noggin

Emergency

# Guide to AIIMS (the Australasian Inter-Service Incident Management System) and CIMS (Coordinated Incident Management System)

# What is AIIMS

The Australasian Inter-Service Incident Management System (AIIMS) is a nationally recognised incident management structure. Though used primarily by fire, land management, and other emergency agencies, the system provides all organisations a common framework to manage all incidents (natural, industrial, or civil), be they emergencies or important non-emergency activities, like major sporting events, large cultural exhibitions, and big business conferences.

Fundamentally, AIIMS enables multiple agencies who are engaged in incident response or planning to seamlessly integrate their resources (personnel, facilities, equipment, and communications) and activities under a common framework. In practice since the early 1990s, the system is based on the following principles:

**Management by objectives.**
The Incident Control function, in tandem with the rest of the Incident Management team (see below), will determine desired incident outcomes for the purpose of ensuring that all responders understand the direction taken during the response.

**Functional management.**
AIIMS lays out four functional areas: Control, Planning, Operations, and Logistics (more below). This organisation structure is intended to give full representation to al l vital management and information functions, though the composition of the Incident Management team varies depending on the incident in question.

**Span of control.**
A key AIIMS attribute is scalability: for some incidents, a full-scale response will not be necessary, but for others, it will. In this sense, span of control refers to the number of groups or individuals that can be successfully supervised by one person.

**Flexibility.**
AIIMS can be applied to all hazards and used by all agencies.

**Unity of command.**
Responders must work to achieve one set of common objectives. Similarly, individuals should report to only one supervisor.

## The four functional areas of AIIMS.

AIIMS comprises four functional areas. Together, they make the organisational hierarchy depicted below:

1. Control involves management of all activities necessary for the resolution of an incident.
2. Planning involves the collection, analysis, and dissemination of information and the development of plans for the resolution of an incident.
3. Operations involves the tasking and application of resources to achieve resolution of an incident.
4. Logistics involves the acquisition and provision of human and physical resources, facilities, services, and materials to support the achievement of incident objectives.

Source: Managing information in the disaster coordination centre: lessons and opportunities

## Key terms and their meanings.

AIIMS also uses popular incident response terminology, like control, command, and coordination. Here are the relevant definitions:

**Control:** The overall direction of emergency management activities. Control relates to situations and operates horizontally across organisations.

**Command:** The internal direction of the members and resources of an organisation's roles and tasks by agreement or in accordance with relevant legislation. Command operates vertically within an organisation.

**Coordination:** Bringing together of organisations and other resources to support an emergency management response. It involves the systematic acquisition and application of resources.

AIIMS establishes a full Incident Management team (IMT). Here are the roles and responsibilities of the key Incident Management team members:

