# THE NEW ZEALAND COORDINATED INCIDENT MANAGEMENT SYSTEM (CIMS)

**2nd edition**

Safer communities through integrated emergency management

New Zealand Government

The New Zealand Coordinated Incident Management System (CIMS)

2nd edition

April 2014

ISBN 978-0-478-43500-9

Published by 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 first edition published in 1998 by the New Zealand Fire Service Commission.

# Foreword

New Zealand's Coordinated Incident Management System (CIMS) establishes a framework of consistent principles, structures, functions, processes and terminology that agencies can apply in an emergency response. First introduced in 1998, CIMS has significantly enhanced the coordinated response capability in New Zealand, particularly at the incident level.

This second edition of CIMS builds on the first by incorporating experience gained since 1998. In particular, it reflects the lessons identified from the responses to a number of large scale and complex emergencies that occurred in New Zealand from 2010-2012. These emergencies emphasised the importance of CIMS, but also subjected the system to new levels of examination, and identified areas where it needs strengthening. Accordingly, this edition of CIMS also gives effect to recommendations from formal reviews and inquiries into those emergency responses, including:

- The Royal Commission on the Pike River Coal Mine Tragedy;
- The Independent Review of the Civil Defence Emergency Management Response to the 22 February 2011 Christchurch Earthquake;
- The Canterbury Earthquakes Royal Commission;
- The Independent Review of Maritime New Zealand's Response to the MV Rena Incident on 5 October 2011; and
- The CTV Building Coronial Inquest (22 February 2011 Christchurch earthquake).

This revised CIMS establishes a modular and scalable framework for consistent response at any level – from a small, single agency response to a larger, multi-agency response that may require coordination at the community or incident level or higher. CIMS enables agencies to plan for, train and conduct responses in a consistent manner, without being prescriptive. With this approach CIMS is an essential tool in New Zealand's preparedness to effectively respond to emergencies.

However, CIMS will not guarantee effective response management by itself. Successful and effective response rests in the understanding and application of the CIMS concepts by agencies. The responsibility is therefore upon agencies to note and apply CIMS appropriately.

I commend the collaborative efforts of multiple agencies in revising CIMS. Together we can make communities safer through integrated incident management.

**Andrew Kibblewhite**
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 (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 the Prime Minister and Cabinet

Maritime New Zealand

Ministry for Primary Industries

Ministry of Civil Defence & Emergency Management

Ministry of Health

Ministry of Social Development

National Rural Fire Authority

New Zealand Customs Service

New Zealand Defence Force

New Zealand Fire Service

New Zealand Police

The Ministry of Business, Innovation and Employment participated in 2013 for the purpose of developing an Underground Mines Emergency Protocol

 

# Contents

 

# 1 INTRODUCTION

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

This second edition of CIMS builds upon and replaces the first version that was commonly referred to as the 'Blue Book'. It describes how New Zealand agencies use the CIMS framework to coordinate, command, and control incident response of any scale, how the response can be structured, and the relationships between the respective CIMS functions and between the levels of response. It is the primary reference for incident management in New Zealand.

For the purpose of CIMS an incident is an occurrence that needs a response from one or more agencies. Most incidents are emergencies, though CIMS may also be used to manage incidents that are not emergencies, such as large public gatherings and events. Incidents range from small to large; simple to complex; and can be managed at one or multiple levels.

The CIMS framework is developed by a Steering Group consisting of representatives of all the CIMS stakeholder agencies[1] and it is endorsed by the Officials Committee for External and Security Coordination (ODESC). In the future CIMS will be reviewed every five years.

## 1.1 PURPOSE – A COMMON YET MODULAR FRAMEWORK

The purpose of CIMS is to achieve effective coordinated incident management across responding agencies by:

- establishing common structures, functions and terminology used by agencies in incident management, yet within a framework that is flexible, modular and scalable so that it can be tailored to circumstances specific to any level or type of incident; and
- enabling agencies to develop their own processes, procedures and training for the execution of CIMS.

## 1.2 AUDIENCE

The intended audience of CIMS is:

- agency planners and standard operating procedure (SOP) developers
- trainers and professional development personnel (internal and external)
- personnel who have responsibilities in a coordination centre (CC) (see Appendix D *Glossary and acronyms* on page 61 for a full definition), and
- plan and SOP owners (chief executives/managers).

[1] See Acknowledgements on page ii for a list of CIMS stakeholder agencies.

## 1.3 WHEN TO USE CIMS

CIMS is a valuable tool to provide structure, roles, and processes to teams managing incident response. It can be used to provide effective management of a wide range of incidents, including:

- biosecurity incursions
- environmental incidents
- fire
- food safety incidents
- hazardous substance incidents
- marine mammal strandings
- mass maritime arrivals
- multiple or mass casualties
- natural hazard incidents
- communicable disease outbreaks and pandemics
- planned events (for example, celebrations, parades, concerts, official visits)
- public disorder
- public health and medical emergencies
- search and rescue
- transportation accidents, and
- technological failures.

CIMS describes the fundamental elements of response structures, functions, processes, and common terminology. Individual agencies will use CIMS to develop their own standard operating procedures (SOPs) for response that are suited to their unique responsibilities, resources, and legislative authority.

# 2 CIMS FOUNDATIONS

This section describes the foundations of CIMS, including emergency management, legislation, and CIMS principles. It also covers the relationship between doctrine, training and operations, and between coordination, command and control, as well as describing the agency and team response roles.

## 2.1 EMERGENCY MANAGEMENT

CIMS is intended for emergency and non-emergency incidents, but it will most often be applied during emergencies. For the purposes of CIMS, an emergency is defined as a situation that poses an immediate risk to life, health, property, or the environment that requires a coordinated response.

The **components** of emergency management are referred to as the '4Rs'. They are:

- risk reduction
- readiness (to respond)
- response, and
- recovery.

CIMS is applied during response, and therefore must be factored into readiness.

Risk reduction is covered by other measures (such as health promotion, the *Building Code*, or the *Resource Management Act 1991*).

Recovery may use CIMS, business-as-usual arrangements, or an organisation set up specifically for recovery. Recovery needs to be included in readiness planning, and is commenced at the start of a response.

Responses aim to manage the consequences of hazards, support the affected communities, and establish the basis for recovery. Common response **objectives** that provide guidance to responders are listed below. They are not listed in priority order, and vary depending on the incident:

- preserve life (including ensuring responder safety)
- prevent escalation of the emergency
- maintain law and order
- care for the sick, injured, and dependant
- provide essential services
- preserve governance
- protect assets, including buildings and their contents
- protect natural and physical resources
- provide animal welfare, and
- preserve economic and social activity.

## 2.2 LEGISLATION

Agencies use CIMS when developing plans and processes to meet their specific legislative requirements, both before and during an incident. The legislative framework gives agencies the authority to act and the means to work together. Emergency related legislation may give response personnel emergency powers of compulsion, entry, direction and removal. Incident management may occur without these powers being activated.

Various pieces of legislation have provisions to activate and use emergency powers when necessary, including, but not limited to:

- *Health Act 1956*
- *Fire Service Act 1975*
- *Forest and Rural Fires Act 1977*
- *Defence Act 1990*
- *Resource Management Act 1991*
- *Biosecurity Act 1993*
- *Maritime Transport Act 1994*
- *Hazardous Substances and New Organisms Act 1996*
- *Terrorism Suppression Act 2002*
- *Civil Defence Emergency Management Act 2002*
- *Local Government Act 2002*
- *Epidemic Preparedness Act 2006*, and
- *Policing Act 2008.*

Some statutes require a state of emergency to be declared before the use of emergency powers, while other statutes allow for the use of emergency powers by appropriately appointed people. In all cases there is an expectation that responses will be coordinated across agencies.

## 2.3 CIMS PRINCIPLES

CIMS is based on the following principles:

*1) Common structures, roles, and responsibilities*

Common structures, roles, and responsibilities make it possible for agencies to work effectively alongside each other, and for personnel to interchange roles. They facilitate information flow and understanding by creating parallel structures and appointments.

*2) Common terminology*

Common terminology is essential in incident management, especially for multi-agency responses. When agencies have slightly different meanings for terms, confusion and inefficiency can result. Common terminology for functions, processes, and facilities prevents this, improves communications between organisations, and allows faster and more effective responses. Refer to Appendix D *Glossary and acronyms* on page 61 for definitions of the terms commonly used in incident management.

 

*3) Modular and scalable*

The modular and scalable CIMS structure is flexible and can be applied to all responses and to all levels within a response. Agencies may adapt their response structures prior to a response to suit their specific needs, and during a response to reflect changing circumstances. Refer to section 3.4 *Scaling responses* on page 17 for more detail.

*4) Responsive to community needs*

All responses aim to mitigate and manage the consequences for the affected community. This requires response personnel to effectively communicate with communities, understand their needs, and base their response and recovery actions on these needs. Communities will actively participate in a response rather than wait passively for assistance. Community response actions need to be coordinated with the official response.

*5) Integrated response coordination*

Integrated response coordination is the organisation of the responding agencies into a single, cohesive response. Section 3.5 *Integrated response coordination* on page 20 discusses this in more detail.

Consolidated action planning is a key component of integrated response coordination, as are resource coordination, and integrated information management and communications (see below).

*6) Consolidated action planning*

Action Plans describe response objectives, agency and team tasks, and the measures 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. A multi-agency Action Plan must have input from all support agencies to be effective.

Appendix A, *Action Plan process* on page 44 describes how to develop an Action Plan, and suggested content is listed in *Recommended content for Action Plans* on page 57 of Appendix C.

*7) Integrated information management and communications*

Integrated information management and communications enable effective information sharing, supporting more effective action planning and response coordination, as well as wider situational awareness. It aims to establish a common operating picture (an understanding of the situation based on the best available information, shared between all response agencies), and requires a common communications plan, standard procedures, clear text, common communication means, and common terminology.

*8) Resource Coordination*

Resource coordination organises resources across all response agencies. Agencies inform each other of their available capabilities and resources so that procurement and use of resources can be managed efficiently. Lead agencies monitor resource information, and may set priorities for allocating critical resources. This consolidates control of resources, maximises resource use, provides accountability, and improves situational awareness.

*9) Designated response facilities*

Designated response facilities with clearly defined functions assist in effective incident management (see section 3.6.1 *Facilities* on page 21).

*10) Manageable span of control*

Span of control means the number of individuals or teams one person can manage effectively. The optimum span of control is between two and seven.

## *Supporting intentions*

In addition to the principles there are three supporting intentions:

*1) Common training standards and accreditation*

Common training standards, supported by accreditation, help to ensure that personnel in key positions have the requisite skills and experience to perform their roles, and to provide equivalence between organisations. Common training enhances personal relationships between agency personnel and may provide economies of scale.

*2) Regular review*

Regular review of CIMS ensures its effectiveness and relevance. Lessons are only learned when doctrine is amended and training is updated to reflect the new information.

*3) International compatibility*

Maintaining international compatibility ensures that New Zealand agencies and personnel are able to operate effectively with overseas organisations and personnel, and enables New Zealand response agencies to more easily analyse and incorporate lessons from overseas experience.

## 2.4 DOCTRINE, TRAINING AND OPERATIONS

Doctrine is the body of principles and practices that guide an agency's actions in support of their objectives. It is authoritative, but requires judgement in application.

CIMS is an element of emergency management doctrine that agencies use to manage incidents. To be effective, doctrine needs to be supported by robust education, training, and professional development.

Doctrine informs training, ensuring that the correct material and content is taught. Training then lays the foundation for effective response operations. Experience has shown that doctrine is not applied during response if personnel have not received sufficient training.

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

The relationships between doctrine, training, and operations are shown in Figure 1 below.

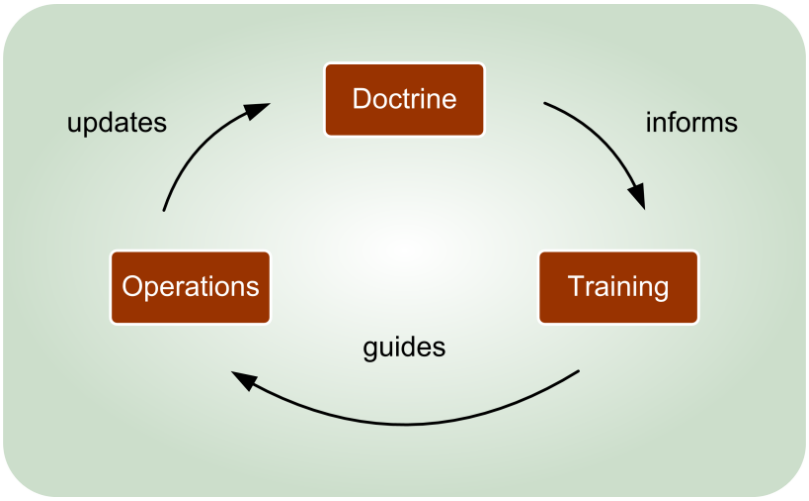


**Figure 1 The relationship between doctrine, training, and operations**

## 2.5 COORDINATION, COMMAND AND CONTROL

Command and control define who has the authority to make decisions, and what the parameters of that authority are.

**Coordination** is the bringing together of agencies and resources to ensure a unified, consistent, and effective response. Command and control assist with coordination by defining authority between and within agencies.

**Command** (authority within an agency) is executed vertically within each agency, and includes the internal ownership, administrative responsibility, and detailed supervision of an agency's personnel, tasks, and resources. Command cannot normally be exercised outside an agency.

**Control** (authority across agencies) is executed horizontally, and is the authority to direct tasks to another agency, and to coordinate that agency's actions so they are integrated with the wider response. Control authority is established in legislation or in an emergency plan. Control does not interfere with another agency's command authority to supervise or organise its personnel, resources, and how its tasks are conducted.

Agencies can apply command and control within their own structures at department, unit, or team level.

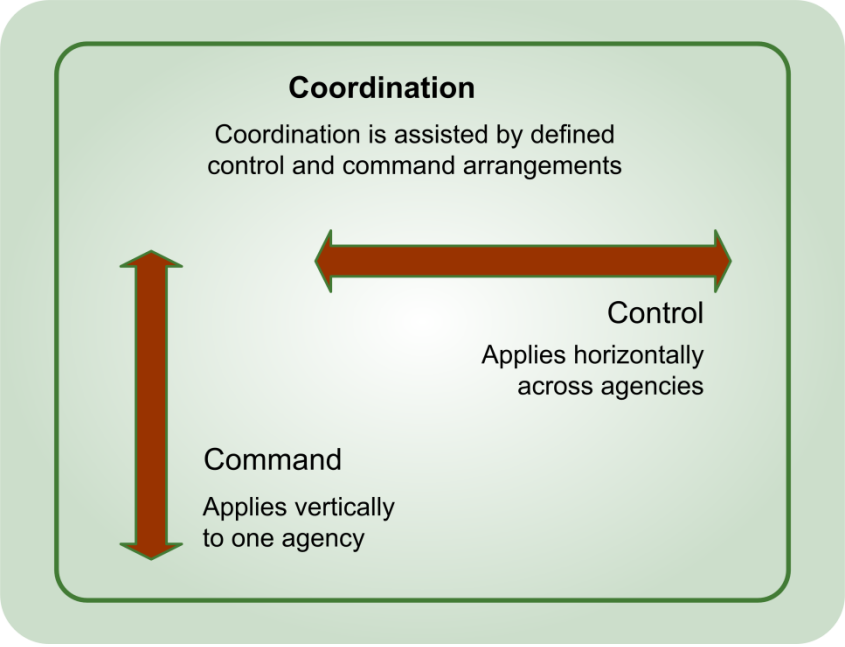


**Figure 2 Coordination, command, and control**

## 2.6 LEAD AGENCY, SUPPORT AGENCY AND UNIFIED CONTROL

A **lead agency** is the agency with a mandate to manage the response to an incident through legislation, under protocols, by agreement, or because it has the expertise and experience. The lead agency establishes control to coordinate the response of all agencies involved.

The lead agency may change between risk reduction, readiness, response, and recovery. It may also change as the incident progresses, if the required authority or expertise changes.

