DARWIN PORT
LANDBRIDGE

Partnering in growth, connecting people and supporting potential

Integrated Critical Incident Management Plan (ICIMP)

Rev 0.0 – June 2025

General Manager Operations

OPS-LEG-01

Published June 2025

Contents

Attachments

Annexes

Accompanying Documents

Strategic Business Resiliency Framework - LSO-STD-31 Rev [0]

Business Continuity Plan EXE -POL 22 Rev [5]

The Darwin Port Integrated Critical Incident Management Plan outlines key organisational principles and practices aimed at enhancing disaster resilience.

This document:

- Standardises strategic response methodologies to ensure alignment and consistency across multiple disaster resilience stratagems and response plans.
- Promotes the adoption of best practices to strengthen disaster resilience within Darwin Port operations.
- Facilitates interoperability between jurisdictions, agencies, the private sector, local businesses, and community groups by advocating the use of common language and coordinated, agreed-upon principles.

Darwin Port follows the principle of prudent over-reaction and rapid de-escalation when assessing whether to activate the arrangements under this ICIMP.

It is easier and more effective to scale down an over-reaction than to escalate an under-reaction.

1 Section One – Administration

1.1 Version Control

Version Number:	OPS-LEG-01
Revision Number:	0
Issue Date:	Feb 2025
Copy Number:	Master

1.2 Disclaimer

The information provided by Trafalgar Consulting Group (TCG) in relation to the development of the Darwin Port Integrated Critical Incident Management Plan (ICIMP) is intended for general guidance and informational purposes only. While TCG has made every effort to ensure the accuracy, reliability, and completeness of the information presented, it is provided on an “as is” basis without warranty of any kind, express or implied.

TCG shall not be held liable for any loss, damage, or other consequences, whether direct or indirect, arising from the use, reliance upon, or interpretation of the information contained in the ICIMP.

Trafalgar Consulting Group assumes no responsibility or liability for any errors, omissions, or inaccuracies in the information contained within the ICIMP or for any outcomes resulting from its use.

This disclaimer applies to all individuals, agencies, and organisations involved in the development, implementation, or use of the Darwin Port ICIMP.

1.3 Confidentiality and Copyright Notice

This material is classified in accordance with its sensitivity and is protected by copyright, with all rights reserved. No part of this document may be reproduced, distributed, or transmitted in any form or by any means, except as permitted by the applicable classification level or the Darwin Port Document Management Policy, or with prior written consent from Trafalgar Consulting Group. Unauthorised use, disclosure, or reproduction of this document is strictly prohibited.

1.4 Distribution Table

Distribution Management Record					
Copy #	**Version #**	**Date of Issue**	**Position**	**Full Name**	**Signature**
01					
02					
03					
04					
05					
06					
06					
08					
09					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

Table 1

Note: A master copy of this Integrated Critical Incident Management Plan is held by the General Manager – Operations. It is responsibility the General Manager – Operations to ensure that this table is maintained.

1.5 Amendment Record

Document Control Record					
Version	**Section(s)**	**Page(s)**	**Revision Date**	**Actioned By**	**Approved By**

Table 2

1.6 Glossary of Terms

Term	Definition
Activation	Process whereby all or a portion of a plan is put into effect.
AIIMS (Australasian Inter-service Incident Management System)	A standardised framework in Australia and New Zealand for managing emergency incidents, ensuring coordination and accountability across agencies.
Asset	A resource or item of value to Darwin Port, including premises, IT systems, data, equipment, and staff.
Combat Agency	An agency that undertakes direct actions to combat a specific aspect of an incident, often under the direction of the Control Agency.
Command	The internal direction of personnel and resources by an agency to fulfill its operational responsibilities.
Control Agency	The Organisation or agency with statutory authority to direct response efforts for a specific type of incident.
Coordination	Organising response activities among multiple agencies to avoid duplication and optimise resources.
Critical Incident	An event, occurrence, or set of circumstances that: • Has a specific and identifiable spatial extent within the port area. • Is limited in duration and can be measured over time. • Necessitates human intervention due to potential or actual impacts on port operations, safety, or the environment. • Has defined concluding conditions or outcomes which determine its end. • Falls under the authority of a designated individual with decision-making power to control or resolve the incident.
Critical Incident Management Centre (CIMC)	The Centre where the Critical Incident Management Team manages briefings and planning during an incident.
Integrated Critical Incident Management Plan (ICIMP)	The document outlining Darwin Port's framework, policies, and tools for managing critical incidents.
Critical Incident Management Team (CIMT)	A task-built team responsible for responding to and recovering from a critical incident, comprising operational and specialist members.
Debriefing	A formal review after an incident to evaluate actions taken and identify improvements.
Disaster	A major disruption requiring significant coordinated responses to help the community recover, such as a flood.