| Title | Role | Responsibilities |
|---|---|---|
| Incident Controller | • Overall responsibility for the management of all activities and personnel deployed to resolve the incident<br>• Establishment of systems and procedures for the safety, health, and welfare of all response personnel and members of the public who may be involved in an incident<br>• Issuing of warnings and incident information to the public and affected stakeholders<br>• Management of the relationship with agencies and people affected, or likely to be affected, by the incident | • Take charge and exercise leadership, including the establishment of the incident management structure<br>• Set objectives for the incident response, considering the safety of the community as a priority<br>• Develop and approve plans and strategies to control the incident<br>• Implement the IAP (Incident Action Plan) and monitor its progress<br>• Provide information and warnings to communities so that they can make informed decisions<br>• Establish effective liaison and cooperation with all relevant agencies, affected communities, and others external to the IMT<br>• Obtain and maintain human and physical resources required for the resolution of the incident<br>• Apply a risk management approach, and establish systems and procedure for the safety and welfare of all response personnel<br>• Ensure appropriate financial delegations are in place and that these delegations are made known to the appropriate response personnel<br>• Ensure relief and recovery considerations are addressed<br>• Ensure collaboration between response and recovery agencies |
| Planning Officer | • Evaluation and analysis of intelligence on the current and forecast situation<br>• Preparation of options analysis and development of incident objectives and strategies<br>• Undertake risk assessments<br>• Preparation and distribution of the IAP, monitor and review the IAP implementation<br>• Develop a Communications Plan for the incident (as part of the IAP) and other plans as required<br>• Collection and maintenance of information on resources allocated<br>• Provision of management support services | • Obtain a briefing from the Incident Controller or the position that you report to<br>• Establish the Planning Section, appropriate to the size and complexity of the incident<br>• Appoint unit coordinators as required and delegate tasks<br>• Manage the personnel within the Planning Section<br>• Adjust the structure of the Planning Section throughout the incident<br>• Provide a safe working environment for personnel within the Planning Section<br>• Establish and maintain a log of activities and decisions for the Planning Section<br>• Communicate Section performance to the Incident Controller or the position you report to<br>• Prepare shift handover and brief the incoming Planning Officer<br>• Manage the continuity of Planning activities across shift changes Checklist<br>• Obtain intelligence from the Intelligence Unit/Section to support the development of the IAP<br>• Consider sources of local knowledge and information relevant to the incident; communicate with the Community Liaison Unit, if established, to facilitate obtaining of local knowledge<br>• Identify new and emerging risks for the incident and address these in the IAP<br>• Monitor effectiveness of risk mitigation strategies<br>• Provide strategic advice to the IMT based on information received<br>• Undertake options analysis involving alternate incident objectives and strategies and identify the risks and likely outcomes associated with each<br>• As part of options analysis, make recommendations on incident objectives and strategies, including justifications for discussion by the IMT and approval by the Incident Controller<br>• Schedule and conduct meetings for the IMT and the Planning Section<br>• Prepare the IAP for the next operations period and any longer-term planning required<br>• Disseminate the IAP throughout the incident management structure<br>• Develop changeover and demobilization plans and manage their implementation<br>• Develop and review the Communications Plan and its implementation<br>• Develop and maintain an effective register of all resources, required, en route, allocated to, and released from the incident<br>• Regularly communicate progress of strategies and the IAP to the Incident Controller<br>• Provide management support services (radio, telephone, computer operators, support in information transfer within the IMT and administrative support)<br>• Collect, collate, and store incident records<br>• Maintain a personal log of activities and decisions made<br>• Conduct handover briefing |

| Title | Role | Responsibilities |
|---|---|---|
| Intelligence Officer | • Collection of information on the current and forecast incident situation<br>• Analyzing and processing that information into timely, accurate, and relevant intelligence<br>• Organizing and displaying that intelligence in the form of a Common Operating Picture<br>• Disseminating intelligence products, particularly to the Planning Section<br>• Share intelligence products with others beyond the Incident Management Team<br>• Focusing activities so that critical intelligence needs are met, and a common operating picture is shared to support decision-making, planning, and monitoring of the response | • Obtain a briefing from the Incident Controller or the position that you report to<br>• Establish the Intelligence Section appropriate to the size and complexity of the incident<br>• Appoint unit coordinators as required and delegate tasks<br>• Manage the personnel within the Intelligence Section<br>• Adjust the structure of the Intelligence Section throughout the incident<br>• Provide a safe working environment for personnel within the Intelligence Section<br>• Establish and maintain a log of activities and decisions for the Intelligence Section<br>• Communicate Section performance to the Incident Controller or the position you report to<br>• Prepare shift handover and brief incoming Intelligence Officer<br>• Manage the continuity of Intelligence activities across shift changes |
| Public Information Officer | • Dissemination of information, advice, and safety messages to the public<br>• Provision of timely and relevant information, including safety messages to those who may be impacted by the incident<br>• Ensure that the Incident Controller is involved in the development and approval of media releases<br>• Ensure that the Incident Controller is kept up-to-date regarding media conferences and media releases | • Obtain a briefing from the Incident Controller<br>• Establish the Public Information Section appropriate to the size and complexity of the incident<br>• Appoint unit coordinators as required and delegate tasks<br>• Manage the personnel within the Public Information Section<br>• Adjust the structure of the Public Information Section throughout the incident<br>• Obtaining information on the current and projected incident situation from the Planning or Intelligence Section when established<br>• Maintain ongoing communication with the Planning/Intelligence Section regarding accuracy of information released to the public<br>• Disseminating incident information to the public and affected communities<br>• Liaise with affected communities<br>• Liaise and coordination with other agencies and media personnel to endure one consistent picture is provided to the public and affected communities<br>• Provide a safe working environment for personnel within the Public Information Section<br>• Establish and maintain a log of activities and decisions for the Public Information Section<br>• Communicate Section performance to the Incident Controller or the position you report to<br>• Prepare shift handover and brief incoming Public Information Officer<br>• Manage the continuity of Public Information activities across shift changes checklist<br>• Prepare safety messages and other media releases for the Incident Controller's approval<br>• Assess the level of media interest in the incident and response<br>• Establish a media center (within or close to the ICC) with appropriate equipment and personnel to assist so that the level of media interest can be effectively dealt with<br>• Notify other agencies' media officers of the media center location and contact information<br>• Prepare a schedule for media briefings and distribute accordingly<br>• Determine which supporting agencies media representatives should be present at media conferences<br>• Coordination of the media and information being released about the response |