When the lead agency cannot be readily identified, response agencies may adopt a joint 'Unified Control' structure (see below).

A **support agency** is an agency that provides support to the lead agency in a response. The lead agency tasks and coordinates support agencies' resources and actions. The type of incident determines which support agencies are involved, and these agencies may change as the response progresses.

While an agency may have the lead for a particular response, support agencies often have statutory responsibilities and specific objectives of their own, which the lead agency needs to accommodate.

The lead agency is responsible for ensuring arrangements and plans are in place prior to incidents where they will have the lead. Support agencies are responsible for assisting in the development of these. Integration of support agencies into the response is a fundamental responsibility of lead agencies.

**Unified Control** is when the control of an incident is shared between two or more agencies by agreement through a combined decision-making body. The command appointments for each agency establish an agreed concept of operations and a single Action Plan. Unified Control is usually applied when:

- more than one agency has a mandate to manage a particular incident
- it is unclear if any agency is the lead, or
- the lead agency determines that a joint approach will be more effective.

Agencies applying Unified Control establish a joint coordination centre (CC), with key appointments filled by the most appropriate personnel from any agency. Agency command appointments do not have to be present at all times, but need to come together to agree on key decisions.

Other than a combined Control function, the joint CC follows usual CIMS practices.

# 3 RESPONSE MANAGEMENT

This section describes response management, including the CIMS functions, the incident management team, response levels, scaling responses, integrated response coordination and the protocols that support response management.

## 3.1 THE CIMS FUNCTIONS

Incident responses require a wide range of information to be analysed and activities to be carried out. CIMS divides the resulting tasks and responsibilities into seven functions to enable multiple agencies to coordinate resources effectively, and make it easier for their personnel to work alongside each other. Figure 3 below shows the seven functions:

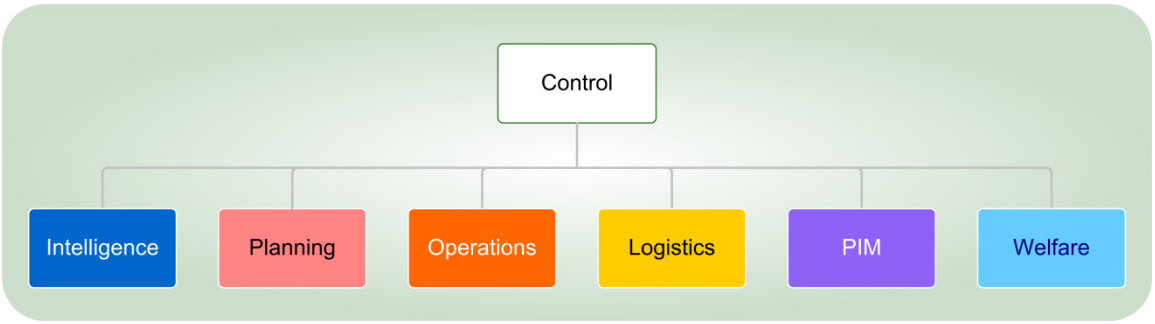


**Figure 3 CIMS functions**

All the CIMS functions need to be considered at an incident, whether they are carried out by a single person in charge of a small response, or by teams of personnel in a major response. Agencies may condense or amend the functions to suit their requirements and the specific objectives for a particular incident.

The responsibilities for each of the functions are summarised in Table 1 below. Detailed descriptions of the functions are given in 4.2 *CIMS functions* on page 28.

| Function | Responsibilities |
|---|---|
| **Control** | Coordinates and controls the response |
| **Intelligence** | Collects and analyses information and intelligence related to context, impact and consequences; also distributes intelligence outputs |
| **Planning** | Leads planning for response activities and resource needs |
| **Operations** | Provides detailed direction, coordination, and supervision of response elements on behalf of the Control function |
| **Logistics** | Provides personnel, equipment, supplies, facilities, and services to support response activities |
| **Public Information Management** | Develops and delivers messages to the public, directly and through the media, and liaises with the community if required |
| **Welfare** | Coordinates the delivery of emergency welfare services and resources to affected individuals, families/whānau, and communities |

**Table 1 CIMS functions**

## 3.2 INCIDENT MANAGEMENT TEAM

The Incident Management Team (IMT) assists the Controller by providing advice and specialist knowledge, and handling detailed work.

The members of the Incident Management team (IMT) are shown in Figure 4 below. In addition to the CIMS function managers, the Incident Management Team may include:

- a Response Manager
- technical experts with knowledge relevant to the incident, and
- risk advisors.

These additional appointments are described in *Other Control function roles* on page 30. The response elements or direct reports for a Controller should be arranged in a way that supports a manageable span of control, which is normally two to seven.

An additional person may be present during IMT meetings to record decisions (this person is not a member of the IMT).

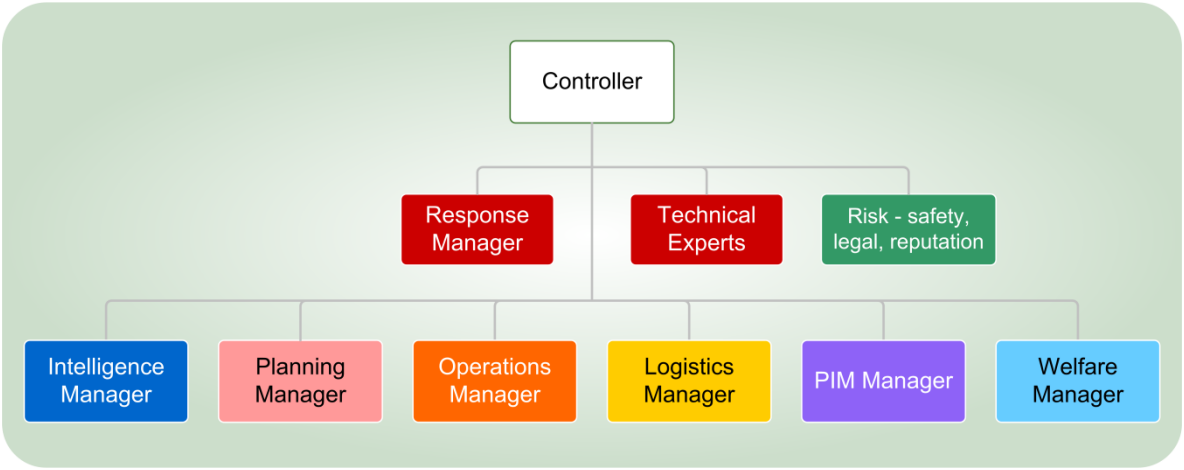


**Figure 4 Incident Management Team**

## 3.3 RESPONSE LEVELS

This section explains how CIMS operates at the various response levels.

CIMS provides a framework where a lower response level is supported and/or coordinated from the next higher level, when this is activated. The five response levels in CIMS are shown in Figure 5 below.

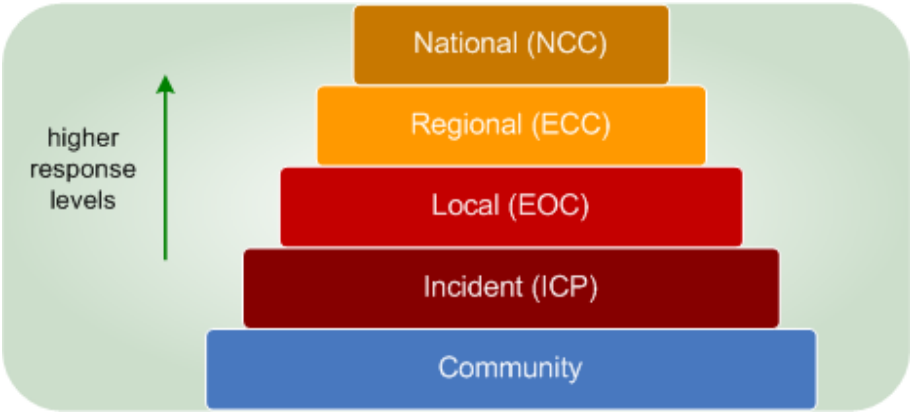


**Figure 5 Response levels**

Response levels are coordinated from coordination centres (CCs) - see section 3.6.1 *Facilities* on page 21 for more information about CCs.

| Response Level | Description |
|---|---|
| National | Includes agency coordination centres and headquarters, national level sector coordinating entities, and all-of-government coordination across national agencies.<br>Coordinated from National Coordination Centres (NCC). |
| Regional | Includes CDEM Groups, district health boards, enlarged rural fire districts, and regional agency offices.<br>Coordinated from Emergency Coordination Centres (ECC). |
| Local | Includes local authorities, rural fire districts, and agency offices at the local (district/city) level.<br>Coordinated from Emergency Operations Centres (EOC). |
| Incident | The first official level of agency response. It includes first responders.<br>Coordinated from Incident Control Points (ICP). |
| Community | The general public including individuals, families/whānau, community groups and businesses. |

**Table 2 Response level descriptions**

Most incidents only require the activation of one or two response levels. Generally only large scale incidents require all levels of response to be activated.

The following subsections describe each of the response levels in more detail. Also see section 3.4 *Scaling responses* on page 17 for further detail about incident and higher levels, how they can be structured and how they relate with each other.

### 3.3.1 Community level response

Communities, organisations and businesses self-respond to emergencies, either as part of official pre-existing arrangements or on their own in a spontaneous or emergent manner. Response agencies need to accommodate, link with, support and coordinate community participation in response.

Wherever possible, communities and the business sector should be appropriately incorporated in response coordination planning before incidents occur. Although CIMS is designed to apply to official response agencies, its principles can be applied at the community level where they form part of such pre-planned structures.

### 3.3.2 Incident level response

Incident level response is the first official level of agency response and is carried out by first responders. Response personnel conduct physical actions such as clearing obstructed roads, treating casualties, fighting fires and conducting rescues. Incident level response might have from one or two personnel to several hundred.

Initially, the 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 an incident grows in size or becomes more complex, the lead agency may assign a more senior or better qualified Incident Controller, and the Incident Controller may appoint others to perform relevant CIMS functions. An Incident Controller may also be a technical expert, for example, a mine expert in a mining incident. The Incident Controller coordinates and directs the response.

The coordination centre (CC) for an incident level response is the Incident Control Point (ICP). The Incident Controller must establish an ICP at or near the scene of the response or at a base for the coordination of team operations across an extended area (such as biosecurity teams on farm visits).

Several ICPs can be established when a response is required at various or dispersed sites. In such cases each ICP has an Incident Controller. ICPs can be supported, coordinated or directed by higher level response if required.

See section 3.4 *Scaling responses* on page 17 for further detail on the scaling of incident level response.

### 3.3.3 Local level response

The CC for a local level response is an EOC. EOCs are usually activated for the purpose of multi-agency or multi-incident coordination. It is staffed and managed by the lead agency, and supplemented by personnel representing, or provided by, other agencies.

The Local Controller controls the local level response for the incident, and directs, coordinates, and/or supports all ICPs and any support agencies. They also liaise with any ECCs and neighbouring EOCs when applicable.

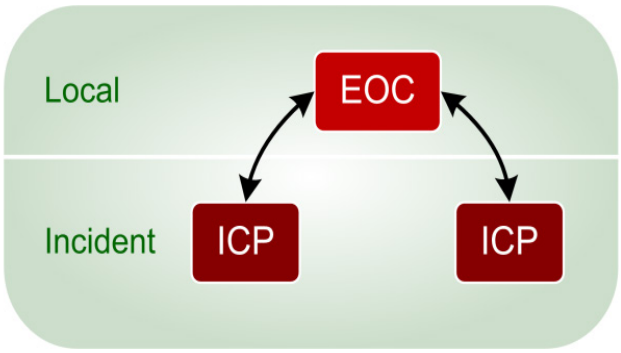


**Figure 6 EOC and ICP coordination**

When an EOC is established, Incident Controllers report to the Local Controller, while ICP personnel communicate with their peers in the corresponding EOC function. Supporting agencies work within the CIMS framework while applying their own SOPs.

Support agency personnel need to be incorporated in lead agency EOCs, either in functions or as Liaison Officers. Supporting agencies decide whether or not to activate their own EOCs.

### 3.3.4 Regional level response

A regional level response may be activated:

- to direct, coordinate, and support incidents with regional or national implications
- when a local response requires wider coordination, and
- when the Regional Controller or their governance deems it necessary.

The Regional Controller controls the regional level response for the incident, and directs, supports and coordinates local responses. The CC for a regional level response is an ECC.

ECCs communicate with EOCs, who in turn communicate with ICPs (see Figure 7 on page 15). ECCs 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.

When incidents cross jurisdictions, or jurisdictions are unable to fulfil their role, the ECC may support a neighbouring regional jurisdiction. ECCs may also activate to support a single responding EOC within their region.

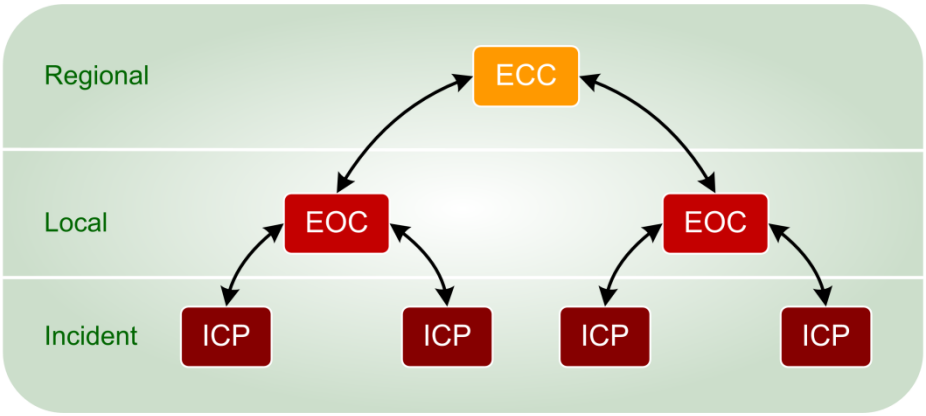


**Figure 7 ECC, EOC, and ICP coordination**

### 3.3.5 National level response

National level response includes a combination of the following layers:

- control from a National Coordination Centre (NCC), which can be based at the National Crisis Management Centre (NCMC),
- all-of-government coordination by the NCMC,
- agencies commanding their own resources from their own NCC while liaising with other agencies and the NCMC, and
- the system of Domestic and External Security Coordination (DESC).

When the response is nationally led, the lead agency NCC directs priorities, sets national objectives and manages national level coordination. Support agency NCCs maintain command of their own agency operations, ECCs maintain control of the regional level response and EOCs maintain control of the local level response (see Figure 8 on page 16), although with all levels subject to the direction of a National Controller.

Some support agencies may use their business-as-usual arrangements to support the response, rather than activating an NCC or response structure.

NCCs usually communicate with ECCs (rather than directly with EOCs or ICPs) to ensure national objectives are implemented and coordinated.

More information on the mechanisms of national level response is available in Appendix B *National response* on page 53.