Term	Definition
Emergency	An Emergency is an event, occurrence, or set of circumstances that: • Has a limited spatial extent and impact within the port, • Requires prompt intervention to mitigate risks but does not pose an immediate critical incident threat, • Can be managed and concluded by on-site personnel or port authority staff with standard response measures, • May escalate if not addressed, but generally remains within a single operational area and requires limited coordination with external agencies. • An Emergency is a heightened alert status below a Critical Incident, mobilising targeted response actions to address immediate risks and prevent further escalation.
Lead Combat Agency/Agencies	Government agencies that manage all phases of emergency and disaster response, including Police, Fire, Ambulance, and Disaster Management Groups.
Evacuation Plan	A plan outlining the safe removal of people from areas threatened by an incident, ensuring protection and minimising risks.
Incident Action Plan (IAP)	A written or verbal strategy detailing objectives and actions to be implemented during an incident, updated as needed.
Incident Controller (CIC)	The person responsible for overall management and coordination of resources and operations during a critical incident.
Issue	An event or circumstance that could harm or has harmed Darwin Port's reputation, image, or brand.
Lead Agency Or **Lead Combat Agency**	The Lead Combat Agency /Agencies with the expertise and resources primarily responsible for managing a specific situation.
Liaison Officer	An officer facilitating communication between agencies during incident management to ensure alignment and coordination.
Logistics Section	The section responsible for sourcing, maintaining, and providing resources, personnel, and equipment during an incident.
Operations Officer	The individual responsible for managing on-scene response activities in line with the Incident Action Plan (IAP).
Operations Section	The section that directs tactical responses during an incident, managing field operations and coordinating resources to achieve incident objectives.
Planning Officer	The individual overseeing the Planning Section, developing and maintaining the Incident Action Plan (IAP) to ensure clear objectives and strategies.

Term	Definition
Planning Section	The section responsible for collecting, analysing, and disseminating information, and developing strategies through the Incident Action Plan (IAP).
Port of Darwin	Means the area of water and land comprised within the boundaries as defined within the Darwin Port Maritime Security Plan. The Port Boundaries are gazette as per the requirements of the Maritime Transport and Offshore Facilities Security Act (MTOFSA).
Port Operator	Is defines as the entity declared by the Department of Home Affairs as the designated operator of the Port of Darwin as per the requirements of the Maritime Transport and Offshore Facilities Security Act (MTOFSA).
Public Information Officer	The designated person managing communication with the media and public, providing accurate and timely incident updates.
Public Information Section	The section that directs internal/external communications with key stakeholders via the CMT Leader.
Recovery Operations	Actions to restore the affected area or community after a critical incident, including cleanup, rehabilitation, and long-term support.
Risk Assessment	The process of identifying hazards, evaluating their likelihood, and analysing their impacts to prioritise response actions.
Situation Report (SitRep)	A report updating the status of the incident, response efforts, and progress, shared with agencies and stakeholders.
Span of Control	The maximum number of personnel or units one supervisor can effectively manage, typically five to seven.
Staging Area	A designated location where resources, personnel, and equipment are assembled for deployment during an incident.
Strategic Business Resiliency Framework (SBRF)	A structured framework designed to ensure the resilience of Darwin Port Operations by integrating risk management, business continuity planning, and adaptive strategies to address Critical Incidents and emergencies and ensure the sustainability and operational continuity of port activities.

Table 3

Note: Key terms have been provided for consistency and clarity in Darwin Port ICIMP, ensuring effective critical incident and emergency management across, landside waterside and maritime operations.

1.7 References and Supporting Documents

1.7.1 External References

Reference	Jurisdiction
Australasian Inter-service Incident Management System (AIIMS).	International
ISO 22301 Business Continuity Management.	International
Maritime Transport and Offshore Facilities Security Act (MTOFSA) 2003 (Cth)	National
Australian Standards Handbook HB:221 Business Continuity Planning Guidelines.	National
National Emergency Risk Assessment Guidelines: practice guide Australian Government.	National
Australian Disaster Resilience Handbook Collection:	National
Australian Institute of Disaster Resilience – Australian Emergency Management	National
Emergency Management Act (EMA) 2013 (NT)	State/Territory
Ports Management Act (PMA) 2015 (NT)	State/Territory
Work Health and Safety Act (WHSA) 2011 (NT	State/Territory
Marine Pollution Act 1999 (NT)	State/Territory

Table 4

1.7.2 Internal References

Document Title
Darwin Port Business Continuity Framework and Plan
Darwin Port Maritime Security Plan
Darwin Port Cyclone Preparation Plan

Darwin Port National Oil Spill Response Plan
Darwin Port Safety Management for Darwin Port Pilot Vessels
Darwin Port Marine Pilot Operational Management Manual
Darwin Port Legislated Port Safety Plan
Darwin Port Risk management Policy and Framework
Darwin Port Material Risk Register

Table 5

2 Section Two - Strategic Business Resiliency Framework

2.1 Strategic Business Resiliency Framework – Overview

The Strategic Business Resiliency Framework (SBRF) is the integrated framework adopted by Darwin Port to collectively define and unify the range of internal standalone response documents, policies, and guidelines outlined in Table 5. These documents form the cornerstone of Darwin Port's capability to effectively manage emergency situations, critical incidents, and risks, while also addressing broader challenges associated with natural disasters, security threats, and operational disruptions. By offering a cohesive structure, the SBRF ensures operational continuity, safety, and resilience across all port activities, while maintaining compliance with legislative and regulatory requirements and meeting stakeholder expectations.