| Title | Role | Responsibilities |
|---|---|---|
| Operations Officer | • Managing, supporting, and providing advice and direction to the Division or Sector Commanders or Functional Unit Coordinators<br>• Undertaking strategic planning<br>• Briefing the Incident Controller and IMT<br>• Maintaining effective communications within the Operations Section and with other sections<br>• Issues resolution<br>• Implementation of strategies to resolve the incident<br>• Management of all activities that are undertaken directly (in the field) to resolve the incident<br>• Management of all resources (people and equipment) assigned to the Operations Section | • Obtain a briefing from the Incident Controller or the position that you report to<br>• Establish the Operations Section appropriate to the size and complexity of the incident<br>• Appoint unit coordinators as required and delegate tasks<br>• Manage the personnel within the Operations Section<br>• Adjust the structure of the Operations Section throughout the incident<br>• Provide a safe working environment for personnel within the Operations Section<br>• Establish and maintain a log of activities and decisions for the Operations Section<br>• Communicate Section performance to the Incident Controller or the position you report to<br>• Prepare shift handover and brief incoming Operations Officer<br>• Manage the continuity of activities across shift changes |
| Logistics Officer | • Providing support for control of the incident through the organization and provision of human and physical resources, facilities, services, and materials<br>• Providing support and control for the demobilization of equipment and services | • Obtain a briefing from the Incident Controller or the position that you report to<br>• Establish the Logistics Section appropriate to the size and complexity of the incident<br>• Appoint unit coordinators as required and delegate tasks<br>• Manage the personnel within the Logistics Section<br>• Adjust the structure of the Logistics Section throughout the incident<br>• Provide a safe working environment for personnel within the Logistics Section<br>• Establish and maintain a log of activities and decisions for the Logistics Section<br>• Communicate Section performance to the incident<br>• Manage the continuity of Logistics activities across shift changes |
| Finance Officer | • Accounting for expenditure during the incident<br>• Managing insurance and compensation issues during the incident<br>• Collection and recording of cost data<br>• Cost estimation and recovery for the incident | • Obtain a briefing from the Incident Controller or the position that you report to<br>• Establish the Finance Section appropriate to the size and complexity of the incident<br>• Appoint Unit coordinators as required and delegate tasks<br>• Manage the personnel within the Finance Section<br>• Adjust the structure of the Finance Section throughout the incident<br>• Provide a safe working environment for personnel within the Finance Section<br>• Establish and maintain a log of activities and decisions for the Finance Section<br>• Communicate Section performance to the Incident Controller or the position you report to<br>• Prepare shift handover and brief incoming Finance Officer<br>• Manage the continuity of Finance activities across shift changes |

Source: Queensland Coastal Contingency Action Plan, Department of Transport and Main Roads

# Introducing CIMS (Coordinated Incident Management System)

Across the Tasman Sea, neighbouring New Zealand's emergency management arrangements are coordinated under the legal auspices of the Civil Defence Emergency Management (CDEM) Act 2002, tenets of which are now associated with the National Civil Defence Emergency Management Plan Order 2015.

