable, and, if not, reducing the magnitude of their impact and the likelihood of their occurrence to an acceptable level. Readiness involves developing operational systems and capabilities before an emergency happens, including self-help and response programmes for the general public and specific programmes for emergency services, lifeline utilities and other agencies. Response involves actions taken immediately before, during or directly after an emergency to save lives and property, and to help communities recover. Recovery involves the coordinated efforts and processes used to bring about the short-, medium- and long-term holistic regeneration and enhancement of a community following an emergency.
Action Plan	Action Plans are developed during an emergency (or immediately before an emergency) and describe response objectives, tasks, and measures and resources needed to coordinate the response. They are proactive, seeking to pre-empt hazard impacts where possible and to resolve the situation as quickly as possible. Depending on the scale of the emergency, Action Plans may be developed at the national level, the CDEM Group level, the local level or the incident level.
affected area	The area directly affected by an incident.
Agency	Agency means a government or non-government organisation or entity (other than a CDEM Group) with responsibilities under the National Civil Defence Emergency Management Plan Order 2015.
Assembly Area	The area, managed by Logistics, where resources are organised and prepared for deployment. It may have facilities for response personnel wellbeing and for equipment maintenance. It is usually set up at an established facility away from an incident.
briefing	An overview of an operation that can be formal and structured or informal. It provides a common operating picture of how an incident is being, or is to be, managed and how resources are to be deployed.
Business Continuity Plan	A plan that outlines response to a business interruption in a timely manner.
CDEM	See <i>civil defence emergency management (CDEM)</i> .
CDEM Group	See <i>Civil Defence Emergency Management Group (CDEM Group)</i> .
CERT NZ	CERT NZ is a key component of New Zealand's Cyber Security Strategy 2015, contributing to the delivery of the Strategy's vision of 'a secure, resilient and prosperous online New Zealand'.

Glossary term	Definition
CIMS	See <i>Coordinated Incident Management System (CIMS)</i> .
Civil Defence Centre (CDC)	A Civil Defence Centre (CDC) is a facility that is established and managed by a CDEM Group during a response to support individuals, families/whānau and the community. CDCs are open to members of the public and may be used for any purpose including public information, evacuation, welfare or recovery, depending on the needs of the community.
civil defence emergency management (CDEM)	The activities that guard against, prevent or overcome any hazard, harm or loss that may be associated with an emergency. The Civil Defence Emergency Management Act 2002 provides a comprehensive definition of civil defence emergency management.
Civil Defence Emergency Management Group (CDEM Group)	A group established under section 12 of the Civil Defence Emergency Management Act 2002. All local authorities must be members of a CDEM Group, and all local authorities and emergency services must have representatives on a Co-ordinating Executive Group of the CDEM Group (the CDEM Group may co-opt other people as required). CDEM Groups respond to and manage the adverse effects of emergencies in their area (from an Emergency Coordination Centre) and plan for and carry out recovery activities.
cluster	Cluster means a group of organisations that interact to achieve common CDEM outcomes.
command	Command applies vertically to a team, unit, or organisation. It includes the internal ownership, administrative responsibility and detailed supervision of personnel, tasks and resources. Command cannot be exercised across organisations unless specifically agreed.
common operating picture (COP)	A common operating picture (COP) is a representation of relevant incident information that can be shared across relevant functions and agencies during a response. A COP is achieved through a system of protocols, procedures and tools that facilitate shared awareness and understanding of the situation and enable consolidated planning.
communications plan	A plan that defines the communications arrangements used to pass information between response personnel, to Governance and to the public. This may list telephone numbers, email addresses, radio frequencies, schedules for teleconferences, media conferences, etc.
community	A group of people who: • live in a particular area or place (geographic or place-based community) • are similar in some way (relational or population-based community), or • have friendships or a sense of having something in common (community of interest). People can belong to more than one community, and communities can be any size. With increasing use of social media and digital technologies, communities can also be digital.