The SBRF encompasses all of the relevant documents that may be referenced when the Integrated Critical Incident Management Plan (ICIMP) is activated, ensuring that all incident-specific and operational guidance is readily accessible and systematically aligned. This integration provides a seamless framework where supporting plans, such as the Port Emergency Plan, the Cyclone Preparedness Plan, and the National Oil Spill Response Plan, work in concert under the ICIMP to address the unique demands of any critical incident. The ability to draw on these interconnected documents enhances coordination and ensures that responses are comprehensive, efficient, and adaptable to evolving circumstances.

Recognising that effective response and resilience rely on a collaborative and systematic approach, the SBRF consolidates these diverse documents into an overarching strategy. This integration is not just about streamlining processes but also about fostering an organisational culture of preparedness and adaptability. By ensuring that all plans and protocols are aligned under a single framework, the SBRF enhances the port's ability to anticipate and mitigate risks, respond effectively to incidents, and recover rapidly with minimal disruption to operations.

Within the SBRF, the Integrated Critical Incident Management Plan (ICIMP) serves as a cornerstone operational component, focused specifically on managing critical incidents. The ICIMP provides a structured approach to incident management, combining clear escalation protocols, defined roles and responsibilities, and standardised recovery procedures to ensure consistent and effective responses.

This central role ensures that all relevant supporting plans and policies are fully integrated and effectively utilised during critical incidents, creating a unified response that minimises operational impacts, protects stakeholders, and preserves safety and compliance across all areas of port activity.