That Order compels emergency services to use the CIMS (Coordinated Incident Management System) framework to guide the coordination of operations. Further, practitioners fulfilling key response roles at the national, CDEM Group, and local levels are to be trained and practised in the use of CIMS.

So, what is CIMS? First developed in 1998 to provide emergency management agencies with a framework to coordinate and cooperate effectively in a response, CIMS, the primary reference for incident management in New Zealand, is largely based on similar systems used in North America and Australia (NIMS and AIIMS respectively).

The purpose of the system is to enable personnel to respond effectively to incidents through appropriate coordination across functions and organisations. CIMS does so by:

Establishing common structures, functions, and terminology in a flexible, modular, and scalable framework that can be tailored to specific circumstances

Providing organisations, with due consideration to each organisation's unique responsibilities, resources, and legislative authority, a framework that they can use to develop their own CIMS-aligned processes and procedures supportive of both own-organisation responses and multi-organisation interoperability

To what hazards and risks does CIMS apply? By statute, CIMS should be used to provide effective management to the following incidents:

Biosecurity incursion incident

Environmental damage incident

Fire incident

Food safety incident

Hazardous substance incident

Marine mammal stranding

Mass maritime arrivals

Missing person incident (search and rescue)

Natural hazard incident

Business continuity disruption

Communicable disease outbreak and pandemic

Public disorder incident

Public health and medical emergency

Transportation accident

Crime and terrorism

Technological failure

Not just those, CIMS can also be used for the pre-emptive management of potential incident-inducing situations. Those include planned events, such as celebrations, parades, concerts, and official visits.

# CIMS principles and characteristics

What are the larger principles that CIMS reflects? Well, the primary goal of incident and emergency management in New Zealand is to protect people and property from all hazards and risks. While emergency management in New Zealand operates across [risk] reduction, readiness, response, and recovery, CIMS primarily focuses on response to incidents and emergencies, but it must also be factored into readiness and recovery. Its core principles include:

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

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

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

CIMS shares other structural similarities with systems like AIIMS. These include the following characteristics

| Characteristics | Description |
|---|---|
| Common structures, roles, and responsibilities | Common structures, roles, and responsibilities make it possible for organisations to work effectively alongside each other and for personnel to interchange roles. They facilitate information flow and understanding of structures and relationships. |
| Common terminology | Common terminology for functions, processes, and facilities prevents confusion, improves communications between organisations, and supports more efficient and effective responses. |
| Interoperability | Interoperability is the ability for systems, processes, personnel, and equipment to effectively operate together. It is the intended result of the common approach established by CIMS and its supporting arrangements (e.g., doctrine, training, and exercise programmes). Ideally, staff will be familiar with the environment they will work in and the personnel they will work with. |
| Management by objectives | Response objectives are established by the Controller, assisted by the Incident Management Team (IMT), who consults with Governance on desired outcomes. These objectives are then communicated to everyone involved so that they know and understand the direction being taken and work towards the same end so that unity of effort is achieved. Objectives are reviewed regularly against the situation and against progress towards resolving the incident. |

| Characteristics | Description |
|---|---|
| Consolidated planning | Consolidated planning in response and transition to recovery is the process that establishes the basis for the overall response. The planning process requires input from all the functions and organisations involved. Consolidated planning supports:<br>• The development of effective Action Plans, Long-term Plans, Contingency Plans, and Recovery Plans<br>• Organisations involved to have a cohesive and efficient response<br>• Situational awareness between agencies and organisations<br>• Coordinated activities to achieve common response objectives<br>• Reduced risk, duplication of effort, and conflicting actions |
| Integrated information management and communications | Integrated information management and communications between functions and organisations support situational awareness through the development and evolution of a common operating picture. This is essential for effective planning and response coordination, supporting successful delivery of objectives and transitioning to recovery. A common operating picture is dependent on common information protocols, processes, and procedures, as well as interoperable information management systems and consistent data standards. Integrated communications support consistent messaging to all stakeholders and communities. |
| Coordination of resources | Resource coordination involves the consolidation and control of resources. It maximises resource use across and between response elements, provides accountability, and improves situational awareness. It requires an awareness of available capabilities and resources so that procurement and use of resources can be managed efficiently and appropriately. The Controller directs resource coordination with the support of the Incident Management Team (IMT). |