Glossary term	Definition
community level response	The first level of response, which involves the general public including individuals, families/whānau, community groups and businesses. May be informal or part of the official response. See <i>community</i> .
context	The setting of an incident, including factors such as physical environment, weather, transport routes, weekend vs. workday and population distribution.
Contingency Plan	A plan developed to coordinate the response to a situation that has not, but may, occur.
Control (function)	The function responsible for coordinating and directing the response element. It sets priorities and objectives and determines how best to implement them.
control (verb)	The authority to assign tasks to another organisation and to coordinate that agency's actions so that it integrates with the wider response. Control operates horizontally between response agencies. Control authority is established in legislation or in an emergency plan. Control does not include internal ownership, administrative responsibility or the management of another agency's resources.
Controller	The person in charge of a response element who directs response activities and fulfils management functions and responsibilities. The person exercising control.
COP	See <i>common operating picture (COP)</i> .
Coordinated Incident Management System (CIMS)	Coordinated Incident Management System (CIMS) is the primary reference for incident management in New Zealand. The purpose of CIMS is to achieve effective coordinated incident management across responding agencies for all emergencies regardless of size, hazard or complexity. Pronounced sims.
coordination	The bringing together of organisations and resources to ensure unity of effort, and a consistent and effective incident response.
Coordination Centre	A Coordination Centre is the location from which a Controller and Incident Management Team manages a response. There are four types of Coordination Centres. • Incident Control Points (ICPs) operate at an incident level. • Emergency Operations Centres (EOCs) operate at a local level. • Emergency Coordination Centres (ECCs) operate at a CDEM Group level. • National Coordination Centres (NCCs) operate at a national level.
cordon	A means of controlling and restricting movement to and from an area. An inner cordon directly surrounds an incident and only tactical groups from the responding agencies operate there. An outer cordon is further from the incident and controls access to the area of operations.

Glossary term	Definition
doctrine	Doctrine is the body of principles and practices that guide an organisation's actions in support of their objectives. It is authoritative but requires judgement in application.
ECC	See <i>Emergency Coordination Centre (ECC)</i> . Pronounced E-C-C.
emergency	A situation that poses an immediate risk to life, health, property or the environment that requires a coordinated response. The Civil Defence Emergency Management Act 2002 provides the statutory definition.
Emergency Coordination Centre (ECC)	An Emergency Coordination Centre (ECC) is a Coordination Centre that operates at the CDEM Group or regional level to coordinate and support one or more activated EOCs.
Emergency Operations Centre (EOC)	An Emergency Operations Centre (EOC) is a Coordination Centre that operates at the local level to manage a response.
EOC	See <i>Emergency Operations Centre (EOC)</i> . Pronounced E-O-C.
function	An activity, or grouping of activities, that address some of the core responsibilities of a response.
Governance	The senior authority overseeing the response. This may be Chief Executives or senior managers within an organisation, or political leaders. Governance is not responsible for providing operational coordination or support — this duty falls to the Controller and their Coordination Centre.
GSMEAC	Acronym for G round, S ituation, M ission, E xecution, A dministration and L ogistics, and C ommand, C ontrol and C ommunications. It is a standard format used when directing actions.
handover	The process to hand over the incident to the next shift. It involves changing personnel and equipment and relaying essential information.
ICP	See <i>Incident Control Point (ICP)</i> . Pronounced I-C-P.
impact analysis	An analysis of the hazards and environment that aims to determine the most likely and the most dangerous scenarios that could occur. These are critical in forming a proactive Action Plan and response.
IMT	See <i>Incident Management Team (IMT)</i> . Pronounced I-M-T.
incident	An event that needs a response from one or more agencies. It may or may not be an emergency.
Incident classification	A descriptor to indicate the complexity of an incident.
Incident Control Point (ICP)	Single location where an Incident Controller and members of their Incident Management Team coordinate and manage response operations at an incident level response.