2.2 Strategic Business Resiliency Framework Structure

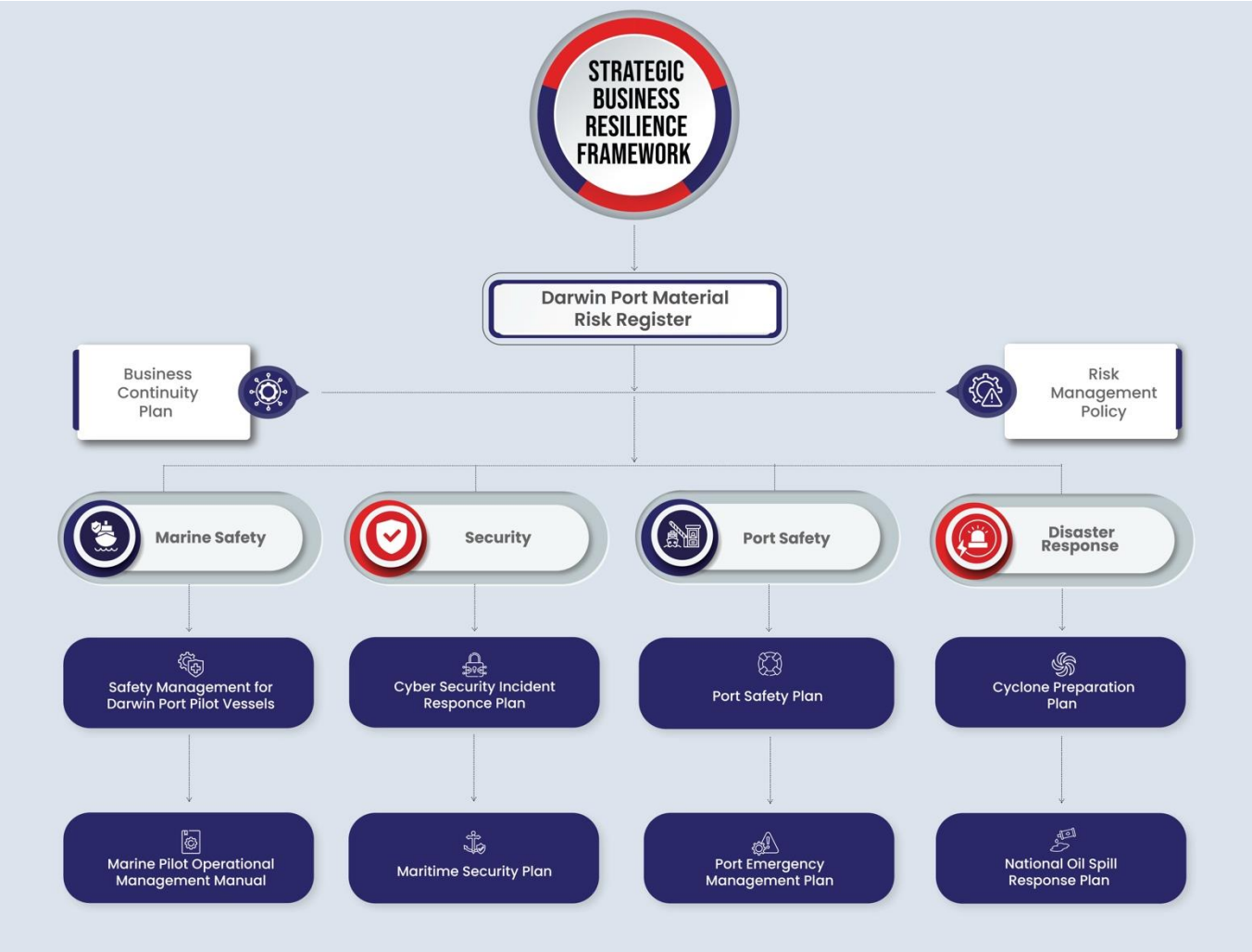


Figure 1 – SBRF Inter - Relationships

2.3 Integrated Critical Incident Management Plan (ICIMP) – Overview

The ICIMP is a strategic framework designed to address and mitigate serious and extreme incidents that pose significant risks to Darwin Port's operations and its role within the broader community. Critical incidents are characterised by:

- Rapid and unforeseen developments that challenge conventional response timelines.
- Situations that overwhelm existing response mechanisms.
- Disruptions to port operations with cascading effects on regional and community functions.
- Reliance on external resources for effective resolution.

- While Darwin Port implements robust measures to mitigate risks and safeguard its operations, it is acknowledged that even the most well-prepared organisations may face critical incidents that test their resilience. The ICIMP provides a structured approach to respond to such incidents strategically, ensuring that impacts are managed effectively and disruption is minimised.
- The ICIMP is grounded in core principles of strategic incident management, including:
- Taking immediate and decisive action upon the identification of a critical incident.
- Preventing further harm to operations, infrastructure, and stakeholders.
- Managing all impacted parties and ensuring alignment across internal and external stakeholders.
- Delivering transparent, accurate, and timely communication to support coordination and maintain trust.
- Protecting the port's reputation through proactive leadership and accountability.

By focusing on these principles, the ICIMP ensures that Darwin Port is equipped to manage strategic risks effectively, safeguard its critical role in the regional economy, and maintain confidence among its stakeholders and the broader community.

2.4 Purpose

The purpose of the ICIMP is to provide a structured and strategic framework for managing critical incidents that have the potential to significantly disrupt Darwin Port's operations, infrastructure, and reputation. The ICIMP is designed to:

- Ensure a coordinated, efficient, and timely response to critical incidents across all levels of management.
- Minimise the operational, financial, and reputational impact of incidents on Darwin Port's core functions and stakeholders.
- Protect critical infrastructure and operational capabilities essential to port activities.
- Mitigate disruption to port operations and facilitate rapid recovery to maintain business continuity.
- Support regulatory compliance and safeguard Darwin Port's standing within the industry and the broader community.

The ICIMP serves as a comprehensive framework for documenting Darwin Port's approach to critical incident management. It provides detailed guidelines for incident evaluation, activation procedures, and incident resolution.

Additionally, it offers management tools, including checklists and protocols, to ensure operations are safeguarded, disruption is minimised, and recovery is optimised.

Through the ICIMP, Darwin Port aims to:

- Fulfil its duty of care obligations to employees, contractors, tenants, and other stakeholders.
- Minimise potential legal, regulatory, and media consequences arising from incidents.
- Provide timely and effective support to port users, including tenants and vessels, during critical incidents.
- Enhance the port's capacity to recover swiftly and effectively from operational or reputational damage caused by incidents.
- Ensure efficient use and coordination of Darwin Port's resources during response and recovery efforts.
- Define roles and responsibilities clearly to ensure a streamlined and effective incident management process.

This plan is integral to Darwin Port's resilience strategy, ensuring that critical incidents are managed with precision and that the port can maintain its role as a vital link in the regional and global supply chain.

2.5 Scope

This plan is designed to manage the response to all critical incidents that affect Darwin Port's land-based and marine-based operations. It applies to all employees, contractors, tenants, visitors, assets, and facilities under Darwin Port's control.

A critical incident is defined as any event or circumstance that significantly disrupts an organisation's ability to function, either immediately or over time, and may also cause emotional or psychological distress to those involved. For Darwin Port, critical incidents encompass a wide range of scenarios, including but not limited to:

- Natural disasters (e.g., cyclones, tsunamis, floods, or fires).
- Environmental threats (e.g., oil spills, invasive species, or pollution-related emergencies).
- Cyber threats (e.g., data breaches, ransomware attacks, or disruptions to critical port systems and infrastructure).
- Port-related incidents (e.g., shipping accidents, vessel collisions, or hazardous material leaks).
- Community-based incidents (e.g., major transport accidents involving ferries or maritime services).

- Industrial accidents (e.g., dockside explosions, equipment failures, or chemical spills in port facilities).
- Port facility-related incidents (e.g., fires on vessels or in port buildings, accidents during cargo handling, or critical equipment failures).
- Threats to port operations, vessels, or personnel (e.g., bomb threats, acts of terrorism, or other security risks targeting maritime infrastructure).
- Serious criminal allegations involving port employees or visitors (e.g., smuggling, human trafficking, or illegal activities at sea).
- Alleged criminal activity within port precincts (e.g., drug trafficking, assaults on port staff or crew members).
- Sudden death or injury of port staff, contractors, or maritime personnel.