| Characteristics | Description |
|---|---|
| Designated response facilities and locations | Designated response facilities and locations, with clearly defined functions or purposes, are essential in establishing the response structure and, when applicable, the hierarchy and relationships between response levels. |
| Manageable span of control | Span of control is the number of individuals or response elements one manager or Controller can manage effectively. The optimum span of control is between three and seven individuals or response elements, although this may be increased based on the:<br>• Experience of the manager or Controller<br>• Administration and technical support available to the manager or Controller<br>• Individuals' or response elements' competence or experience<br>• Familiarity, stability, and complexity of the incident, and the level of responsibilities and delegations<br>• Availability of appropriate plans, processes, and procedures |

# Other CIMS highlights

**Theory of lead and support agencies:**

Often, hazards or risks can be managed by one agency alone. Others require the support of other organisations. For the latter use case, CIMS has formalised a theory of lead and support agencies.

Lead agencies are those mandated by legislation or expertise to manage hazards resulting from incidents. Organisations supporting those lead agencies are support agencies.

As the name suggests, lead agencies are responsible for monitoring and assessing the situation, planning and coordinating the response, reporting to Governance, and coordinating the dissemination of public information – they must develop and maintain the capability and capacity to ensure they are able to perform their role and may draw on the advice and expertise of others in doing so.

It falls, as such, to the lead agency (through the person of the Incident Controller) to integrate support agencies into the response. While the Controller may task and coordinate support agencies' resources and actions, that person must recognise and accommodate support agencies' statutory responsibilities and/or specific objectives.

It is important to note that lead agencies may change as incidents evolve; after all, required authority or expertise changes. The lead agency may also change its priorities between (risk) reduction, readiness, response, and recovery.

In their turn, support agencies are required to develop and maintain capability and capacity to perform their role, often that means fulfilling their statutory responsibilities and pursuing their own specific objectives in addition to, or as part of, the support that they provide to a lead agency.

Sometimes, support agencies must render assistance by repurposing existing capabilities. They must also assist the lead agency in the development of Action Plans.

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

**Engaging iwi/Māori:**

As treaty partners to the crown and members of the wider community, whānau, hapū, and iwi must be involved in response and recovery (as appropriate to the scale of the incident). Often indispensable to effective response and recovery, iwi/māori involvement ought to occur within a framework of traditional knowledge, values, and practices.

## Incident management benefits of engaging iwi/māori in response and recovery

- Stronger networks
- Improved access to community focal points (i.e., Marae)
- Ability to mobilise resources appropriately
- Understanding of tikanga (marae protocol and burial practices)
- Able to identify and assess iwi needs
- Better understanding of the local landscape, including history and sacred sites
- An ability to link with other cultures

Notably, many iwi/māori may share a similar worldview; but there is still a need to recognise different dynamics within and between iwi, hapū, and marae and to engage with each individually if not collectively represented. There is also a need to recognise that different iwi, hapū, and marae have different resource and asset bases affecting their ability to respond.

As such, engaging iwi/māori in response and recovery should be based on a set of values understood ahead of time. They include:

Mutual respect and shared values that follow the treaty principles of participation, protection, and partnership

Recognition of the capability and capacity of iwi/māori and marae to support response and recovery

Collaboration between iwi/māori and emergency management organisations before, during, and after an event

# Incident management in CIMS

Like AIIMS, CIMS compels deputised Controllers to fulfil certain criteria in establishing management structures for incidents. Incident management structures should be:

Based on functional management

Flexible in approach and adapted to the needs of the incident as required, such as delegating functions, combining functions or adding functions, and/or function resources