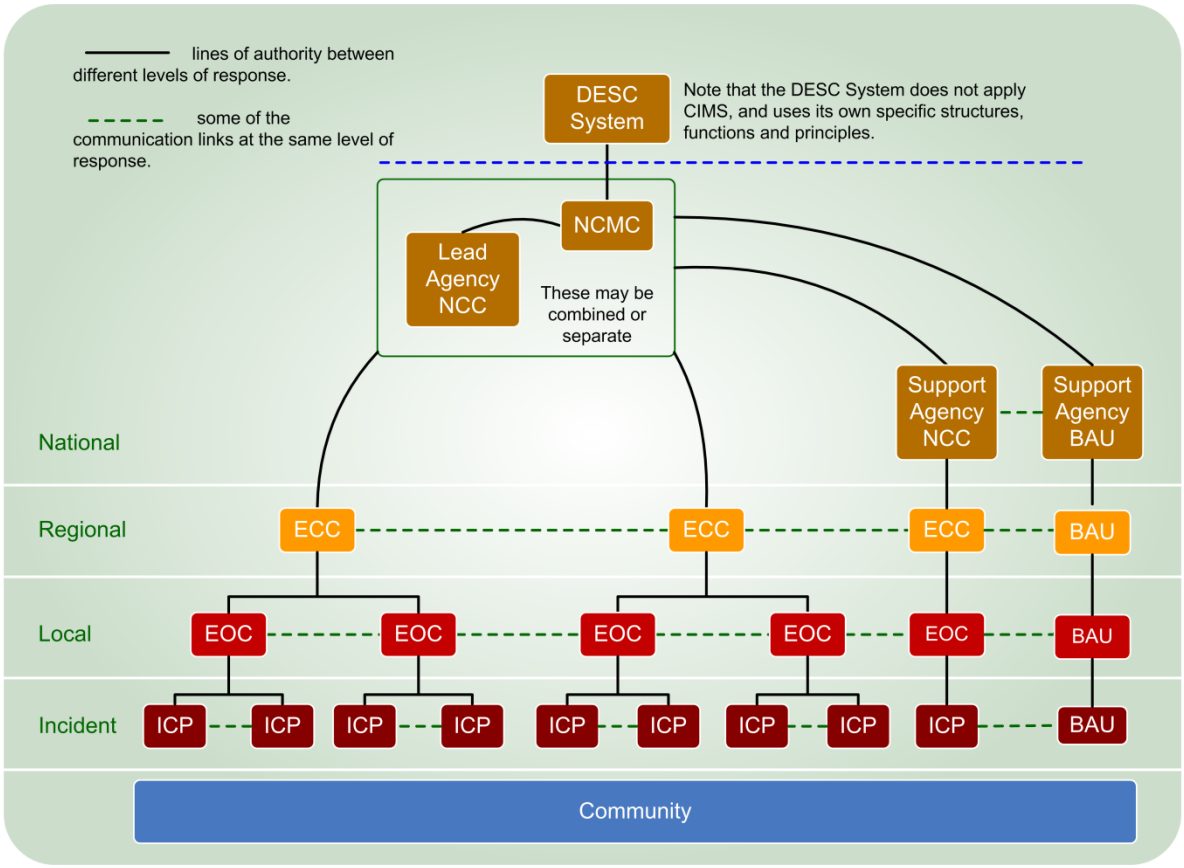


**Figure 8 Relationships between the different response levels**

### 3.3.6 Response level viewpoint

In a multi-level response, Controllers and IMTs at different response levels have differing timeframes to act in, and 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 and months. Likewise an Incident Controller may coordinate small teams, while a Regional or National Controller may coordinate the activities of thousands of response personnel.

These differing viewpoints require understanding on the part of all Controllers and response personnel. Likewise, Controllers and personnel need to adjust their viewpoint 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 Action Plan, but in greater detail and over a shorter timeframe. This is detailed in Appendix A, *Action Plan hierarchy* on page 50.

## 3.4 SCALING RESPONSES

CIMS can be scaled (expanded or contracted) to manage any type or size of incident. This section describes how responding agencies can transition from small scale, low level response coordination structures to larger scale, higher level structures and vice-versa.

Controllers assign functions (and sub-functions) to individual personnel or teams on a scale that reflects the requirements of the incident and the resources available. A protracted response may scale up and down several times depending on the nature of the incident and the required response. A decision to scale the response structure needs to be based on the:

- **safety** of the response personnel, the public, and property
- **size and complexity** of the incident, and the extent of response required, and
- **span of control.**

Action Plan development is affected by the scale of a response, and is covered in *Action Plan hierarchy* on page 50 of Appendix A.

### 3.4.1 Incident level: single agency, small incident

In a single agency incident level response, the personnel and resources are all from one agency, so command and control are relatively simple - there is one line of command. Minimal facilities are needed, and the ICP may be a single vehicle.

In this type of response, the senior first arriving responding officer becomes the Incident Controller and has responsibility for all the CIMS functions required for the response. This initial Incident Controller may be replaced later by a more senior agency officer.

The Incident Controller must consider all of the CIMS functions. For example, there may be victims requiring assistance, media present, or hazards to counter. Due to the small scale of the response, the Incident Controller is likely to assume some functions such as Public Information Management (PIM) but must be prepared to activate more functions if required. The functions most likely to be activated at this type of response are shown in Figure 9 below.

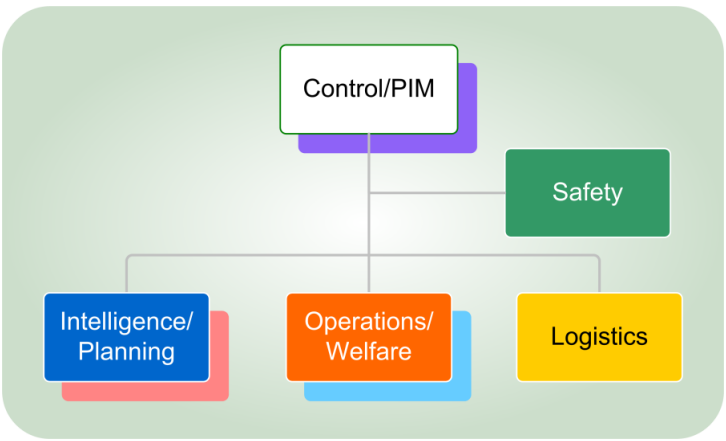


**Figure 9 Incident level: single agency**

The Incident Controller often retains responsibility for the PIM function but as more personnel become available, they may appoint function managers and establish an IMT. Functions likely to be combined are Planning and Intelligence, and Operations and Welfare. The combined functions may separate as the incident progresses.

### 3.4.2 Incident level: multi-agency

In this instance a single agency response progresses into a multi-agency response. The management structure expands to maintain effective control consistent with the scale and complexity of the response. The Incident Controller is likely to appoint CIMS function managers. If the Incident Controller changes, a detailed handover is required. This may be when a more senior or better qualified official assumes the role of Incident Controller, or if control has to be handed to the lead agency.

The Incident Controller, supported by the IMT, is responsible for overall direction of response activities across all responding agencies. This includes tasking and coordinating other support agencies, who action those tasks within their own command structures.

The Incident Controller needs to confirm their authority over support agency response elements if there is no pre-existing understanding, and consider appointing support agency Liaison Officers to the IMT.

Personnel from support agencies need to be included in the ICP to ensure access to their specialist knowledge and the incorporation of their agency's requirements and resources. This also gives the ICP more capacity to cope with the expanded scope and workload.

The most likely functions to be appointed at this level of response are shown in Figure 10 below.

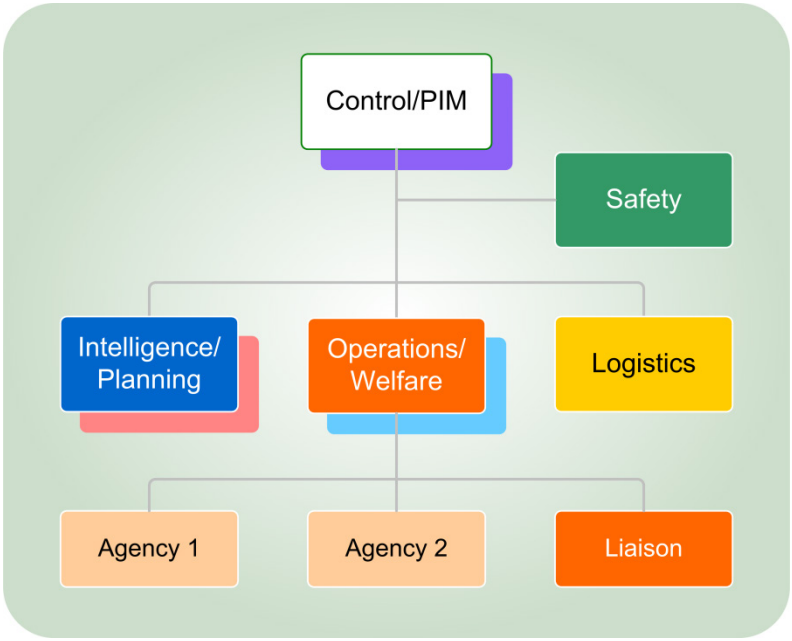


**Figure 10 Incident level: multi-agency**

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 Liaison is activated.

### 3.4.3 Incident level: major incident

When an incident level response becomes protracted and/or large scale, a full IMT may be required. The response site may be divided into sectors, each with an assigned leader reporting to the Incident Controller who coordinates and directs the response from the ICP. The functions may divide further into sub-functions to ensure all aspects of the response are addressed properly. Teams are assigned to the function managers as appropriate.

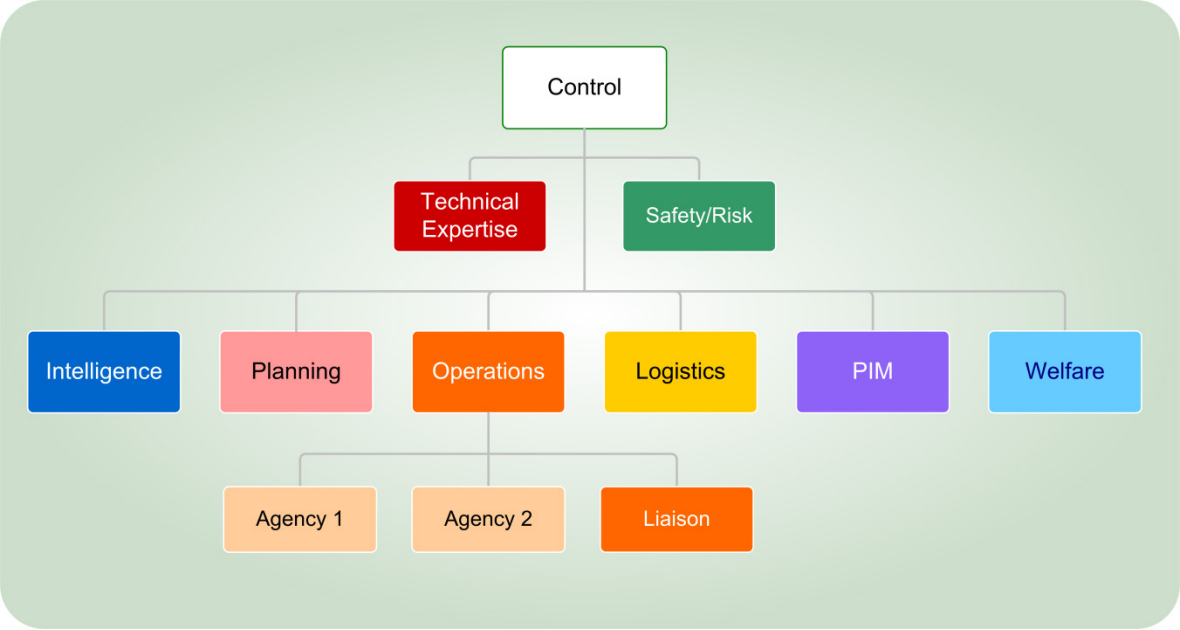


**Figure 11 Incident level: major incident**

More substantial or pre-prepared response coordination facilities may be required, and personnel rosters need to be developed.

Scaling may also be from larger to smaller-scale coordination structures as incidents are brought under control or as the intensity of responses decline. A protracted response may scale up and down several times depending on the nature of the incident itself and the response necessary.

### 3.4.4 Local, regional, and national level

An EOC is established to coordinate multi-agency or multi-incident response between respective ICPs. An EOC is activated:

- when there are several incident level responses at different sites,
- when off-site coordination and support are required, or
- to coordinate multi-agency or multi-incident responses.

Each site has an Incident Controller (possibly with an IMT) and assigned response elements, but these sites require coordination between them and potentially additional support provided by contributing agencies. The Local Controller needs to:

- define their command and control relationship with the Incident Controllers at each 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

Scaling up a response from local level to regional level involves the same steps, as does a scaling up from regional to national. Scaling a response down requires a transfer of authority, responsibility, and resources from a higher CC to a lower one. This needs to be formalised in a document outlining the transfer.

## 3.5 INTEGRATED RESPONSE COORDINATION

The objective of integrated response coordination is to organise the participating response agencies and response levels into a single, cohesive response.

The lead agency integrates support agencies into the response by:

- frequent communication between Controllers
- ensuring close and on-going inter-agency Liaison
- including support agency personnel in the lead agency CC and in the response planning process
- including support agencies in the development and implementation of Action Plans, and
- ensuring coordinated communications and information sharing.

The lead agency Controller and Incident Management Team (IMT) are responsible for coordinating agency response activities, with agencies managing their own personnel and resources.

Integrated response coordination:

- requires consolidated planning, resource coordination, and integrated information sharing and communications
- may be **explicit** (briefings, instructions, and documents such as Action Plans) or **implicit** (discussions, planning, liaison, and working together)
- is more effective when information, intelligence, and response coordination facilities are shared (when practicable), and
- applies vertically (between response levels) and horizontally (between agencies).

## 3.6 SUPPORTING PROTOCOLS

This section covers facilities, assigning personnel, changeovers, movement control, risk management, and personnel identification.

### 3.6.1 Facilities

Response facilities are used at every response level to coordinate the response, hold resources, and/or deliver services (see section 3.3 *Response levels* on page 12 for more information).

Response facilities need to be clearly identified by signage and documentation so their purpose and location is clear. For example, 'Wainui Police EOC' would be the Police local coordination centre at Wainui. Designation of facilities is normally included in the coordination section of an Action Plan.

#### *Coordination centres*

A coordination centre (CC) is where the Controller and IMT manage their response from. It needs to be large enough to accommodate all the personnel, equipment, and facilities required to effectively manage the Controller's response element. The CC may be as small as a single vehicle or desk, or as large as an entire building with dozens of personnel. There are four types of CC:

- **Incident Control Point (ICP)** is an incident level CC. There is only one ICP at an incident level response site; separate ICPs may be established at other response sites.
- **Emergency Operations Centres (EOCs)** are local level CCs
- **Emergency Coordination Centres (ECCs)** are regional level CCs, and
- **National Coordination Centres (NCCs)** are national level CCs.

#### *Assembly Areas*

Assembly Areas may be required if there is a significant amount of resources being mobilised. They are used by Logistics for receiving incoming resources, organising and storing them, and then transporting them to where they are needed. They are normally established at local, regional, and national response levels.

#### *Staging Areas*

Staging Areas are used for gathering and organising resources at incident level responses. If an incident grows, more staging areas may be needed. A Staging Area provides a safe location for:

- resources to be received and held prior to deployment
- resources to prepare 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).

Staging Areas are managed by Operations, who work with Logistics when resource management is required. 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.

Considerations when establishing Staging Areas include:

- proximity to the location where assignments are made
- safety of the location
- having separate entrances and exits
- placing them off main traffic routes, but where they can still be easily located
- ensuring they are able to accommodate anticipated levels of resources
- whether separate locations are required for different types of resources, and
- any potential environmental damage by vehicles or personnel.

### *Safe Forward Points*

A Safe Forward Point is a safe area at an incident level response. Managed by Operations, the Safe Forward Point is used mainly as a meeting place for personnel. Resources called forward for deployment may be held at the Safe Forward Point for final briefings, or to await movement to their task areas.

## 3.6.2 Assigning personnel

The Controller should appoint function managers on the basis of:

- skills from experience and formal training
- personal attributes, particularly being able to handle stressful situations, and to work as part of a team
- relevant technical knowledge, and
- ability to have an effective relationship with the Controller.

### *Primary and secondary appointments*

In large scale responses, key appointments such as the function managers need to have a primary and one or more people assigned as secondary (or deputy) appointments. The primary appointment needs to be rostered at times when key response activities are happening. Secondary appointments are rostered on for less active periods, and manage on the basis of the systems, processes, and decisions made by the primary appointment to ensure continuity of direction.

During longer responses it may be necessary to rotate personnel appointed to both primary and secondary key appointments.

### 3.6.3 Managing changeovers

Changeovers are a major factor in incident management effectiveness and efficiency. During changeovers, incoming personnel are briefed by the personnel they are replacing. The IMT plan and manage changeovers, and need to ensure:

- outgoing personnel leave once they have briefed their replacements
- changeovers:
  - increase personnel safety and reduce risk
  - do not disturb response operations, and
  - are staggered to ensure continuity of response operations.