This plan ensures that responses to critical incidents are aligned with maritime operational requirements while addressing the specific risks inherent to Darwin Port's unique operating environment. It incorporates measures to safeguard operational resilience, protect personnel and assets, and ensure effective coordination with external agencies and stakeholders. The plan also accounts for emerging threats, such as environmental and cyber risks, reflecting Darwin Port's commitment to comprehensive and adaptive risk management.

2.6 Objectives

The primary objectives of the ICIMP are to provide a structured, systematic approach to managing critical incidents at Darwin Port, ensuring alignment with industry best practices and emergency management principles. The objectives of this plan are:

- To provide clear guidelines and documented instructions that support a coordinated and effective response to critical incidents, ensuring consistency across all levels of management and operations.
- To establish a common framework for assessing incidents, integrated with Darwin Port's risk management and business continuity systems, enabling timely activation and escalation of appropriate responses.
- To align with emergency services frameworks, including critical incident management principles such as those outlined in AIIMS (Australasian Inter-Service Incident Management System), to ensure interoperability and effective collaboration with external agencies.
- To define critical incident management roles, responsibilities, and accountabilities clearly, ensuring that all personnel understand their authority and function within the incident management process.

- To demonstrate to stakeholders, including regulators, tenants, and the broader community, that Darwin Port has a robust and effective critical incident management capability.

2.7 When to Use This Document

This Integrated Critical Incident Management Plan (ICIMP) is to be activated upon the declaration of a "Critical Incident." The Critical Incident Management Team (CIMT) will then use the ICIMP for the duration of Darwin Port's response to the incident. A critical incident can be declared by a General Manager or above, or a Delegated Authority, following the assessment methodology outlined in this Plan.

Darwin Port follows the principle of prudent over-reaction and rapid de-escalation when assessing whether to activate the arrangements under this ICIMP. It is easier and more effective to scale down an over-reaction than to escalate an under-reaction.

Upon declaring a Critical Incident, a CIMT Leader will be appointed and then activate the CIMT.

Note: Contact details for the standing members of the CIMT and their alternates are listed in the "Critical Incident Management Team" Can be Found in Annex A – CIMT Contact Details.

3 Section Three (3) – Fundamentals of Incident Management

3.1 Incident Management Overview

The Darwin Port Strategic Business Resiliency Framework outlines two (2) distinct levels of incident management:

3.1.1 Emergency Management Response

This level addresses immediate threats to life and safety, providing clear instructions for port users to respond swiftly to urgent situations. This includes actions such as evacuating a building upon hearing a fire alarm or sheltering in place during an Active Armed Offender event. The goal of this response is to protect lives and ensure immediate safety.

3.1.2 Critical Incident Management

Once an incident escalates and meets the threshold to be declared a critical incident, this plan is activated. It focuses on managing the broader implications of the event, coordinating resources, and implementing recovery actions to minimise operational disruption and ensure continuity. The Integrated Critical Incident Management Plan involves a structured approach to addressing the long-term impacts on the Ports operations and its stakeholders.

A critical incident can arise from a sudden event or a gradually escalating situation. When routine operations can no longer manage the threat, a coordinated and strategic response becomes essential—this is where Critical Incident Management comes into play.

Effective management of a critical incident requires thorough planning and deliberate action. It involves an appropriate response across all levels of Darwin Port, with clearly defined roles and responsibilities assigned to capable individuals. These individuals must be well-prepared and trained to carry out their duties effectively. A common approach to incident assessment is vital, supported by a well-defined escalation process to ensure the appropriate response level is activated at the right time.

3.2 Incident Classifications

This structured approach is enabled by Darwin Ports Integrated Critical Incident Management Plan, which forms a key part of the Strategic Business Resiliency Framework. By ensuring coordination and preparedness, this framework allows Darwin Port to manage incidents effectively, minimise operational impact, and safeguard assets and stakeholders.

3.2.1 Optimising Response: Flat Emergency Model & Tiered Critical Incidents

The Darwin Port Integrated Critical Incident Management Plan (ICIMP) utilises a dual-structured approach, maintaining a flat model for Emergencies while implementing a three-tiered escalation system for Critical Incidents. This approach ensures efficiency, clarity, and proportional resource deployment across different types of incidents.

The flat model for Emergencies allows for a streamlined and rapid response, ensuring that on-site personnel can immediately mobilise standard resources without unnecessary procedural delays. By keeping Emergency response straightforward, the port can address incidents swiftly, prevent escalation, and maintain operational continuity without overcomplicating decision-making processes. Since Emergencies are contained within a limited scope and typically resolved using internal protocols, a flat model ensures that personnel can act decisively without needing to escalate through multiple levels of approval.