Glossary term	Definition
incident level response	The first level of official response, carried out by official first responders. Response personnel perform physical actions such as clearing obstructed roads, treating casualties, fighting fires and conducting rescues. Constitutes the large majority of responses.
Incident Management Facility	See <i>Coordination Centre</i> .
Incident Management Team (IMT)	A group of incident management personnel that support the Controller. It includes the Controller and the managers of the Planning, Intelligence, Operations, Logistics, PIM and Welfare functions. It could also include a Response Manager, Recovery Manager, Risk and Legal Advisors, and Technical and Science Advisors.
Information Collection Plan	A document that gathers all unanswered questions that an Incident Management Team or support agency may have into a set format and allocates these to agencies to answer. It provides a structured, targeted and methodical approach to information gathering.
Intelligence (function)	The function that collects, analyses and disseminates response information, particularly information related to the status, hazards, consequential risks and context of the incident.
intent	A formal statement that gives clear direction on a Controller's objectives regarding a response. It is normally expressed as objectives, a concept of operations or an end state. Also referred to as the aim or mission statement.
Iwi/Māori representation	A representative or representatives of whānau, hapū and/or iwi at a Coordination Centre.
jurisdiction	An organisation's, or agency's, area of responsibility.
lead agency	The agency with the primary mandate for managing the response to an emergency.
Legal advisor	A person dedicated to advising the Controller and other CIMS functions on legal interpretations and implications with regards to matters such as Acts and contracts.
Liaison (verb)	The act of formal communication between agencies participating in response and recovery.
Liaison officer	A lead agency staff member that performs the Support Agency Representatives Coordination sub-function of Operations.
local level response	The second level of official response (between incident and regional levels).
Logistics (function)	The function that supports a response through the provision of resources, which help maintain the response plan and the affected communities.

Glossary term	Definition
Long-term Plan	A plan developed to plan for response activities beyond the current and subsequent operational period. Long-term Plans may look hours, days, weeks or months in advance, depending on the level of the response and the scale of the incident.
National Coordination Centre (NCC)	A national level Coordination Centre that coordinates a national response and provides support to regional level response activities.
National Crisis Management Centre (NCMC)	The National Crisis Management Centre (NCMC) is a secure, all-of-government coordination centre used by agencies to monitor, support or manage a response at the national level. It can also be used as a National Coordination Centre.
NCC	See <i>National Coordination Centre (NCC)</i> . Pronounced N-C-C.
national level response	The fourth and highest level of official response (above regional).
National Security System (NSS)	New Zealand's arrangements to coordinate central government functions in response. Described in the National Security System handbook on the DPMC website.
NCMC	See <i>National Crisis Management Centre (NCMC)</i> . Pronounced N-C-M-C.
NGO	Non-governmental organisation
objective	Breaking the intent down into specific objectives — best described as Specific, Measurable, Achievable, Relevant and Time-bound (SMART) .
ODESC	See <i>Officials' Committee for Domestic and External Security Coordination (ODESC)</i> .
Officials' Committee for Domestic and External Security Coordination (ODESC)	The mechanism at the national governance level for providing strategic direction and for coordinating the all-of-government response. ODESC is a group of chief executives, which is chaired by the Chief Executive of the Department of the Prime Minister and Cabinet.
operational	The planning and command, control and coordination of actions or campaigns to achieve strategic outcomes. The operational level links strategy to tactics by establishing operational objectives and end states, initiating actions, and applying resources to ensure the success of an operation.
operational period	The period of time scheduled for execution of the Action Plan.
Operations (function)	The function responsible for the coordination of the response, detailed task planning and the implementation of the Action Plan. It is also responsible for coordinating volunteers and liaising with other agencies.
organisation	Any organised group that is participating in an agency response. This includes agencies, industries, businesses and/or community groups.
PIM (function)	See <i>Public Information Management (PIM)</i> . Pronounced 'pim'.
Planning (function)	The function that prepares and updates Action Plans and other plans such as Long-term or Contingency Plans.