Reflective of the scale and complexity of the incident, the tempo of operations, and the evolution of the incident

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

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

Here are the considerations that the Controller must have when delegating functions:

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

To ensure appropriate coordination and communication between the respective functions and organisations, the Controller establishes an Incident Management Team (IMT). Now, who is the rest of this team? Besides the Controller, the IMT typically consists of function managers of the respective CIMS functions that have been established or delegated. In complex incidents, the IMT should also include:

- Response Manager
- Senior support agency representatives
- Recovery Manager
- Iwi-mandated representation
- Technical and Science Advisors with relevant knowledge
- Risk and Legal Advisors

The Controller maintains overall responsibility and ultimate decision making. However, the IMT helps by carrying the responsibility for resolving the incident. The IMT allows the Controller to maintain an overview of the situation, develop high level objectives, link with Governance, and, when applicable, maintains direct relationships with other Controllers in the response.

In other words, the IMT supports the Controller in managing up (within its own organisation and Governance structures), down (within its command lines), and across (the functions and organisations it works with) in accordance with the commonly agreed objectives.

Further IMT responsibilities include:

- Maintaining a common operating picture and communicating it
- Engaging with affected people and communities to determine their needs and intended actions
- Agreeing on an Action Plan
- Supporting the establishment and sourcing of necessary resources
- Managing staff effectively
- Implementing the Action Plan and monitoring its progress
- Keeping the respective response elements informed of the decisions and the Action Plan
- Determining when an incident moves to an emergency, as defined in the Civil Defence Emergency Management Act 2002

# Incident management facilities

Personnel are not the only resources that matter during an incident. Structures and facilities help, as well.

While establishing an incident management structure, the Controller must also establish an incident control or coordination facility (or facilities) from where the incident management structure or structures operate. These facilities are Coordination Centres.

The specific Coordination Centre depends on the size and complexity of the incident, in conjunction with the lead agency's internal or legislative arrangements. The following coordination centres are used in CIMS:

| Response level | Coordination centre |
|---|---|
| Incident | Incident Control Point |
| Local | Emergency Operations Centre (EOC) |
| Regional | Emergency Coordination Centre |
| National | National Coordination Centre |

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

Examples of additional facilities include:

| Facility | Purpose |
|---|---|
| Assembly area | May be required if a significant amount of resources are being mobilised. It is used for receiving incoming resources, organising and storing them, and then transporting them to where they are needed. Assembly Areas are normally established at local, regional, or national levels. |
| Inner cordon | Established directly around incident level response operations. Only personnel from the responding agencies operate in this inner cordon. All other people are evacuated. |
| Outer cordon | Established further from the incident level response operations. Used to control access to the area of operations. |
| Staging area | Used for gathering and organising resources at the incident level. Provides a safe location for:<br>• Resources to be received and held prior to deployment<br>• Resources to be prepared for assigned tasks (equipment checks, planning, briefings, and loading)<br>• Response personnel to recover after returning from a task (cleaning, repairs, rest, meals, reorganisation, and resupply)<br>A Staging Area needs to be distinct from other response facilities, even when they are located together, to ensure resources and personnel are kept separate. More than one Staging Area may be required. |
| Safe forward point | Established for holding resources that are called forward for deployment, for briefings, or to await movement to their task areas. |

# How incident management systems can improve your response efforts

So why do these systems, AIIMS and CIMS, matter? And how can they bolster incident response efforts? For starters, organisations today face a growing number of ever-more complex incidents, operations which to be successful involve cooperation and coordination with peer organisations.

Inter-agency, inter-service cooperation isn't simple, though. In the case of disasters, multiple agencies are likely to respond all at once, often across overlapping jurisdictional boundaries.

Each of those responding agencies is likely to bring with it a unique set of competencies, experiences, systems, even terminology. Melding everything together, especially in the height of an emergency, is an operational nightmare that often impedes the effectiveness of the response.

AIIMS and CIMS, on the other hand, are nationally recognised throughout their respective jurisdictions. They, therefore, provide the requisite standardisation to support inter-service coordination, for virtually any kind of incident. Specifically, the systems make it possible for peer organisations to know what each other is doing.