Conversely, the three-tiered structure for Critical Incidents provides greater scalability and strategic control when dealing with high-impact events. This tiered approach enables the port to distinguish between varying levels of severity, ensuring that response measures and resource allocation are proportionate to the evolving situation. By defining Significant, Major, and Critical levels, the model allows for gradual escalation, bringing in external resources only when necessary and ensuring that decision-makers can communicate the severity of an incident effectively. This structured escalation prevents overreaction to minor incidents while ensuring that serious threats receive an appropriately scaled response, aligning with AIIMS principles for structured crisis management.

By combining a flat Emergency response model with a tiered Critical Incident structure, Darwin Port maximises efficiency for routine incidents while ensuring a measured, resource-conscious, and coordinated approach for more complex crises.

3.3 Understanding the Difference: Emergency vs. Critical Incident

3.3.1 Emergency

An Emergency within the port is a localised event that demands immediate attention but remains within the control of on-site personnel. It occurs within a limited area and does not yet pose a significant threat to overall port operations, infrastructure, or safety. Emergencies require prompt intervention to prevent them from escalating, but they are typically managed using standard response procedures by the port authority, security teams, or operational staff. The response is targeted and proportional, drawing on existing resources without the need for extensive coordination with external agencies. While an Emergency can disrupt normal operations in a specific area, it remains contained and manageable within the port's standard contingency framework. However, if an Emergency is not controlled effectively or conditions deteriorate, it may escalate into a Critical Incident, triggering a more complex and resource-intensive response.

3.3.2 Critical Incident

A Critical Incident, on the other hand, represents a significant and immediate threat to the port's operations, infrastructure, safety, or environment. Unlike an Emergency, a Critical Incident has a clearly defined spatial impact, often affecting multiple operational areas or posing a broader risk that requires high-level intervention. It is time-sensitive, requiring rapid and coordinated human intervention to prevent catastrophic consequences. The complexity of a Critical Incident necessitates structured decision-making, with a designated authority—such as the Critical Incident Management Team (CIMT)—taking control of the situation. The response to a Critical Incident often extends beyond standard port resources, requiring external agency support, emergency services, regulatory oversight, and crisis management protocols. Unlike an Emergency, a Critical Incident does not resolve itself through routine response measures; it requires a scaled, multi-agency approach to bring the situation under control, mitigate long-term impacts, and implement recovery strategies.

3.4 Emergency Declaration and Management within the Port

3.4.1 Declaring an Emergency

An Emergency within the port is declared when an event meets the defined criteria, necessitating immediate, but controlled intervention without constituting a Critical Incident. The declaration of an Emergency is the first escalation point in the Critical Incident Escalation Chain and serves as an early activation of structured response actions to prevent further deterioration of the situation.

The decision to declare an Emergency is made by the Port Duty Manager, Port Security Team, or an authorised operational lead, based on a structured assessment of the situation, including:

- Nature and severity of the incident (impact on safety, security, or operations).
- Likelihood of escalation into a wider security, safety, or environmental event.
- Resources required to manage the situation within standard operational parameters.
- Need for external support, such as emergency services or regulatory bodies.

Once an Emergency is declared, standard response measures are activated, including:

- Mobilisation of on-site personnel – security teams, operations staff, and first responders take immediate control of the situation.
- Incident communication protocols – internal notifications to key personnel, ensuring that relevant stakeholders are informed.
- Incident containment and mitigation – rapid implementation of measures to stabilise the situation, following established Standard Operating Procedures (SOPs).
- Initial incident assessment – dynamic risk assessment to determine if the situation is stabilising or requires further escalation.

If the incident remains contained within operational limits, the Emergency is resolved at this stage. However, if risk factors indicate a worsening situation, escalation to a Critical Incident is considered following the SBRF and ICIMP principles.

Examples of emergencies that has not escalated into a Critical Incidents:

- **Minor Fuel Spill at a Berth**

  A vessel experiences a minor diesel spill while refuelling. Port operations deploy containment booms, and environmental teams mitigate the spill without external regulatory intervention.

Resolution: The incident remains under control, following the Port Environmental Management Plan, and does not disrupt broader port operations.

- **Fire Alarm Activation in a Terminal**

A smoke detector triggers a fire alarm in a port terminal, but on-site personnel quickly identify it as a minor electrical fault with no active fire present.

Resolution: Engineering teams rectify the issue; fire services are notified but do not escalate beyond standard attendance.

- **Workplace Injury at a Cargo Handling Area**

  A stevedore suffers **a minor injury** while handling cargo. Immediate first aid is provided, and the worker is transported to medical care without major operational disruption.

Resolution: The incident is logged, reviewed under workplace health and safety (WHS) protocols, and closed without external agency escalation.

The First Escalation Point in the Critical Incident Management Chain

The declaration of an Emergency serves as the initial structured response in the Critical Incident Management Chain. If an event shows signs of escalation beyond standard response capabilities, it may transition to a Critical Incident, requiring:

- **AIIMS-based command structure activation** – establishing a Critical Incident Management Centre (CIMC).
- **Multi-agency coordination** – engaging emergency services, regulatory authorities, or external security forces.
- **Strategic decision-making** – executive-level involvement in managing high-risk operational disruptions.