Table 3 below summarises the responsibilities for outgoing and incoming personnel.

| Outgoing personnel | Incoming personnel |
|---|---|
| Set changeover time and locations, and inform incoming team | Receive briefing |
| Brief subordinate personnel | Manage changeover of subordinates |
| Brief replacement | Ensure Action Plan is understood |
| Leave | Plan the next changeover |

**Table 3 Changeover responsibilities**

Changeovers need to be based on a roster which assigns response personnel to a particular shift. Depending on the level or scale of the response, the rosters may be developed by the Controller, Operations Manager, Logistics Manager, or the Personnel or Administration sub-functions, with input from the other function managers.

### 3.6.4 Movement control

Managing movement at incident level responses reduces the risks for response personnel and the public, as well as interruptions to operations. Movement control is also required during evacuations. Movement control may use cordons, road blocks, checkpoints, and/or contra-flow traffic.

#### *Cordon*

A cordon restricts movement into and out of an area, using equipment, personnel, and the area's natural features to assist with restricting movement.

An **inner cordon** is established directly around incident level response operations, and only personnel from the responding agencies operate in this inner cordon. All other people are evacuated.

An **outer cordon** is established further from the incident level response operations and is used to control access to the area of operations. The Safe Forward Point, Staging Area, and other agency specific facilities are usually sited between the inner and outer cordons.

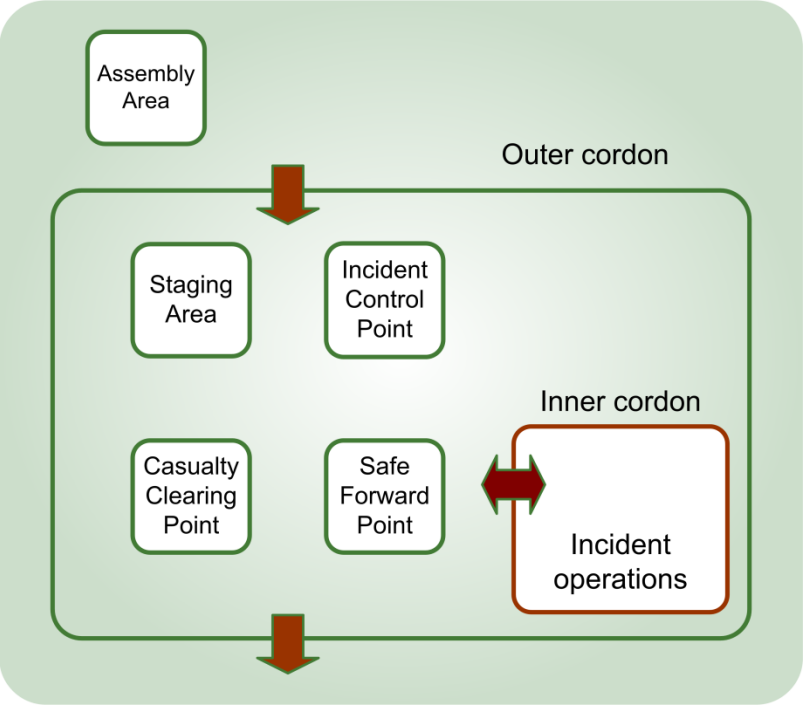


**Figure 12 Cordons**

### *Road-block*

A road-block is any barrier or obstruction preventing or limiting the passage of vehicles. It is used to control who comes into or leaves an area.

### *Checkpoint*

A road checkpoint is a position used to observe and control traffic. Traffic may be stopped but no physical obstruction is placed on the roadway to prevent access.

### *Casualty clearing point*

Casualties are moved from the inner cordon to a casualty clearing point for secondary triage and treatment. If required, ambulances are loaded here to convey casualties to medical facilities.

### 3.6.5 Risk management

Risk management is the process of analysing exposure to risk, and determining how best to handle that exposure. The specific risk management considerations depend on the objectives of the response. Examples of risk management considerations within CIMS are:

- safety for response personnel and members of the public
- legal issues, and
- the reputations of the associated response and governance organisations.

Controllers must ensure that their response element uses effective risk management practices, and that every function contributes to risk management.

For further detail on risk management, refer to *AS/NZS ISO 31000:2009 Risk Management – Principles and guidelines*

### 3.6.6 Personnel identification

Functions and roles are identified on vests, nametags, or armbands by colours and text.

It is particularly useful to recognise personnel by function during changeover, for visitors, or for other agencies' personnel. Identifying colours or other identification are primarily used in CCs at local, regional, and national levels. They may be used at incident level, though agency procedures may require other identification. Table 4 lists the CIMS function colours.

| Colour | Function |
|---|---|
| White | Controller |
| Red | Control personnel (including assistants, and technical experts) |
| Dark Blue | Intelligence |
| Pink | Planning |
| Orange | Operations |
| Yellow | Logistics |
| Purple | Public Information Management |
| Light Blue | Welfare |
| Green | Safety/Risk Management |
| Grey | Recovery |

**Table 4 Identification colours for CIMS functions**

# 4 RESPONSE MANAGEMENT FUNCTIONS

This section describes the structure and functions used in the CIMS framework to best manage incident responses.

## 4.1 CIMS STRUCTURE

Figure 13 below shows the overall CIMS structure at a CC where all the functions and sub-functions are activated.


**Figure 13 Overall CIMS structure at a CC (all functions).**

The following paragraphs describe Governance and detail the CIMS functions. As noted previously, agencies may condense or amend the functions (particularly the sub-functions) to suit their requirements and the specific objectives for a particular incident.

### 4.1.1 Governance

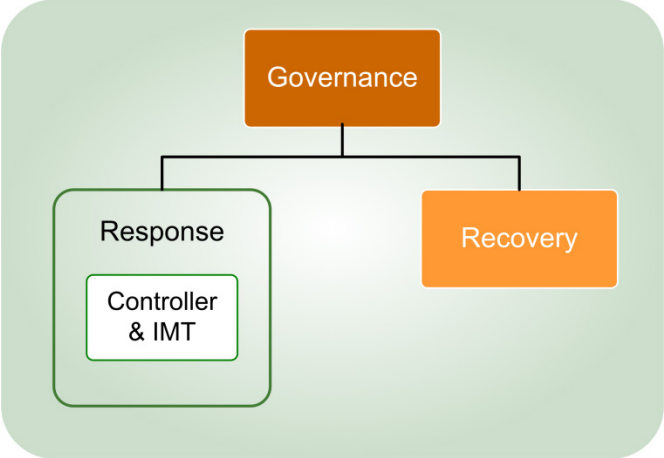


**Figure 14 Governance**

Every response has executive oversight, known as Governance. It may be carried out by chief executives, senior agency managers or by political leaders. Governance has ultimate responsibility for the response, but delegates authority and operational control to a Controller.

Governance arrangements are determined by legislation and agency procedures. Examples of governance for different levels of response are:

- communications centre giving instructions to response personnel (incident level),
- senior officials within an agency,
- elected officials or board members, and
- Domestic and External Security Coordination (DESC) system for national responses (see Appendix B *National response* on page 53 for more information).

Governance may provide terms of reference, delegation of authority, or other directives that state the required response achievement, preferably in written form. Such directives are then used as a basis for action planning.

Governance is generally limited to responsibilities relevant to the specific level of response. Examples of governance responsibilities are:

- making strategic, rather than operational decisions,
- providing high-level support, advice, and direction to the response,
- activating a significant response and allocating the delegated resources,
- declaring, extending, or ending a 'state of emergency',
- providing a spokesperson,
- liaising with other levels of governance, and
- deciding on special funding arrangements.

Recovery is outside the scope of CIMS, but Governance also oversees recovery, and may direct a Controller to carry out early recovery actions as part of the response.

Governance elements need to be briefed regularly by the Controller on developments, activities, planning, and messages that need to be delivered to the media and the public.

## 4.2 CIMS FUNCTIONS

This section describes each of the seven CIMS functions in turn.

### 4.2.1 Control (function)

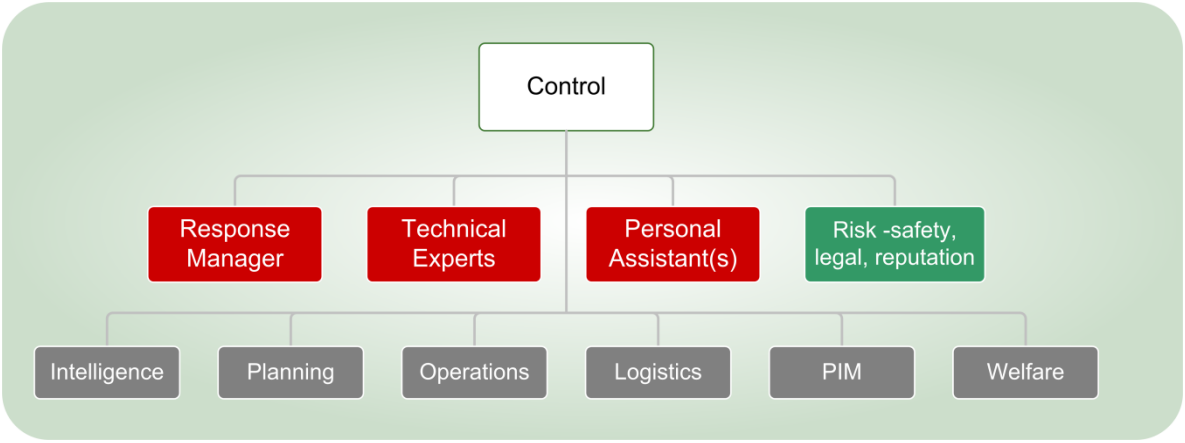


**Figure 15 The Control function**

Control is responsible for coordinating and controlling the response element. The IMT is headed by the Controller. 'Controller' is used for the person with the responsibilities described below, although the title may vary between agencies and response levels. The Controller may be supported by a Response Manager, technical experts, personal assistant(s), and risk advisors.

The Controller is responsible for:

- setting objectives and providing an Action Plan that describes how they will be achieved
- directing the response
- ensuring responder and public safety
- controlling personnel and equipment, and all subsidiary response elements
- ensuring the establishment of the CC and any subsidiary CCs
- maintaining situational awareness
- determining critical resources and managing their use
- briefing governance
- establishing and maintaining communications with other agencies and the community
- ensuring the response stays within proscribed resource and budget limits
- acting as a spokesperson if a dedicated spokesperson has not been appointed, and
- managing the transition from response to recovery with the Recovery Manager.

Controllers need to:

- balance the need for accurate advice and information against the need for timely decisions,
- document key decisions and their rationale, as they are made,
- follow the intentions of their governance, and/or higher Controllers,
- focus on the actions of their response element, and
- be aware of decisions of neighbouring Controllers.

The Controller is also responsible for determining whether a dedicated spokesperson is required to reduce pressure on themselves. Appropriate spokespeople include senior members of the response's Governance (such as a minister, mayor, or chief executive), or a member of the IMT (for example, a technical expert).

Controllers may also need to allocate time for servicing and briefing governance. When this becomes a major task, a Controller needs to delegate duties and tasks to their IMT and/or Response Manager. Controllers may need to set up a policy group to support them in liaising with governance.

A Controller is required at each level of the response. Figure 16 below shows how there may be multiple Controllers within a single response.

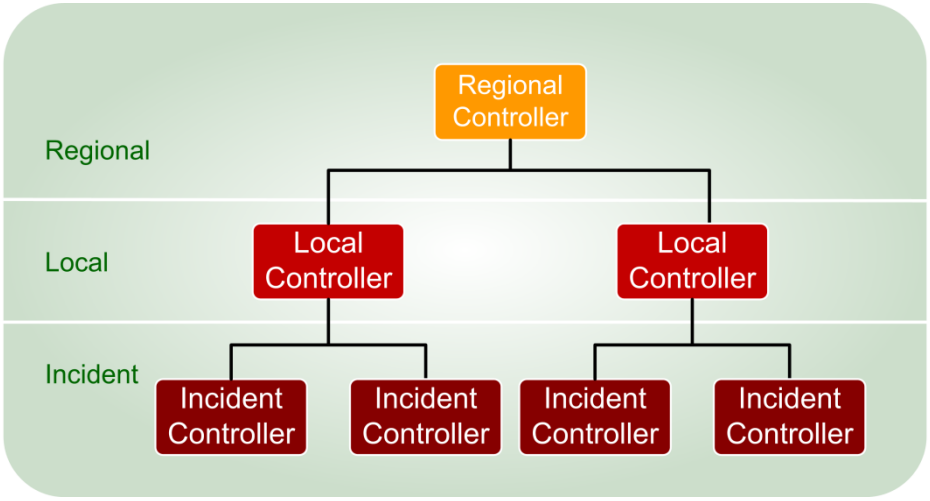


**Figure 16 Controllers at different levels during a response**

### *Other Control function roles*

The **Response Manager** may be delegated responsibility for overseeing the detailed operation of the CC, making some decisions in the absence of the Controller, ensuring the Action Plan is implemented, and resolving internal conflicts. This frees the Controller from the details involved in operating the CC, and allows them time to think ahead. The Response Manager may represent the Controller outside of the coordination centre. Some agencies call the Response Manager a different term, such as the Chief of Staff, or Deputy Controller.

**Controller's personal assistants** are responsible for recording meetings and decisions, managing the Controller's diary, answering calls and responding to emails, and ensuring that the Control administrative arrangements are in place.

**Technical Experts** provide specialist advice on aspects of the response. Examples include scientists specialising in the hazard (such as volcanologists during a volcanic eruption), environmental experts (such as hydrologists during a flood) or industrial experts (such as mining experts during a mine incident). These experts may be assigned to Planning, Intelligence, and/or Operations, but retain a direct relationship to the Controller. They may also serve as Liaison Officers if they are members of a responding agency.

In a larger response where there are is a shortage of technical experts, these experts may be centralised into an advisory group at the highest activated response level. This ensures the Controller can assign their expertise to where it will have the most effect.

A **Safety or Risk Advisor** monitors safety conditions and advises the Controller on measures to minimise the risks to assigned personnel.

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

### 4.2.2 Intelligence

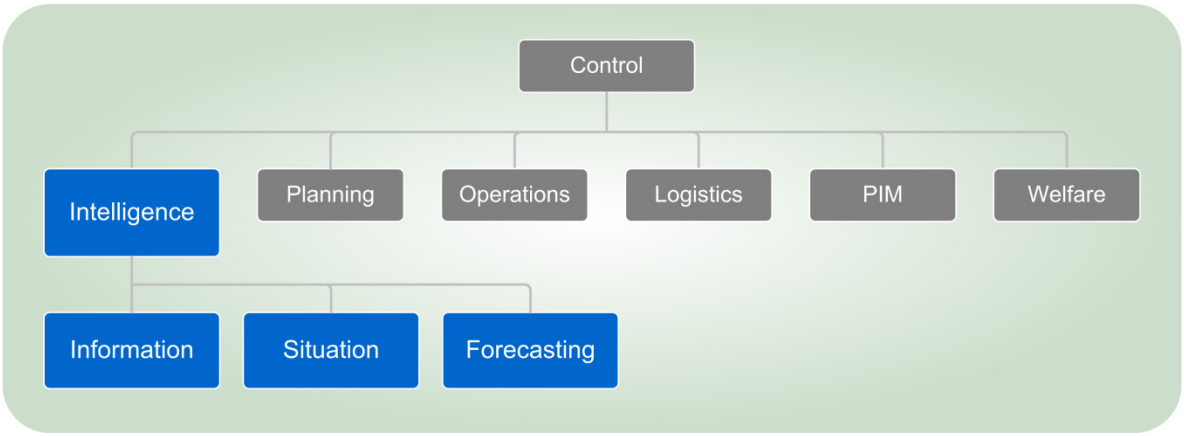


**Figure 17 Intelligence**

Intelligence is the function responsible for the collection and analysis of response information, especially (but not limited to) that relating to the status, hazards and the context of the incident. Intelligence responsibilities are to:

- gather, collate, and analyse response information,
- develop and distribute processed intelligence as situation reports, situation maps, and other outputs aimed at developing a common operating picture,
- develop and distribute intelligence that forecast how the incident may develop,
- manage the information collection plan (see *Information collection plans* on page 52), and
- contribute to the development of the Action Plan.