Glossary term	Definition
Planning team	The wider group of stakeholders required to provide input to enable a viable planning process to occur.
people and animals	Individuals, families/whānau and communities, including animals.
Public Information Management (PIM) (function)	The function that prepares, distributes and monitors information to and from the media and the public.
Readiness [to respond]	One of the 4Rs of emergency management. Readiness involves developing operational systems and capabilities before an incident happens. <i>See 4Rs.</i>
Recovery (function)	The function in CIMS for ensuring that the response considers how the affected community can be supported to recover and that decisions or actions (or lack of) made during response consider any implications for recovery. It is also responsible for beginning initial recovery planning and establishing recovery team resources.
recovery	The co-ordinated efforts and processes used to bring about the immediate, medium-term, and long-term holistic regeneration and enhancement of a community following an emergency.
Regional level response	The third level of official response (between the local and national levels).
resources	All personnel, supplies, facilities and equipment available, or potentially available, for assignment to incidents.
Resource Request	A formal request by a function, support agency or Coordination Centre for personnel, vehicles, plant or equipment required for incident functions or tasks.
response	One of the 4Rs of emergency management. Response is the actions taken immediately before, during or directly after an incident that save or protect lives and property and that bring the consequences to a point of stability. <i>See 4Rs.</i>
response element	A team, or group, that makes up part of the response. It might be a single small team or all of the personnel and equipment assigned to a Controller. Each element should consider all of the CIMS functions, even if all are carried out by a single individual.
Response Manager	A Response Manager assists the Controller and oversees activity in the Coordination Centre. Some agencies use the terms Chief of Staff.
Risk advisor	A person dedicated to monitoring, assessing and advising the Controller of risks related to a response or recovery.
risk management	The process of analysing exposure to risk and determining how to manage that exposure.
[risk] reduction	One of the 4Rs of emergency management. [risk] Reduction involves identifying and analysing long-term risks to life and property, taking steps to eliminate these risks if practicable, and reducing the magnitude of their impact and their likelihood of occurring. <i>See 4Rs.</i>

Glossary term	Definition
Safe Forward Point	A safe location near the incident used mainly as a meeting place for personnel.
Safety (function)	The function that supports the Controller to ensure that all those involved in a response or recovery are kept safe in accordance with the requirements of the Health and Safety at Work Act 2015.
Safety Advisor	Safety Advisors are assigned to monitor safety conditions, and develop measures for making sure all personnel stay safe.
Science Advisor	An advisor with the specialist skills or knowledge in a particular science that is needed to support incident operations (e.g. geo-science, weather, forensics, medical, etc.).
SitRep	See <i>Situation Report (SitRep)</i> .
Situation Report (SitRep)	A brief description of an incident, usually given at regular intervals.
situational awareness	An understanding and appreciation of the complexities of an incident, including an understanding of the environment, the situation, likely developments, and implications
SOP	See <i>standard operating procedure (SOP)</i> .
span of control	The number of groups or individuals that one person can successfully supervise or manage.
Staging Area	A designated location where resources are gathered and prepared before being sent to the incident area.
standard operating procedure (SOP)	Written practices adopted by an agency. Standard operating procedures describe how actions or functions are performed.
Status Report	An internal verbal or written update on a function of cluster's progress that is created between SitReps.
strategic	The macro dimension of emergency management. It can have both a domestic and international focus and relates to the strategic aim or purpose of the government, local government or agency.
strategy	The general direction of operations, best defined as 'what we need to do'. A strategy may be a broad general statement about what needs to be completed or it may be a number of prioritised goals.
support agency	Any agency or organisation, other than the lead agency, that has a role or responsibilities during a response.
support agency representative	A support agency representative is an agency representative that coordinates with other agencies during an emergency. Support agency representatives may attend the Coordination Centre occasionally, or be present full-time.
tactical	Involves task-specific planning and actions to achieve a strategy. The tactical level is where the operation or campaign is executed.
Technical Advisor	An advisor with the specialist skills or knowledge in a particular technical area that is needed to support incident operations (e.g. mining, engineering, cultural, etc.).

Glossary term	Definition
tempo	The rate at which activities in the operational period occur. This is usually established by the Controller, but can be driven by external factors, e.g. subsequent or other incidents, political drivers or an adverse unforeseen consequence of the response.
Unified Control	An application of command and control used to bring control of an incident to one combined decision-making body when two or more agencies assume joint lead of a response.
Welfare (function)	The function responsible for ensuring planned, coordinated and effective delivery of welfare services to individuals, families/whānau and communities, including animals that are affected by an incident.