By proactively addressing Emergencies, Darwin Port can prevent escalation into full-scale Critical Incidents, maintaining operational resilience and ensuring swift, structured responses to all emerging risks within the port environment.

3.4.2 Emergency Escalation & Resource Allocation

Level		Impact	Command Level	Resource Allocation
	Emergency	Localised incident with limited impact on port operations	Port Duty Manager / On-site Personnel	Managed using standard operating procedures (SOPs) and contingency plans; internal resources only; no external agency involvement unless escalation is required

Table 6

3.4.3 Critical Incident Levels and Escalation Framework

The Integrated Critical Incident Management Plan Framework within the port follows a structured escalation model, ensuring that incidents are managed effectively and proportionally to their severity.

The Darwin Port Integrated Critical Incident Management Plan identifies three (3) distinct levels of Critical incident.

3.4.3.1 Level Three (3) – Significant Incident

Definition:

A Level Three (3) Significant Incident is an event that causes operational disruption, but remains limited in scope and severity, with minimal impact on wider port operations.

Management & Response:

- Led by Port Operations/General Manager.
- Managed through Operational Contingency Plans and Standard Operating Procedures (SOPs).
- Activation of Business Continuity Plans (BCP) may be required for minor disruptions.
- Critical incident Management Team is activated, but external support is generally not required at this stage.

Escalation Criteria:

If the situation worsens, impacting multiple operational areas or showing early signs of uncontrollability, it escalates to Level Two (Major Incident).

3.4.3.2 Level Two (2) – Major Incident

Definition:

A Level Two (2) Major Incident has a substantial impact on port operations or specific critical infrastructure, requiring broader coordination and additional resource allocation.

Management & Response:

- ICIMT is fully established, led by a senior executive (General Manager or above).
- Requires Port-wide coordination and the implementation of Operational Contingency Plans to mitigate risk and stabilise operations.
- Mobilisation of moderate external resources, such as specialist contractors or emergency services in a supporting role.

Escalation Criteria:

If the incident poses significant risk to life, infrastructure, or critical port functions, requiring multi-agency coordination and emergency declarations, it escalates to Level One (1) (Critical Incident).

3.4.3.3 Level One (1) – Critical Incident

Definition:

A Level One (1) Critical Incident represents a severe and widespread impact on port operations or critical infrastructure, requiring immediate high-level intervention and external resource mobilisation.

Management & Response:

- CIMT assumes full control, operating under a Port-led but externally directed structure.
- Multi-agency coordination is activated, engaging emergency services, regulatory bodies, and external crisis management teams.
- Implementation of BCP/Recovery Plans to safeguard long-term operational continuity.
- Deployment of significant external resources, including specialist security, law enforcement, or emergency response personnel.

Escalation Criteria:

Level 1 represents the highest level of crisis escalation. The focus shifts from containment to long-term recovery and continuity planning, ensuring the port can resume operations in a controlled manner.

3.4.4 Incident Escalation & Resource Allocation

Level		Impact	Command Level	Resource Allocation
	**Level 1 – Significant**	Localised operational disruption	Port Led / General Manager	Internal staff, SOPs, BCP activation
	**Level 2 – Major**	Substantial impact on port operations or infrastructure	General Manager & CIMT	Moderate external support, operational contingency plans
	**Level 3 – Critical**	Severe, widespread operational and infrastructure impact	Full ICIMT, Multi-agency Response	Significant external resources, recovery and crisis management

Table 7

3.5 Guidance of Managing Emergencies

Darwin Port utilises reference and guidance information on the process for managing emergencies, critical incidents, and business disruptions through several interrelated plans. The following details the core focus of each plan and their Inter-relationships under the Strategic Business Resiliency Framework.

3.5.1 Darwin Port Business Continuity Plan

The Darwin Port Business Continuity Plan is a key component of the port's risk management strategy, designed to manage disruption-related risks and ensure operational resilience. Based on AS/NZS 5050:2010 and ISO 22310**,** the framework integrates governance, risk management, and business planning with Darwin Port's strategic objectives. It provides a scalable and flexible approach to continuity management, equipping managers with the tools and knowledge to implement effective plans while aligning with stakeholder priorities. This plan ensures Darwin Port can minimise disruptions, protect critical operations, and maintain stakeholder confidence during periods of uncertainty.

3.5.2 Integrated Critical Incident Management Plan (ICIMP)

Is the overarching plan detailing how the port responds to emergencies, integrates with local authorities, and activates internal response teams. This plan supports first response protocols in accordance with local sites emergency response procedures. The aim is to safeguard anyone affected, as well as to manage and contain the situation as rapidly and safely as possible. This may include support of off-site responding agencies, such as police and fire services.

3.5.3 Maritime Security Plan

Focuses on safeguarding the port from potential security threats, including terrorist attacks, by implementing preventive measures, early detection systems, and structured responses to protect lives and infrastructure.

3.5.4 Cyber Security Plan

Is designed to protect the Ports digital infrastructure and information systems from cyber threats, such as hacking, data breaches, and malware. It establishes protocols for preventing, detecting, and responding to cyber incidents that could disrupt operations or compromise sensitive data.