Effective intelligence contributes to situational awareness and gives the CC an understanding of how the incident can be expected to progress, allowing the development of proactive plans to mitigate, manage, and eventually resolve the incident. An intelligence cycle provides a structured process to achieve this (see *Intelligence cycle* on page 32).

Intelligence is the primary function with responsibility for analysing and understanding the context of the incident, and it also analyses information from all response functions and sources. The incident context may include:

- hazards (natural or man-made)
- community, demographic, cultural, and human factors
- terrain (geology, topography, vegetation, and hydrology)
- climate and weather
- infrastructure, and
- economic factors.

A Response Log is maintained to record intelligence activities, to ensure better situational awareness, assist with collation, and to provide an official record of the function's actions.

### *Intelligence sub-functions*

**Information** is responsible for managing the intelligence collection plan, identifying sources, collecting and collating information, and carrying out the initial analysis and initial verification.

**Situation** is responsible for identifying the intelligence needs of various audiences (and feeding these back to Information), analysing information, and distributing intelligence outputs.

**Forecasting** is responsible for intelligence relating to subsequent operational periods, which may be days, weeks, and or months into the future.

### *Intelligence cycle*

Intelligence delivers its responsibilities by applying an appropriate intelligence cycle, such as the one shown in Figure 18 below.


**Figure 18 Intelligence cycle**

#### 1. Direction/ Information collection

Direction comes from the IMT and Intelligence Manager, and determines the scope and boundaries for intelligence activities, including the information to be collected for intelligence analysis.

Information collection involves the systematic collection of relevant information from other functions, agencies, and sources. Information collection needs to be planned well to ensure timely and effective identification of relevant information sources. Information must be systematically acquired throughout the response. The information collection plan assists with prioritising and targeting the collection of information.

Intelligence is not responsible for holding all response information, as each function holds the information relevant to itself.

### 2. Information processing

Information processing involves evaluation and collation. Evaluation is the appraisal of an item of information in terms of its credibility, reliability, relevance, and accuracy.

Collation involves the systematic and planned management of the collected information, so that it is assembled into meaningful groupings and stored in ways that make the information easy to access and use.

Intelligence Logs are developed and maintained to provide an easily searchable record of all key intelligence input, outputs, and decisions that form a critical part of the overall record for the response.

### 3. Interpretation, development, and distribution

Interpretation is the analysis of all collected and collated information.

Development is the managed process of creating outputs that meet the needs of Controllers, response agencies, and other CC functions. These outputs help to ensure a common operating picture is achieved and maintained. Intelligence outputs may include situation reports (SitReps), impact analysis reports, intelligence summaries, status reports, and maps.

Distribution is the planned and managed process of providing intelligence outputs to users within agreed timeframes.

### 4. Monitoring and review

Monitoring and reviewing the information collection and processing ensures that the collection and processing steps are focused on key information gaps, and that the distributed intelligence output meets the needs of the recipients.

### 4.2.3 Planning

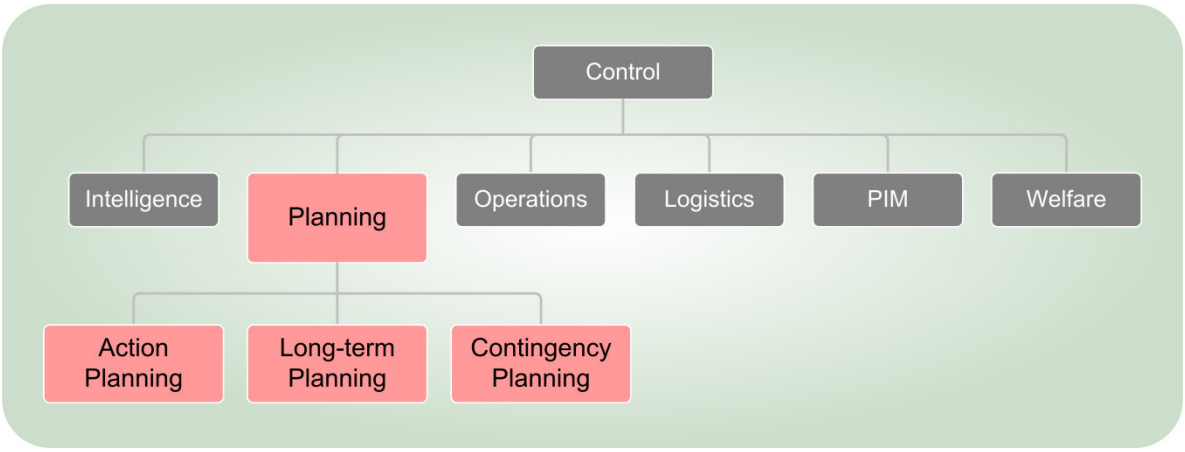


**Figure 19 Planning**

Planning is the function responsible for overseeing the development of Action Plans. Planning is also responsible for:

- developing long-term plans and contingency plans,
- assisting with planning the transition to recovery,
- convening and conducting planning meetings, and
- forecasting medium-to-long term resourcing requirements that will need to be provided by Logistics and supporting agencies.

Successful planning depends on the following inputs:

- the Controller's intent for the response. This may be informed by a higher level Action Plan or manager/officer, or by a documented instruction from the governance entity (such as a Terms of Reference, or Delegation of Authority),
- ongoing guidance and continual input from the Controller,
- impact and context analysis from Intelligence,
- response information from Operations, PIM, Welfare, and support agencies, and
- available response resources (immediately available and en route) from Logistics, Operations, and support agencies.

Intelligence provides the initial impact analysis and the incident's expected development. for use in determining planning objectives. Hazard and context updates are used by Planning when developing and analysing options, along with response information from Operations, PIM, Welfare, and Logistics.

Planning may require the following processes to operate effectively:

- a planning process (refer to Appendix A, *Action Plan process* on page 48), and
- a response log to record planning inputs and decisions, to ensure better situational awareness and as an official record of the functions actions.

The Controller has ultimate responsibility for the Action Plan; Planning is responsible for carrying out the planning process.

### *Planning sub-functions*

**Action Planning** is responsible for developing the Action Plan to meet the Controller's intentions. The Action Plan needs to be the first priority for Planning.

**Long-term Planning** is responsible for scoping and developing plans for response activities beyond the current and subsequent Action Plan. Long-term planning may apply within hours, days, weeks, or even months, depending on the response level and the scale of the incident. Long-term planning may include provision for the transition from Response to Recovery.

**Contingency Planning** is responsible for developing plans for a particular situation that has not, but may occur. 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.

Long-term and contingency plans use the same process, inputs, and personnel as the Action Plan. They are often completed with less detail because of personnel and time constraints. Long-term plans and contingency plans depend on more assumptions and estimates than Action Plans, as they cover situations that are yet to happen.

### 4.2.4 Operations

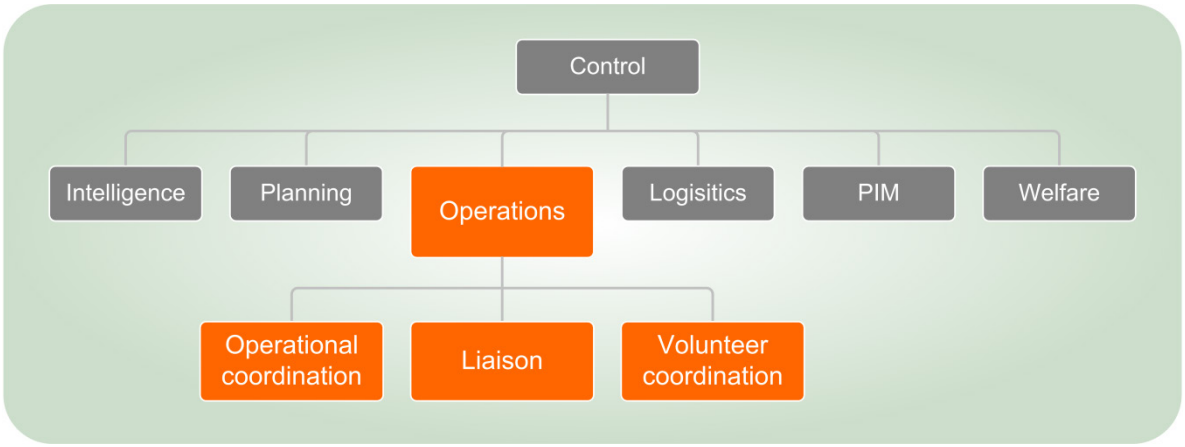


**Figure 20 Operations**

Operations is responsible for the day-to-day coordination of the response, detailed task planning, and the implementation of the Action Plan. Operations is also responsible for volunteer coordination, and liaising with other agencies.

Operations oversees the actions of agencies involved in response efforts. It should include personnel from other agencies, organisations, and businesses that have a major role in the response.

Operations' main responsibilities are:

- coordinating day-to-day response activities on behalf of the Controller,
- contributing to the development of the Action Plan,
- implementing the Action Plan, making minor amendments as the situation changes (the Operations Manager is responsible for assessing whether any changes require the Controller's approval),
- planning response tasks in detail,
- integrating Liaison Officers into the CC,
- forecasting resource use or needs to Logistics,
- recommending to the Controller which resources are critical,
- coordinating volunteer activities,
- keeping the Controller and IMT informed about the response, and
- resolving minor conflicts between response agencies.

Operations may require the following to operate effectively:

- a tasking process, including detailed planning, monitoring, and amendment of tasks, and
- a response log, to record operations activities, in order to ensure better situational awareness, and as an official record of the function's actions.

### *Operations sub-functions*

**Operational Coordination** is responsible for most of Operation's responsibilities. It coordinates the activities of the response agencies, plans tasks, monitors the implementation of the Action Plan, and resolves any operational problems that do not need to be escalated to the Control function.

Subordinate response elements report on their progress and activities to Operational Coordination, either directly or through Liaison Officers.

**Liaison** is responsible for establishing personal communication between agencies, enabling more accurate and timely information sharing. Liaison is activated when personnel (called Liaison Officers) are assigned to a CC. Liaison Officers may liaise with any other agency's Liaison Officers within a CC.

Liaison Officers pass information between the CC and their agency, and can advise on their agency's capabilities and intentions, and help resolve problems. They do not usually have authority to make decisions or commit resources, but regularly communicate with personnel at their agency who do have this authority.

Some Liaison Officers are based in the CC ('attached'), and other Liaison Officers are based at their agency ('external'). External Liaison Officers only attend the CC for the purpose of meetings and briefings, and usually coordinate with Operations.

Support agencies automatically provide Liaison Officers to the lead agency's CC. The lead agency may provide a Liaison Officer to key support agencies.

Liaison is personnel intensive, and during large-scale responses Liaison may need to be rationalised to a few coordination facilities.

Liaison Officers need:

- workable communications with their own agency's CC, preferably telephone, email, or any other relevant information management system, and
- to be familiar with the key appointments and functions within the lead agency CC.

Note: Liaison can link directly with the Controller in a small scale incident or when it will not impact on effective span of control.

**Volunteer Coordination** is responsible for liaising with volunteer groups (both established and spontaneous), and ensuring that their efforts are coordinated with the rest of the response. Volunteer Coordination personnel travel to volunteer bases in the community to determine their needs, goals, and capabilities and then communicate these to Planning and Operations. These personnel also convey any resource requests from volunteer groups, as well as task requests from the CC. Significant volunteer organisations may be requested to assign a Liaison Officer to the CC.

Logistics are responsible for the registration and any required training of spontaneous volunteers, and Operations for their coordination and tasking.

### 4.2.5 Logistics

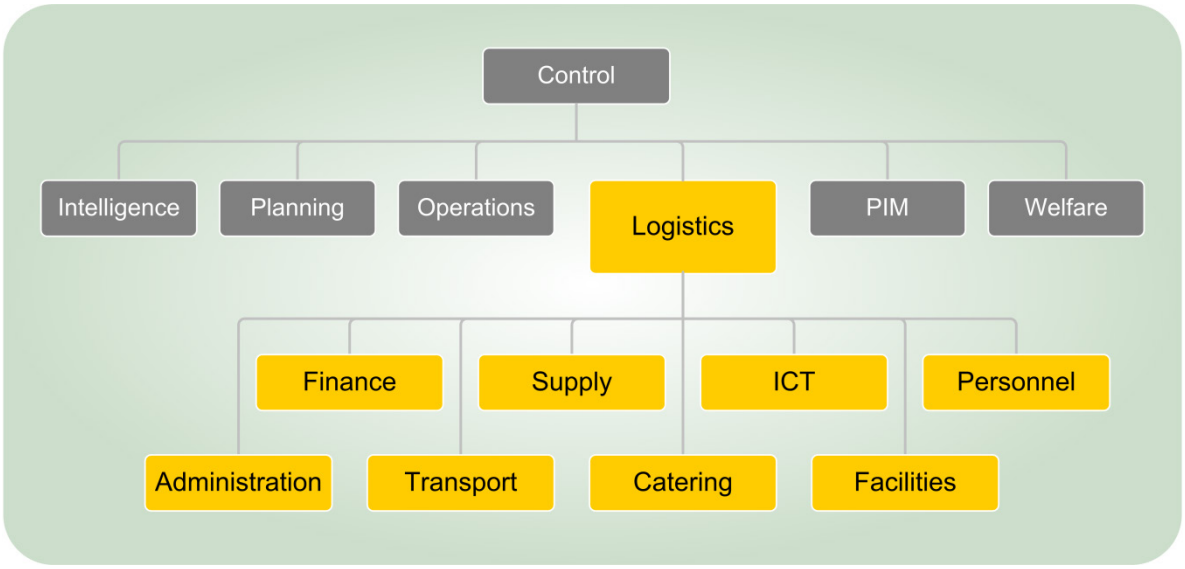


**Figure 21 Logistics**

Logistics is responsible for providing and tracking resources to support the response and the affected communities, and providing logistics advice to other CIMS functions. Resources may include personnel, equipment, supplies, services, facilities, and finance. Logistics actions generally precede those of other functions, so must be completed promptly to allow the other functions to operate effectively.

Logistics' main responsibilities are:

- receiving authorised resource requests, and procuring the resources,
- requesting, receiving, storing, maintaining, and issuing procured resources,
- notifying lower level CCs of resources available,
- participating in the development of the Action Plan,
- tracking resource use and financial expenditure,
- activating and operating any required Assembly Areas,
- providing transport,
- overseeing communications into and out of the CC,
- establishing and maintaining information technology networks,
- providing record-keeping and administration support,
- collating and matching offers of assistance, and
- advising the Controller and the IMT of logistics issues and resource levels.

Logistics may require the following processes or advice to operate effectively:

- procurement,
- tracking, to record resource arrival, issue, maintenance, and disposal,
- finance, including recording and tracking of expenditure,
- legal advice, and
- a response log, to record significant logistics activities.

### *Logistics sub-functions*

**Supply** at a CC is responsible for 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** is responsible for providing transport, and for equipment maintenance. Transport works with Supply to transport resources from Supply's holding areas to where they are needed. Transport may be carried out by the Supply team.

**Finance** tracks response costs, pays accounts and invoices, provides authorised cash advances, and audits financial accounts. This team should, as far as possible, use the business-as-usual finance system for the response agency. In some agencies, in a larger response or at a higher response level, Finance may be a stand-alone IMT function.

**Information Communications Technology (ICT)** is responsible for establishing and maintaining the communications links and information technology networks in the CC. Communications receives messages, logs them, and then distributes them to relevant functions, and send radio or courier messages on behalf of other functions. In more complex responses, a communications plan may be needed. In some agencies this is part of Operations or a separate function.

**Facilities** is responsible for securing buildings and land for use by response personnel, and maintaining these throughout the response. Facilities may assist Welfare with providing buildings and accommodation for affected members of the public. Facilities arranges contracts to procure the use of commercial facilities, and Supply provides procurement advice and input.