Both systems designate roles and responsibilities for personnel involved in incident response, as well as formalise a cohesive chain of command, comprehensible to everyone involved in emergency services.

Clarifying roles from the planning phase onward, as AIIMS and CIMS do, helps to promote a safer working environment during an incident.

Moreover, the organisational structure laid out is flexible and scalable, adaptable to most incident types, complexities, sizes, and environments – remember even non-operational personnel are accounted for. In sum, both systems provide the following benefits:


Define organisational functions, communication flows, roles, and responsibilities


Enable standardisation of technology


Promote effective resource management


Adaptability, scalability, and widespread adoption contribute to operational efficiency


Take a risk management approach


Facilitate comprehensive planning


Furnish a competency-based approach to filling positions

Finally, both AIIMS and CIMS go a long way towards improving the efficiency of incident response. As a result, the scalable, flexible systems have been widely adopted not just in emergency management but in wider industry; see, for instance, the increasing popularity of AIIMS in the Australasian oil and gas industry as a framework for dealing with incident response.

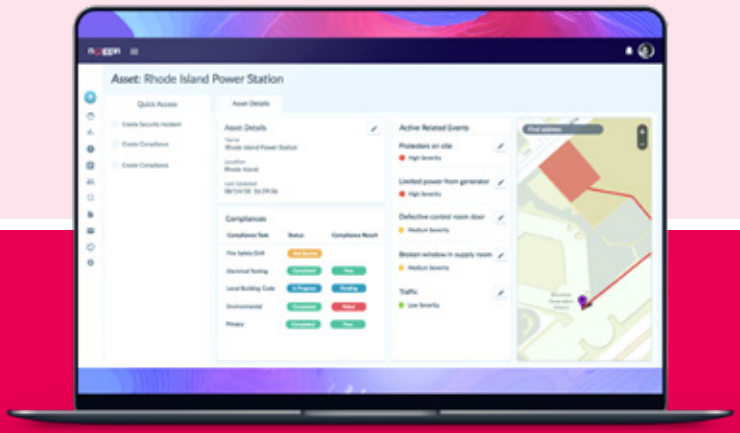
An incident management structure alone won't fix everything, however. To be successful in response efforts, organisations need to layer AIIMS and CIMS onto other incident response best practices, using advanced software like Noggin Emergency.

## Sources:

i. *Australian Fire Authority Council: AIIMS-4 Principles Online Course. Available at https://www.afac.com.au/docs/default-source/poster-archive/afac-placeholder---copy-(7).pdf.*
ii. *Department of Transport and Main Roads: Queensland Coastal Contingency Action Plan: 2017. Available at https://www.msq.qld.gov.au/-/media/MSQInternet/MSQFiles/Home/Environment/Contingency-plans/qccap.pdf?la=en.*
iii. *Teams might also include hazardous materials responders, urban search and rescue assets, community emergency response teams, anti-terrorism units, special weapons and tactics teams, bomb squads, emergency management officials, municipal agencies, in addition to diverse and sundry private organizations. James Carafano, Preparing Responders to Respond: The Challenges to Emergency Preparedness in the 21st Century: The Heritage Foundation. Available at https://www.heritage.org/homeland-security/report/preparing-responders-respond-the-challenges-emergency-preparedness-the.*
iv. *Ibid.*

Like what you read? Follow Noggin on social media

@teamnoggin  facebook.com/teamnoggin  linkedin.com/company/noggin-it




noggin
for Emergency

Meet the next-generation tool for corporate crisis and business continuity management teams to collaborate, plan, track their response, and share information. Built on the Noggin Core platform, Noggin Emergency gives response teams and decision makers the tools to know what's happening, collaborate quickly and effectively, make better decisions, and enact the right plans to take action when it counts the most.

The Noggin Emergency solution pack is backed by the Noggin Library with hundreds of plans and best-practice workflows, out of the box, and installed in minutes.

To learn more,
visit: **www.noggin.io**
or contact: **sales@noggin.io**