**Catering** provides meals and drinks to response personnel (foodstuffs are ordered by Supply). Catering arrangements must be made where a response lasts more than six hours and responders are not self-supporting. This function may be combined with Supply. Catering may also work with Welfare to arrange catering support for the affected communities.

**Personnel** is responsible for managing human resources, including registering and training response personnel (including spontaneous volunteers), and payment of staff (where required). Personnel from other agencies report to Personnel for registration, attend any briefings or training, and are then directed to their assigned team.

**Administration** is responsible for arranging clerical support, cleaning, maintenance, pool vehicles and record-keeping, particularly of key response documents. Administration is usually activated to support local or higher level CCs, though they may be activated at large incidents or Assembly Areas.

### 4.2.6 Public Information Management (PIM)

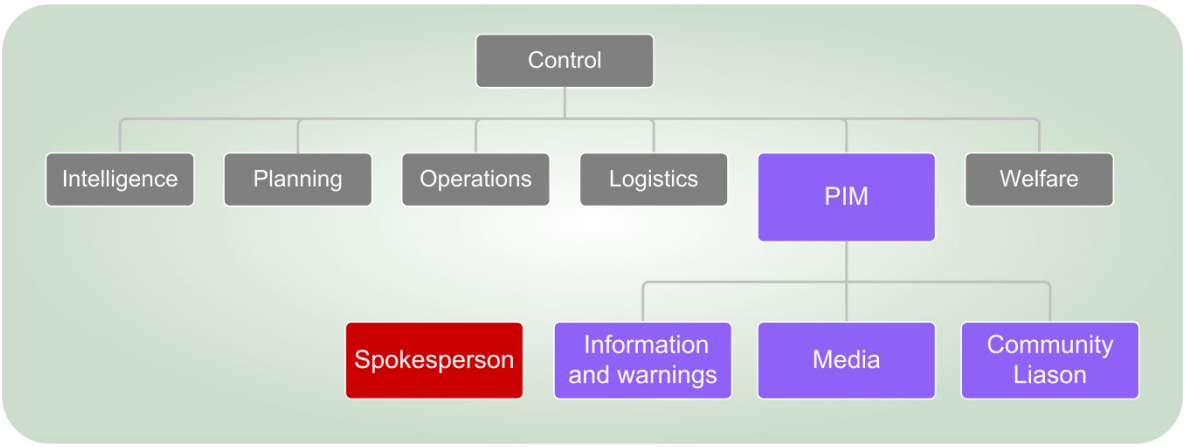


**Figure 22 Public Information Management**

Public Information Management (PIM) is responsible for informing the public about the incident and the response (including actions they need to take), media liaison and monitoring, and community liaison. On the Controller's direction PIM also issue warnings and advisories.

PIM's main responsibilities are:

- preparing and sharing information directly to the public (via social media, public meetings, pamphlets etc.), or via the media. Note that the content of official information such as warnings is generated by official processes, and approved by the Controller,
- monitoring the public and media reactions and passing information to the relevant CIMS functions,
- coordinating with other response agencies' PIM activities,
- preparing spokespeople for interviews and media conferences (see below)
- liaising with the community,
- working with the media, including arrangements for media visits and media conferences,
- liaising with VIPs and their personnel about site visits,
- ensuring call centres, helplines and reception personnel have current public information and key messages,
- participating in the development of the Action Plan, and
- advising the Controller on PIM issues.

The lead agency has responsibility for developing key messages and coordinating with other agencies' PIM personnel to ensure consistency. A multi-agency PIM group may be required to manage PIM during a 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 need to support the lead agency by:

- aligning their messages with the lead agency
- restricting their own messages to their field of expertise, and
- identifying spokespeople to the lead agency.

PIM also has responsibility for briefing and preparing spokespeople before they engage in interviews, and need to ensure the spokesperson is informed about:

- the audience
- key messages to communicate
- questions they can expect, and
- what the media already knows.

### *PIM sub-functions*

**Media** works with media organisations to distribute key messages through interviews, media releases and media conferences, as well as monitoring media broadcasts. This sub-function monitors and interacts with social media to distribute key messages direct to the public, to gather response information and to gauge public reaction. It also advises spokespeople, prepares for media conferences, and ensures call centres and helplines have updated information.

**Community Liaison** carries out two-way communication with affected communities. This enables the CC to obtain local knowledge, needs and intentions, and allows a direct means of passing on key messages. Community Liaison personnel work with community stakeholders, including businesses.

Community Liaison personnel may:

- develop a community engagement strategy, determining when, where, who, and how to engage
- organise and facilitate community meetings
- produce community newsletters, posters, and pamphlets, and
- log issues raised by community members and obtain responses.

**Information and warnings** gathers information from other CC functions to provide tailored information, warnings and advisories (approved by the Controller) to the public. Key sources are the Intelligence function, Operations and Community Liaison. These are then normally distributed through Media and Community Liaison.

### 4.2.7 Welfare

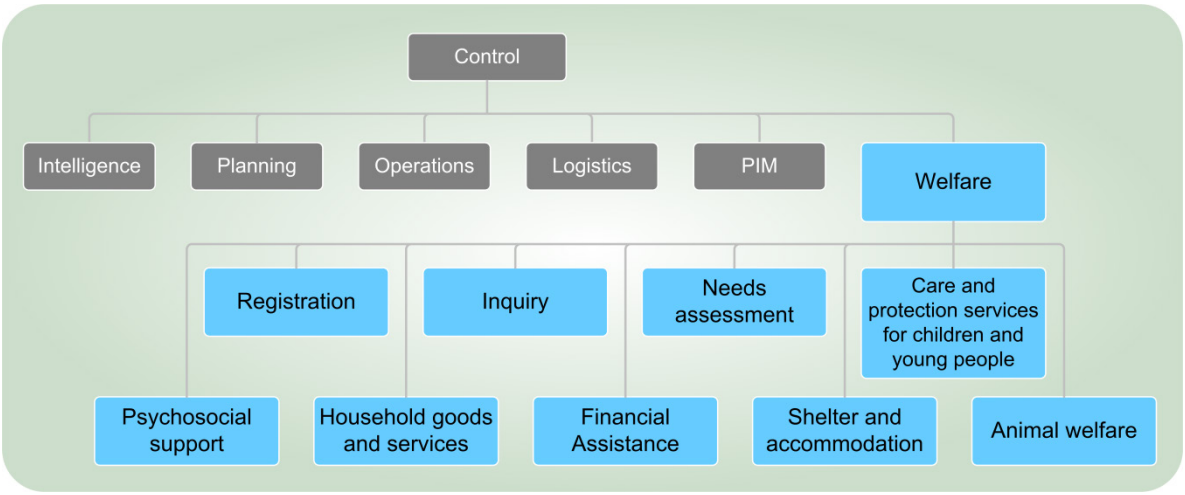


**Figure 23 Welfare**

An incident may be an emergency or a non-emergency. The welfare services described here are activated in response to an emergency.

Welfare is responsible for managing the consequences of an incident on individuals, families/whānau, and communities. The Welfare Manager also advises on the Welfare resources, organisational structure, and facilities.

The consequences of an incident dictate the extent of emergency welfare services required. At incident level these services relate to meeting the immediate needs of the affected people. For incidents affecting only a few people, emergency welfare requirements may only include providing shelter in a safe place and information about the response. In such smaller scale responses Welfare may be structured as a sub function of Operations.

If the incident requires significant welfare management, the Welfare sub-functions mentioned below must be considered. The Controller may access emergency welfare services (and/or welfare coordination) provided by a civil defence emergency management (CDEM) agency for these purposes. CDEM Welfare arrangements are detailed in local, CDEM Group, and national plans.

#### *Welfare sub-functions*

The sub-functions of Welfare include:

- Registration
- Inquiry
- Needs assessment
- Care and protection services for children and young people
- Psychosocial support
- Household goods and services
- Financial assistance
- Shelter and accommodation, and
- Animal welfare.

# APPENDICES

# APPENDIX A ACTION PLAN PROCESS

This appendix describes the planning process to develop an Action Plan. An Action Plan details the desired outcome and key tasks for the management of an incident, and the measures that will be taken to achieve the outcome. An effective Action Plan:

- integrates all of the agencies into a cohesive response
- increases situational awareness between agencies
- coordinates activities towards a common goal, and
- reduces risk, duplication, and conflicting actions.

Each response element develops its own Action Plan, ensuring it is consistent with the Action Plan from the lead agency. A summary of suggested content is listed in *Recommended content for Action Plans* on page 57 of Appendix C.

The Action Plan is the Controller's document, usually drafted by other personnel on the Controller's behalf. The Controller determines intentions and sets the objectives for the Action Plan. The Planning function supports the Controller by managing the planning process and ensuring that the Action Plan meets the Controller's intentions and objectives.

Each response element plans for different tasks, resources, and local conditions. Higher-level Action Plans focus on assigning tasks, allocating resources, and confirming coordination arrangements. Response elements follow the higher-level Action Plan to plan their assigned tasks, working within the designated coordination arrangements. This requires horizontal coordination between response elements as well as vertical oversight.

Action Plans cover the duration of the incident or an operational period defined by a Controller. The operational period needs to allow sufficient time for the Action Plan's objectives to be achieved.

New Action Plans should not be developed at arbitrary periods, such as the start of a new shift. New Action Plans are only developed:

- when the objectives in the original Action Plan are achieved
- if the situation changes significantly and the original Action Plan objectives cannot be achieved, or
- the objectives are changed by the Controller.

Action Plans need to be **documented** so they can be communicated effectively, and to ensure continuity of operations (particularly during changeover periods). Issuing an Action Plan in a face-to-face briefing allows the Controller to emphasise the key elements of the plan, answer any questions, and gauge understanding of the Controller's intent.

Action plans are **updated** when some of the arrangements in the Action Plan (such as times, locations, sequencing of actions and resource allocation) have to be amended due to unforeseen circumstances. If the objectives and overall concept of operations does not change, an updated version of the Action Plan (version 1.1, 1.2 etc.), with the changes highlighted, is sufficient. Many of these changes originate from Operations, as they often have to amend the Action Plan during implementation.

### *Contributors to the plan*

Incident level Action Plans:

- may be developed by the Controller, perhaps with one or two others
- may be handwritten in smaller incidents
- are prepared in line with agency procedures, and
- are likely to be communicated verbally to key response personnel.

From the local response level and higher, Action Plans are a team effort, with direction and oversight from the Controller.

The recommended participants in the Planning Team are:

- the Planning Manager, to lead the planning process
- IMT function managers, and any other key personnel responsible for implementing the Action Plan
- key support agencies' representatives/Liaison Officers, preferably with authority to make decisions on behalf of their agency, and
- technical experts.

The **Controller** must be available at key stages within the planning process to ensure that it is proceeding in line with their intentions. At a minimum, the Controller is required for the following steps (of the process described in *Planning process* on page 46):

- Initial response and assessment (step C)
- Objectives Analysis (step 1), to give their intent at the start and to confirm the planning team's work at the end
- Options Development (step 2), to give guidance at the start, and to confirm the planning team's work at the end
- Decision, deciding on an option (step 4)
- Action Plan Development (step 5), to approve the final draft, and
- Operations briefing (step 6), to present the plan.

### *Planning process*

This planning process is based on the one used by the New Zealand Defence Force and New Zealand Police, and incorporates the 'Operational Planning P' proven in North America.

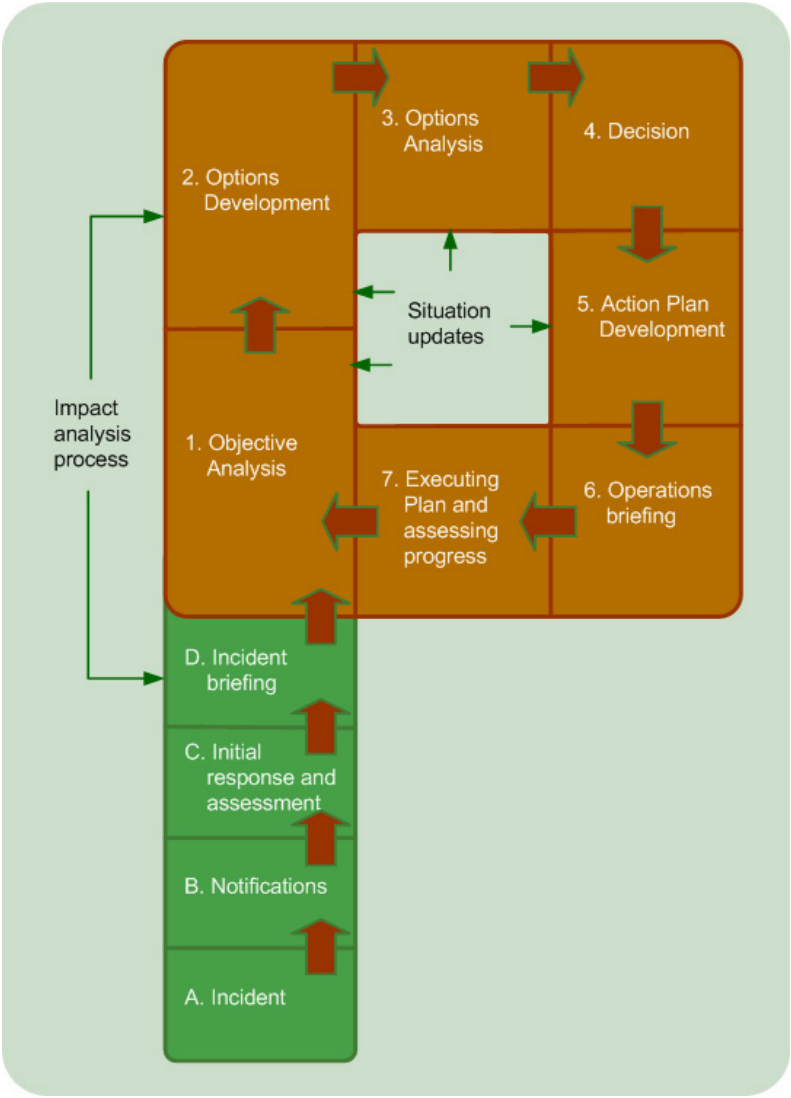


**Figure A-1 Planning process**

The **initial response** is triggered by the incident (steps A-D in Figure A-1, shown in green) and is only carried out at the start of response. Initial response is discussed on page 47 of this appendix.

The **planning process** itself is shown in brown (steps 1-7). Green arrows (impact analysis and situation update) indicate input from Intelligence. Once the planning process has been completed and an Action Plan issued, the process continues in a loop around steps 1-7. The planning process is discussed in detail in this appendix, starting on page 48.

**Impact Analysis** is covered on page 51 of this appendix, as are information collection plans.

### *Initial response*

**A. Incident**

The process begins when an incident occurs, or with recognition that an incident may be about to occur (for example a widespread human disease outbreak overseas, or a tsunami generating earthquake in the Pacific Ocean).

**B. Notifications**

Response personnel are alerted to the incident. This may be via a communications centre following an alert from the public, a warning from a scientific source, or by natural indications (such as a column of smoke or a felt earthquake). The required response is determined and, if applicable, warning and/or advisory messages are issued to inform the relevant response agencies.

**C. Initial response and assessment**

This step covers mobilisation of response personnel, reconnaissance, information gathering, assessment of the situation, and immediate response actions. Incident level Action Plans may be prepared or responders may rely on procedures to coordinate their actions. Initial Action Plans may be created to provide greater coordination during this step and to give enough time for the action planning process to be completed in full. This step may take minutes or it could take several days, depending on the hazards, scale of the response, and the response level.

An initial Action Plan:

- uses the action planning process, but with shortened time-frames and less detail
- focuses on immediate life-saving activities, mobilisation of response assets, and information collection
- does not aim to set the conditions for a transition to recovery, and
- may be issued verbally, though a written record must be kept.

All response levels may issue an initial Action Plan.

**D. Incident briefing**

The initial Action Plan is issued to the relevant response elements at the Incident briefing. This can apply at any response level, and leads to the initiation of the Action Plan process.

### *Action Plan process*

At each stage of the planning process, functions need to ensure that the latest information on hazard impacts and available resources is used.

**1. Objective analysis**

This is the most important step in the planning process; it is when the Controller and planning team determine what the Action Plan is meant to achieve. It consists of the following steps:

a. **Reviewing the situation**, confirming:

- the resources available, including any resources still to arrive
- response actions to date
- initial hazard impacts
- area of operations for the response, including outside the affected area, and
- timeline for the response (in terms of the overall operation and the time available for planning), and the time the Action Plan will be completed. Planners need to ensure that they leave sufficient time so that personnel at lower response levels have enough time to do their own planning and preparation.

b. **Determining the intentions** of the higher levels by accessing the Governance's objectives from a higher level Action Plan or in a Delegation of Authority/Terms of Reference. Use these to determine what part the response element plays in the overall response.

c. **Determining the required tasks**. Some of these may come directly from an Action Plan, Terms of Reference or Delegation of Authority. Many will need to be deduced from the intent of Governance. Choose those that are essential to achieving the Governance intent. These essential tasks become the objectives of the response element. Some other tasks may need to be assigned to agencies in the Action Plan.

d. **Determining freedoms and constraints**. Freedoms are things that the Controller and planners can determine for themselves. Constraints are restrictions imposed by Governance. For example, if Governance has specified a time for the response to be completed, that is a constraint; if there is no specified time, it is a freedom. Constraints can also be set by the Controller, working under a delegation of authority from the lead agency. Considering freedoms and constraints gives planners a clearer understanding of their options and the operational boundaries.

e. **Identifying critical facts and assumptions**. Facts are statements of known data (for example, the resources available at the time of planning). Assumptions are substitutes for fact used to allow planning to proceed (for example, resources that may be made available during the response). Assumptions become information requirements, and should be verified as soon as possible. Assumptions should not be made about the hazard or environment. If these are unknown, they become information requirements.

## 2. Options development

During this step, the planning team develops options that will achieve the objectives. The number of options and detail that is developed depends on the time and personnel available. Ideally, planners consider two or three options, to avoid jumping to a conclusion without having considered alternatives. The options need to be different from each other, must achieve the response objectives, have acceptable levels of risk, and be feasible with the available resources. Experienced Controllers and planners may be able to develop a single option, using their judgement to save time. The Controller or Response Manager may give guidance on what options are to be developed in this step of the process.

All options must be evaluated against the following:

- impact analysis, in particular the most likely, and the most dangerous/worst case scenarios for hazards to develop
- local environment, and how this will affect the response
- available resources, their numbers, location, capabilities, and requirements, and
- available time.

If two or more options are considered, planners may split into teams, one team to each option.

This information is used to generate a concept of operations for each option. The options may be presented as a diagram with a brief description, and need to include key timings and resource groupings.

## 3. Options analysis

In this step, the response option concepts are analysed against the most likely and most dangerous hazard scenarios to determine the most suitable option. The easiest way to do this is to compare the timelines of the concepts against that of the hazard options. When concepts have weaknesses (for example, the concept states that welfare centres will be established by 1100 hours, but the hazard evaluation determines there will be evacuees arriving by 0800 hours) these need to be noted so the concept can be amended. A comparison between the concepts can then be made, and a recommendation made to the Controller. Operations personnel need to take part in this step, to ensure they fully understand the Action Plan they will implement.

## 4. Decision

The planning team present the response options to the Controller, including a recommended option. The Controller may decide which option to pursue (and may amend it) or may require further work on developing them. Once the Controller approves an option it becomes the concept of operations, which is the basis for the Action Plan.

**5. Action Plan development**

During this step, the Action Plan is written. If time is short, it may be written as a brief, to be delivered verbally. It must be documented for future reference. Maps and tables may be included to aid understanding. Specialist sections and appendices need to be written by those functions. These allow important specialist information and instructions to be included, without cluttering the main body of the Action Plan.

To aid the reader, who may have limited time and be working in adverse conditions, plans need to be clear, brief, and avoid jargon. Ideally, formatting, grammar, and spelling are checked. The Controller approves the final version, and this becomes the official Action Plan.

**6. Operations briefing**

Ideally, the Controller verbally briefs subordinate Controllers and/or team leaders who implement the Action Plan; written copies can be handed out and emailed. Some elements of the Action Plan may be briefed by the relevant function manager (Intelligence Manager briefs on hazards, Operations Manager on tasks, Logistics Manager on Logistics), but ideally the Controller leads this brief. A verbal brief allows questions to be asked of the Controller to confirm understanding. SMEAC (Situation, Mission, Execution, Administration and Logistics, and Command and Communications) is a common briefing format used in this step.

**7. Executing the Action Plan and assessing progress**

Once the Action Plan has been issued, the CC personnel assess progress. All Action Plans, including any tasks within them, will require amendment as unforeseen issues arise. Operations is responsible for amending the Action Plan and detailed task planning. Planning may need to issue an updated Action Plan (version 1.1, 1.2 etc.) where these amendments become substantial.

## *Action Plan hierarchy*

In more complex incidents, there are likely to be multiple Action Plans, with each response element having their own. This range of Action Plans may develop in one of two ways, bottom-up and top-down.

**Bottom-up approach**

A bottom-up approach is when an incident starts at a low level of response, and progresses to include higher response levels. Lower level Action Plans do not bind higher response levels, but the arrangements they put in place must be factored into higher level planning. This ensures that changes between current and planned response activities are minimised, and only carried out after careful consideration.

In the example below, a response is initiated at the incident level, followed by activation of an EOC and ECC:

1) An ICP issues an incident level Action Plan.

2) A related incident occurs nearby, leading to the establishment of a second ICP, which issues a separate incident level Action Plan for the second incident.

3) The local EOC activates, and coordinates the two incident level responses. The local IMT develops a local Action Plan that recognises the arrangements already in place at the incident level of response. The two previously issued incident level Action Plans are key inputs to the local Action Plan.

4) The regional ECC activates, and develops a regional Action Plan. The local Action Plan is a key input.

As the incidents continue:

- subsequent incident level Action Plans issued by the ICPs use the local Action Plan as their primary reference and work within its boundaries. Likewise subsequent local Action Plans work to the regional Action Plan.
- emergency services' communications centres and similar functions provide regular status reports to all activated CCs to help maintain a common operating picture.

**Top-down approach**

A top-down approach is when the response is initiated by a higher response level (for example, when a national agency receives a warning from a scientific or intelligence source), or when there is sufficient lead-time to enable a structured approach.

The lead agency develops an Action Plan at their highest activated response level, based on their Governance directives. Each subsequent level develops its own Action Plan based on the level above. In the example described below, an ECC has four activated EOCs and several agencies subordinate to it:

1) The ECC issues a regional Action Plan.

2) The four EOCs each issue their own local Action Plans, based on the ECC's regional Action Plan, and on their own actions so far. The local Action Plans direct and coordinate the actions of their EOCs' response elements in greater detail.

3) Response agencies issue agency specific regional Action Plans, using Liaison and joint planning to ensure that these are aligned with the lead agency's regional Action Plan.

4) Each EOC and response agency has several incident level responses. These develop incident level Action Plans to coordinate their own operations in greater detail than that given in the local Action Plans.

### *Impact analysis*

This is a separate but complementary process. It may incorporate impact assessments from response agencies and is carried out by Intelligence. It needs to include the following steps:

1) Confirm the response area, including the affected area, and any space required for response personnel to deploy and establish support facilities.

2) Consider the environment within the response area - terrain, weather (including forecasts), and demographics. Examples include population centres, transport links, terrain effects on movement, rain and wind etc.

3) Consider the nature and characteristics of the hazards, and how they behave.

4) Combine the environmental and hazard considerations to gain an understanding of how the hazard will develop. Document the most likely (highest probability), and the most dangerous (worst impact) hazard scenarios. It is difficult to plan for every eventuality. Understanding the most likely and the most dangerous scenarios ensures the Action Plan will be able to be adapted to match the development of the incident.

### *Information collection plans*

During planning, there are questions raised that may not have answers available immediately. Some assumptions may be made, and interim answers developed based on the information that is currently available. Answers that cannot be verified become information requirements.

Information requirements are collected in an information collection plan, ensuring that questions are properly defined as information requirements, and assigned to a function or agency for answering. Information sources should be recorded for future use. Intelligence manages this plan.

Each information requirement is recorded in the information collection plan, numbered, dated and then assigned to someone to answer. Once an answer is received, the information requirement is closed. The example below might be for the initial stages of an earthquake response:

| Number | Date/Time | Information Requirement | Assigned | Status |
|---|---|---|---|---|
| 001 | 12/3, 2145 | What is the casualty status? | Ambulance, Police | Open |
| 002 | 12/3, 2200 | What is our access status? | Police | Closed |
| 003 | 12/3, 2245 | What is the infrastructure status? | Police, NZFS, 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 weather forecast for 13 March? | Intelligence | Closed |

**Table A-1 Example of an information collection plan**

# APPENDIX B NATIONAL RESPONSE

This appendix provides more information about national level response. For an overview of all response levels, see section 3.3 *Response levels* on page 12.

There is a connection between national and regional levels of response. National level decisions result in direction and tasks for regional responders. Regional level response result in advice, resource requests and situation updates to inform subsequent national-level decision-making.

### *National agencies*

When activated, a National Coordination Centre (NCC) provides direction to an agency's regional response activities, mobilises agency resources, and manages the flow of information to and from the Domestic and External Security Coordination (DESC) system. When an agency ECC is activated, the related agency NCC often also activates. In some cases national agencies may carry out coordination and direction using business-as-usual arrangements.

The lead agency NCC controls and coordinates the overall response. Support agencies' 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.

### *All-of-government coordination*

All-of-government coordination is the responsibility of the lead agency. This may be achieved through business-as-usual arrangements, working groups, or the lead agency NCC. The lead agency must ensure that all response elements have a coordinated response plan and structure to work to. This is implemented via a National Action Plan, the key document for national agencies and ECCs to inform their own Action Plans.

The government maintains the National Crisis Management Centre (NCMC) which is normally located in the Executive Wing of Parliament (Beehive). This is a permanent, all-hazards national coordination facility. Any national lead agency can use the NCMC as their NCC and/or to coordinate the all-of-government response.

The NCMC's primary role is to coordinate the all-of-government response. The NCMC works to the National Action Plan, leads all-of-government Public Information Management (PIM) and is responsible for collating information for all-of-government use. This includes overseeing national and international mobilisation and deployment of resources, as well as the allocation of tasks to support agencies.

The lead agency usually supplies the key appointments for the NCMC. 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 and non-government organisations may also be represented in the NCMC.

### *System of Domestic and External Security Coordination (DESC)*

DESC provides a mechanism for dealing with major crises or security situations requiring a whole-of-government response. Across New Zealand more generally, it is able to facilitate the coordination of all sectoral, regional, and government capabilities where national planning or a national response is required. The DESC structure is not based on CIMS.

DESC consists of:

- The Cabinet Committee on Domestic and External Security Coordination (DES), is the key decision-making body of executive government in respect of all issues involving security, intelligence and crisis management. DES is chaired by the Prime Minister, and includes senior Ministers with relevant portfolio responsibilities. The membership of DES is flexible depending on the nature of the emergency e.g. pandemic, natural disaster, biosecurity emergency etc.
- The Officials' Committee for Domestic and External Security Coordination (ODESC), a forum of central government chief executives with security responsibilities, chaired by the chief executive of the Department of Prime Minister and Cabinet (DPMC).
- Watch Groups and Working Groups of senior officials as required.

In the context of CIMS, one of the functions of DES is to coordinate and direct the national response to a major crisis or to circumstances affecting national security (such as a natural disaster, bio-security problem, health emergency or terrorist/military threat) within New Zealand or involving New Zealand's interests overseas.

In the context of CIMS, ODESC is the vehicle to ensuring that Ministers and the DES receive coordinated advice from senior officials. Its role includes taking a strategic approach to identifying national priorities and coordinating government's strategic response to major crises, threats or circumstances affecting New Zealand interests abroad.

Watch Groups and Working Groups maintain an ongoing overview of the situation, and advise ODESC.

The DESC system gives direction to the lead agency's NCC, the NCMC and supporting agencies' NCCs. ODESC stands alongside the lead agency and offers any coordinated support that might be necessary to deal with the contingency.

Authorisation to activate international assistance arrangements is given by DES, via ODESC. (Immediate support for lifesaving activities such as medical and urban search and rescue resources can be authorised by National Controllers).

# APPENDIX C RESPONSE DOCUMENTS

CIMS relies on the use of standardised templates to aid information management, information collation and analysis, planning and decision-making. This appendix includes the recommended content for situation reports (SitReps), Action Plans, task plans, resource requests, and incident event reports.

Consider the following when preparing response documents:

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

  Some examples are:
  - Kaipara District Council EOC SitRep #04 2013-04-31
  - Police ECC Action Plan #01 2012-09-31
  - NCMC SitRep #17 2014-02-29
  - USAR ICP SitRep #09 2017-11-31

  This means that when files are stored electronically they sort into a logical sequence that is easy to search through, especially during an incident when many documents, situation reports in particular, are likely to be shared between agencies and between different levels of the response.

### *Response document types*

| Document name | Document purpose |
|---|---|
| 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, to achieve the response objectives. |
| Resource Request | A request from one agency to another for specific resources |
| Task Plan | A description of how a single task will be managed and how response agencies will integrate their activities to achieve it. It works within the arrangements of an Action Plan. |
| Incident Report | A short description of a single occurrence within an incident, for example: a fire in a new location, damage to a particular bridge, a sighting of a missing person. |

### *Recommended content for a situation report (SitRep)*

| Name of field | Comments | Example |
|---|---|---|
| CC | CC issuing the SitRep (include agency) | NZFS Mackenzie District EOC |
| Type of report | | SitRep |
| Report number | Include a hash (#) and include enough digits for maximum required for incident | #002 |
| Incident | Type of incident and location, and time | Tekapo flood April 2013 |
| Date and time issued | | 2013-04-30 0600 |
| Period covered | Date/time SitRep covers (start and finish) | 2013-04-29 0500 to<br>2013-04-29 1700 |

***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 separate "resource request" form but can be summarised here |
| Limiting factors | Anything that is, 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 CC<br>Consider including partner agencies not represented at the CC and external Liaison. |
| Next SitRep due at | Date and time |

## *Recommended content for Action Plans*

### *Action Plan details*

| Name of field | Comments | example |
|---|---|---|
| CC | CC issuing the Action Plan (include agency) | NZFS 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 and location, and time | Tekapo flood April 2013 |
| Date and time issued | | 2013-04-30 0600 |
| Operational period covered | Date/time Action Plan covers (start and finish) | 2013-04-30 0600 to<br>2013-05-03 1700 |

### *Main body*

| Name of field | Comments |
|---|---|
| Summary of incident | A summary of the hazard impacts, environment and response actions to date. This is based on issued SitReps. |
| Aim | A statement of the intent of the Action Plan |
| Objectives | Clear objectives that lead to achieving the aim |
| Plan of action/strategy | Concept of operations describing the response actions that will be done to achieve the aim and objectives. A broad statement of what must happen and when |
| Designated tasks | Specific tasks and timings for each agency under the plan |
| Limiting factors | Matters that may or will limit options, timeframes, outcomes |
| Coordination measures | Times, locations, boundaries, and other measures designed to coordinate the response |
| Resource needs | Who will provide what and when they will do it – including: information, supply, personnel, equipment, transport |
| Information flow | Who needs to know and who has information we need |
| 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. |
| 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 |
|---|---|
| AP prepared by | Name (and rank if applicable), response role, signature, and contact details |
| AP approved by | Name (and rank if applicable), response role, signature, and contact details of response element's Controller |
| Distribution | Include CIMS functions, all partner agencies representatives at the CC, and any other activated sub-functions |

## *Recommended content for a resource request*

***Request details***

| Name of field | Comments | Example |
|---|---|---|
| CC | CC issuing the Resource Request (include agency) | NZFS Mackenzie District EOC |
| Type of report | | Resource request |
| Request number | Include a hash (#) and include enough digits for maximum required for incident | #013 |
| Incident | Type of incident and location, and time | Tekapo flood April 2013 |
| Importance | Urgent priority normal (circle as appropriate) | |
| When request made | Date and time | 2013-04-29 0600 |
| When required | From when and until when, date and time | 2013-04-29 2200 |

***Main body***

| Name of field | Comments |
|---|---|
| Purpose of request | Brief description of the desired effect |
| Resource details | Specific resource types requested and number required including size, voltage, etc. |
| Possible substitutes | Specific resource types and number required |
| Supporting requirements | Fuel, water, operators, etc. |
| Transportation requirements | |
| Delivery address | Specify name and location of staging area/final destination |
| Report arrival to | Name (and rank if applicable), response role, signature, and contact details |

***Approval***

| Name of field | Comments |
|---|---|
| Requested by | Name (and rank if applicable), response role, signature, and contact details |
| Request approved by | Name (and rank if applicable), response role, signature, and contact details |

***Response section***

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

| Name of field | Name of field |
|---|---|
| Supply of resource approved by *(Name and rank, response role, signature, and contact details)* | |
| Resource Available? Yes / No | Number of Resources Supplied |
| Request Filled By | Contact Details |
| Time of Dispatch | Estimated Time of Arrival |
| Supplier | Estimated/Actual Cost |
| Requesting agency confirms receipt | |
| Other Comments | |

## *Recommended content for a task plan*

### *Task plan details*

| Name of field | Comments | example |
|---|---|---|
| CC | CC that is issuing the Task Plan | Mackenzie District EOC |
| Type of report | | Task plan |
| Task plan number | Include a hash (#) and include enough digits for maximum required for incident | #014 |
| Incident | Type of incident and location, and time | Tekapo flood April 2013 |
| Date and time issued | | 2013-04-30 0600 |
| Period covered | Date/time task plan covers (start and finish) | 2013-04-29 1700 to 2013-04-29 0500 |

### *Main body*

| Name of field | Comments |
|---|---|
| Task situation | Relevant current information necessary to inform the task plan and execution |
| Task objective(s) | Definitive (smart) objective(s) this task plan is to deliver to |
| Task plan timeframe | When all tasks in this plan need to be completed |
| Component actions | Individual task actions, in chronological order. May include appreciation, preparatory actions, resource acquisition and transport, task delivery actions, safety actions, stand-down provisions |
| Task resources | Information, intelligence, personnel, equipment, transport (logistics) |
| Public information | Intended public information processes and outputs in relation to this task |
| Telecommunications plan | Frequencies and their purpose/coverage, role cellphone numbers, communications schedule and similar required for this task |
| Task organisation | List/organisation chart of key appointments and people in them for this task |
| Attachments | Lists, tables, maps, etc. |

### *Approval and distribution*

| Name of field | Comments |
|---|---|
| Task plan prepared by | Name (and rank if applicable), response role, signature, and contact details |
| Task plan approved by | Name (and rank if applicable), response role, signature, and contact details |
| Distribution | Include CIMS functions, partner agencies and representatives at the CC<br>Consider including partner agencies not represented at the CC and external Liaison where relevant |
| Task plan update due | Date and time |

### *Recommended content for an incident report*

(An incident report is used to report any specific occurrence within an incident)

| Name of field | Comments |
|---|---|
| Report from | Name (and rank if applicable), response role, signature, and contact details |
| When report created | Date and time |
| When event occurred | Date and time |
| Event location | |
| Event summary | A brief description of what has occurred (for example landslide blocking state highway, collapsed house with occupants, fire in a new location etc) |
| Actions taken | |
| Predicted occurrence development | How this specific occurrence is anticipated to evolve – causal factors, consequences and response |

# APPENDIX D GLOSSARY AND ACRONYMS

| Glossary term | Definition |
|---|---|
| 4Rs | The 4Rs refers to the components of emergency management – risk reduction, readiness (to respond), response, and recovery. |
| Action Plan | A document that describes how the response will be managed and how response agencies will integrate their activities to achieve the response objectives. It is owned by the Controller, and developed by Planning with participation of all the functions and agencies activated. |
| affected area | The area directly affected by an incident. |
| agency | This refers to:<br>• government agencies, including public service departments, non-public service departments, crown entities, and offices of Parliament<br>• local government bodies<br>• non-governmental organisations<br>• lifeline utilities. |
| aim | A broad statement of intent encompassing all objectives and planned activity. |
| Assembly Area | The area where resources are organised and prepared for deployment, and managed by Logistics. 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 | A formal, structured (see *SMEAC* definition on page 67), or informal overview of an operation. It provides a common operating picture of how an incident is, or is to be managed and resources deployed. |
| Casualty clearing point | A location where casualties are moved from the inner cordon for secondary triage and treatment. If required, ambulances are loaded here for onwards movement of casualties to medical facilities. |
| CC | See Coordination Centre. |
| CDEM | see civil defence emergency management |
| changeover | The orderly replacement of personnel. |
| check-in | The location where resources first report when arriving at an incident. Each is recorded on the Resource register. |
| checkpoint | The position from which traffic movement is observed and controlled. Traffic may be stopped but no physical obstruction is placed on the roadway to prevent access. |
| CIMS | see Coordinated Incident Management System |

| Glossary term | Definition |
|---|---|
| civil defence emergency management | Has the same meaning as the definition in the *Civil Defence Emergency Management Act 2002*. |
| Civil Defence Emergency Management (CDEM) Group | All local authorities must be members of a CDEM Group under s12 of the CDEM Act 2002. Under s20 all local authorities and emergency services must have representatives on the Coordinating Executive Group (CEG) of the CDEM Group (the CDEM Group may co-opt other people as required).<br>CDEM Groups lead civil defence emergencies at the regional level from an ECC, and may support incidents led by other response agencies. |
| command | Command operates vertically within an agency. It describes the internal ownership, administrative responsibility, and detailed direction of an agency's personnel and resources. Command cannot normally be exercised outside of an agency. |
| common operating picture | An understanding of a situation based on the best available information, shared among all response agencies. |
| Communications<br>(also Information Communications Technology) | The sub-function within Logistics responsible for establishing and operating the communications links into the CC. These can include email, radio, telephones, or courier messages.<br>Within CIMS, Communications should not be confused with public information management. |
| 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. |
| concept of operations | A clear and concise statement of the sequence of actions chosen by a Controller to accomplish their objectives. |
| context | The setting of an incident, including factors such as physical environment, weather, transport routes, weekend vs workday, and population distribution. |
| contingency plan | An Action Plan developed to coordinate the response to a situation that has not, but may, occur. |
| contra-flow traffic | Traffic that is directed to travel in the opposite direction to usual. It is a method of movement control for road traffic. |
| Control (function) | The function responsible for coordinating and directing the response element. It sets priorities and objectives, and determines how best to implement them. See also Control (verb). |

| Glossary term | Definition |
|---|---|
| Control (verb) | The authority to assign tasks to another agency 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 ownership, administrative responsibility or the management of another agency's resources. See also Control (function). |
| Controller | The person in charge of a response element who directs response activities, and fulfils management functions and responsibilities. The person exercising control. |
| Coordinated Incident Management System (CIMS) | A proactive incident management framework that systematically manages incidents regardless of size, hazard and complexity. Pronounced 'sims'. |
| coordination | The bringing together of agencies and resources to ensure a unified, consistent, and effective incident response. |
| Coordination Centre (CC) | A facility to support a Controller in coordinating a response, or part of it. Coordination centres may be activated to support incident, local, regional, or national level responses. They include Incident Control Points (ICPs), Emergency Operations Centres (EOCs), Emergency Coordination Centres (ECCs), and National Coordination Centres (NCCs). |
| cordon | A means of controlling and restricting movement to and from an area. An **inner cordon** is directly round an incident, and only tactical groups from the responding agencies operate in this cordon. An **outer cordon** is further from the incident, and controls access to the area of operations. |
| debrief | A critical examination of an operation done to evaluate actions for documentation and future improvements. |
| DES | Cabinet Committee on Domestic and External Security Coordination. See Appendix B *National response* on page 53. |
| DESC | Domestic and External Security Coordination. See Appendix B *National response* on page 53. |
| DHB | District Health Board |
| dispatch | To task and move a resource. |
| doctrine | Fundamental principles and practices by which agencies guide their actions in support of their objectives. It is authoritative but requires judgement in application. |
| ECC | see Emergency Coordination Centre. Pronounced E-C-C. |
| emergency | For the purpose of CIMS, an emergency is a situation that poses an immediate risk to life, health, property, or the environment that requires a coordinated response. Also see the definition of emergency in the CDEM Act 2002. |

| Glossary term | Definition |
|---|---|
| Emergency Coordination Centre (ECC) | A regional level CC that coordinates the regional response and provides support to local level responses. |
| Emergency Operations Centre (EOC) | A local level CC that coordinates the local response and provide support to incident level response activities. |
| end state | A short description of what the situation will be when an Action Plan has achieved its objectives. Expressed in the current tense, e.g. “The fire is extinguished, crews and vehicles are preparing to return to their stations, evacuees are receiving welfare support, and investigation is about to commence.” |
| EOC | see Emergency Operations Centre. Pronounced E-O-C. |
| function | An activity or grouping of activities that address the core responsibilities of a response element. |
| Governance | The senior authority overseeing the response. This may be chief executives or senior managers within an agency, or political leaders. The governance function is not responsible for providing operational coordination or support; this duty falls to the Controller and their CC. |
| ICP | see Incident Control Point. Pronounced I-C-P. |
| ICT | see Information Communications Technology |
| impact analysis | An analysis of the hazards and environment, that aims to determine the most likely and the most dangerous scenarios for the hazard(s) to progress. These are critical in forming a proactive Action Plan and response. |
| IMT | see Incident Management Team. Pronounced I-M-T. |
| incident | (1) An occurrence that needs a response from one or more agencies. It may or may not be an emergency.<br>(2) The first official level of agency response (see ‘incident level response’). |
| Incident Action Plan | See Action Plan |
| Incident Control Point (ICP) | Single location where an Incident Controller and members of their IMT coordinate and manage response operations at an incident level response. |
| Incident level response | The first official level of agency response, carried out by first responders. Response personnel conduct physical actions such as clearing obstructed roads, treating casualties, fighting fires, conducting rescues, and delivering welfare services. They are supported and/or coordinated by the higher response levels. |
| Incident Management Team (IMT) | The group of incident management personnel that supports the Controller. Includes the Controller, the managers of Planning, Intelligence, Operations, Logistics, PIM and Welfare; it also may include a Response Manager, risk advisors, and technical experts. |

| Glossary term | Definition |
|---|---|
| information collection plan | A document that gathers all unanswered questions that an IMT may have into a set format and allocates these to agencies for answer. It provides for a structured, targeted, and methodical approach to information gathering. |
| Information Communications Technology | A sub-function within Logistics responsible for communications networks and information technology arrangements. See Communications. |
| Intelligence | (1) The function that collects and analyses response information, particularly that related to status, hazards, consequential risks, and the context of the incident.<br>(2) The collection, evaluation, and analysis of response information, aimed at producing forecasts on how the response may develop. |
| intent | A formal statement that gives clear direction on a Controller's intentions regarding a response. It is normally expressed as objectives, a concept of operations and an end state. |
| jurisdiction | An organisation's or agency's area of responsibility. |
| lead agency | The agency with the mandate to manage a particular incident. It may have this mandate through legislation, protocols or agreement, or because it has the expertise and experience in managing a particular hazard. |
| Liaison | A means of establishing personal communication between response agencies. Liaison Officers may attend the CC occasionally (External Liaison), or be present full-time (Attached Liaison). |
| Logistics | The function that supports a response through the provision of resources which help maintain the response plan and the affected communities. |
| mobilisation | The processes of procuring or activating, assembling and transporting resources to an incident. |
| National Coordination Centre (NCC) | A national level CC that coordinates an agency's national response and provides support to regional offices responding to an incident. |
| National Crisis Management Centre (NCMC) | A permanent, generic national coordination facility for use by any national lead agency. It is intended to coordinate all-of-government responses. |
| NCC | see National Coordination Centre. Pronounced N-C-C. |
| NCMC | see National Crisis Management Centre. Pronounced N-C-M-C. |
| objective | A statement of what is to be achieved; best described as Specific, Measurable, Achievable, Relevant, and Time-bound (SMART). |
| ODESC | Officials Committee for Domestic and External Security Coordination. See Appendix B *National response* on page 53. |

| Glossary term | Definition |
|---|---|
| operational period | The period of time scheduled for execution of the Action Plan. |
| Operations | 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. |
| PIM | see Public Information Management. Pronounced 'pim'. |
| Planning | The function that prepares and updates Action Plans, and other plans such as long-term or contingency plans. |
| Public Information Management (PIM) | The function that, during an incident, prepares, distributes, and monitors information to and from the media and the public. |
| readiness | One of the '4 Rs' of emergency management. Readiness means 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. |
| recovery | One of the '4 Rs' of emergency management. Recovery means the coordinated efforts and processes used to bring about the immediate, medium-term, and long-term holistic regeneration of a community following an emergency. It is not covered in CIMS although CIMS may be applied to elements of recovery. |
| resources | All personnel, supplies, facilities and equipment available, or potentially available, for assignment to incidents. |
| response | One of the '4 Rs' of emergency management. Response means actions taken immediately before, during, or directly after an emergency to save or protect lives and property, and to bring the consequences of the emergency to a point of stability that allows Recovery to take over. |
| 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 cover all of the CIMS functions, even if all are carried out by a single individual. |
| Response Manager | An appointment in a CC that assists the Controller and oversees activity in the CC. Some agencies call the Response Manager another term such as Chief of Staff or Deputy Controller. |
| risk management | The process of analysing exposure to risk, and determining how to manage that exposure. The level of risk is arrived at by examining the likelihood and consequences of the hazard and whether the course of action is acceptable for the outcome that needs to be achieved. (Likelihood x Consequences = Risk). |
| risk reduction | One of the '4 Rs' of emergency management. Risk reduction means identifying and analysing long-term risks to life and property, taking steps to eliminate these risks if practicable, and, if not, reducing the magnitude of their impact and the likelihood of their occurring. It is not covered in CIMS. |

| Glossary term | Definition |
|---|---|
| road-block | A barrier or obstruction preventing or limiting the passage of vehicles. |
| Safe Forward Point | A safe location near the incident; used mainly as a meeting place for personnel. Managed by Operations. |
| Safety | Process of assessing hazards and developing measures to ensure safety of personnel. |
| Safety Advisor | Response personnel assigned to monitor safety conditions, and develop measures for making sure all assigned personnel stay safe. |
| SitRep | see situation report |
| situation report | 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 |
| SMEAC | Acronym for a standard sequence when directing actions; represents **S**ituation, **M**ission, **E**xecution, **A**dministration and Logistics, and **C**ommand and Communications. Sometimes called GSMEAC, with **G**round added at the start of the sequence. |
| SOP | see standard operating procedure |
| Staging Area | A designated location where resources are gathered before being sent to the incident area. Managed by Operations. |
| standard operating procedure | Written practices adopted by an agency. SOPs describe how actions or functions are performed. |
| support agency | Any agency that assists the lead agency and provides services, resources, information, or otherwise contributes to a response. |
| task plan | A document that describes how a task will be managed and how participating agencies will integrate their activities and resources to achieve the task objectives. The specific tasks listed in an Action Plan may need further planning to ensure they are achieved. A task plan is completed by the agency that is leading that part of the response, in conjunction with other agencies involved in planning for and delivering the task. |
| technical expert | An adviser with specialist skills or knowledge that is needed to support incident operations. |
| triage | A process for sorting patients according to severity of condition. Forward triage is a rapid assessment completed inside the inner cordon; it is followed by secondary triage which generally occurs in the casualty clearing area. Triage status usually determines the order and speed in which patients are taken to the treatment area and also helps prioritise where and when patients will be taken to more definitive care. |

| Glossary term | Definition |
| --- | --- |
| 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. |

New Zealand Government