3.5.5 Cyclone Preparation and Response Plan

Ensures the port is prepared to respond effectively to cyclones by implementing precautionary measures, safeguarding infrastructure, and protecting personnel, while facilitating a rapid recovery post-incident.

3.5.6 National Oil Spill Response Plan

Designed to minimise environmental and operational damage by providing immediate, structured responses to oil spills. It outlines how to contain spills, protect marine ecosystems, and comply with environmental regulations.

3.5.7 Safety Management for Darwin Port Pilot Vessels

The Safety Management for Darwin Port Pilot Vessels outlines the purpose, processes, and procedures designed to ensure the safe and efficient operation of pilot vessels within Darwin Port's jurisdiction. Its

primary aim is to safeguard the health and safety of crew, pilots, and other personnel while maintaining the integrity of port operations. The scope of this management system encompasses all activities related to the operation, maintenance, and use of pilot vessels, including navigation, crew training, equipment standards, and emergency response protocols.

3.5.8 Marine Pilot Operational Management Manual

The Marine Pilot Operational Management Manual defines the standards, procedures, and protocols governing the safe and efficient conduct of marine pilotage within Darwin Port. Its purpose is to ensure the safety of navigation, vessels, port infrastructure, and the environment during pilotage operations. The scope of the manual includes all aspects of marine pilot activities, such as pilot boarding, navigation, communication protocols, and coordination with vessel crews and port control. It also addresses training, competency requirements, and emergency response procedures. By providing a structured framework aligned with regulatory and industry standards, the manual ensures consistency, safety, and operational reliability in all marine pilotage operations within Darwin Port.

3.5.9 Crisis Communications – To be implemented

An advanced communications plans for executive management and the critical incident management team in relation to internal and external Critical incident communication. The Critical incident Communications plan acts as blueprints for the Port in times of critical incident so that they can respond immediately.

4 Section Four – Critical Incident Management Framework

4.1 What is a Critical Incident?

A critical incident is a sudden and unexpected event that poses significant threats across multiple domains, including physical safety, psychological well-being, security, cyber integrity, and environmental stability. Such incidents have the potential to cause severe harm to individuals, disrupt normal operations, compromise safety and security measures, and negatively impact environmental conditions. Critical incidents often require immediate and coordinated response and intervention to prevent further harm, escalation, or deterioration of the situation. Additionally, they can:

- Threaten the financial stability of organisations such as Darwin Port or the broader Landbridge Group.
- Attract intense negative attention from media, the public, stakeholders, and tenants, potentially damaging stakeholder relationships.
- Impact regulatory compliance, leading to challenges in meeting legal and industry obligations.
- Incur legal liabilities, exposing the organisation to lawsuits and financial penalties.

Damage the organisation's reputation and be recognised as significant enterprise risks, undermining trust and credibility in the market.

4.2 What is Critical Incident Management?

Critical Incident Management is the process of preparing for, responding to, and recovering from significant events or incidents that have the potential to cause harm, disrupt operations, or pose a serious threat to safety, security, or public order. It involves a coordinated approach to managing the incident effectively, minimising damage, and ensuring a swift return to normalcy.

4.3 What is a Critical Incident Management Strategy?

Darwin Ports Critical Incident Management Strategy includes tactics designed to prevent a critical incident from occurring, whilst also supporting the effective and efficient response and recovery from a critical incident event should one occur. The principal elements of a CIMS are:

4.3.1 Prevention

Prevention is a crucial element of the CMS. Which focuses on the proactively identifying and mitigating risks to reduce the likelihood of critical incidents initially occurring. Effective prevention measures can significantly decrease the potential for harm and disruption, safeguarding an organisation's operations, assets and people.

4.3.2 Preparedness

Preparing for a critical incident is paramount in any business. Being prepared requires a proactive approach. By developing detailed plans, conducting regular training and exercises and ensuring all necessary resources are readily available will enhance the ability to get routine operations underway again with limited interruptions.

4.3.3 Response

The response element of the CMS should focus on the immediate actions taken to manage, contain and mitigate the impact of the incident once it has occurred. By responding rapidly to a critical incident, it will minimise harm to people, assets, ensuring business continuity and maintaining an organisations reputation with other business partners and the immediate community.

4.3.4 Recovery

The recovery phrase begins once the immediate threat is contained and focuses on the rebuilding ad healing. This is done by restoring normal operations and minimising the long-term impact of the incident. Recovery aims to help the organisation return to regular functioning; support affected individuals and learn from critical incident to improve future responses.

4.4 Critical Incident Management Cycle

Figure 2

4.5 Critical Incident Reaction

4.5.1 Pathway Management

Following the critical pathways below provides a clear, visual guide for decision-making during an incident, ensuring that key steps and escalation processes are followed efficiently. It simplifies complex actions, enhances communication, and helps to streamline the response by guiding personnel through the necessary procedures. This ensures that critical incidents are managed effectively and consistently across the organisation.

4.5.2 Critical Incident Decision Pathway

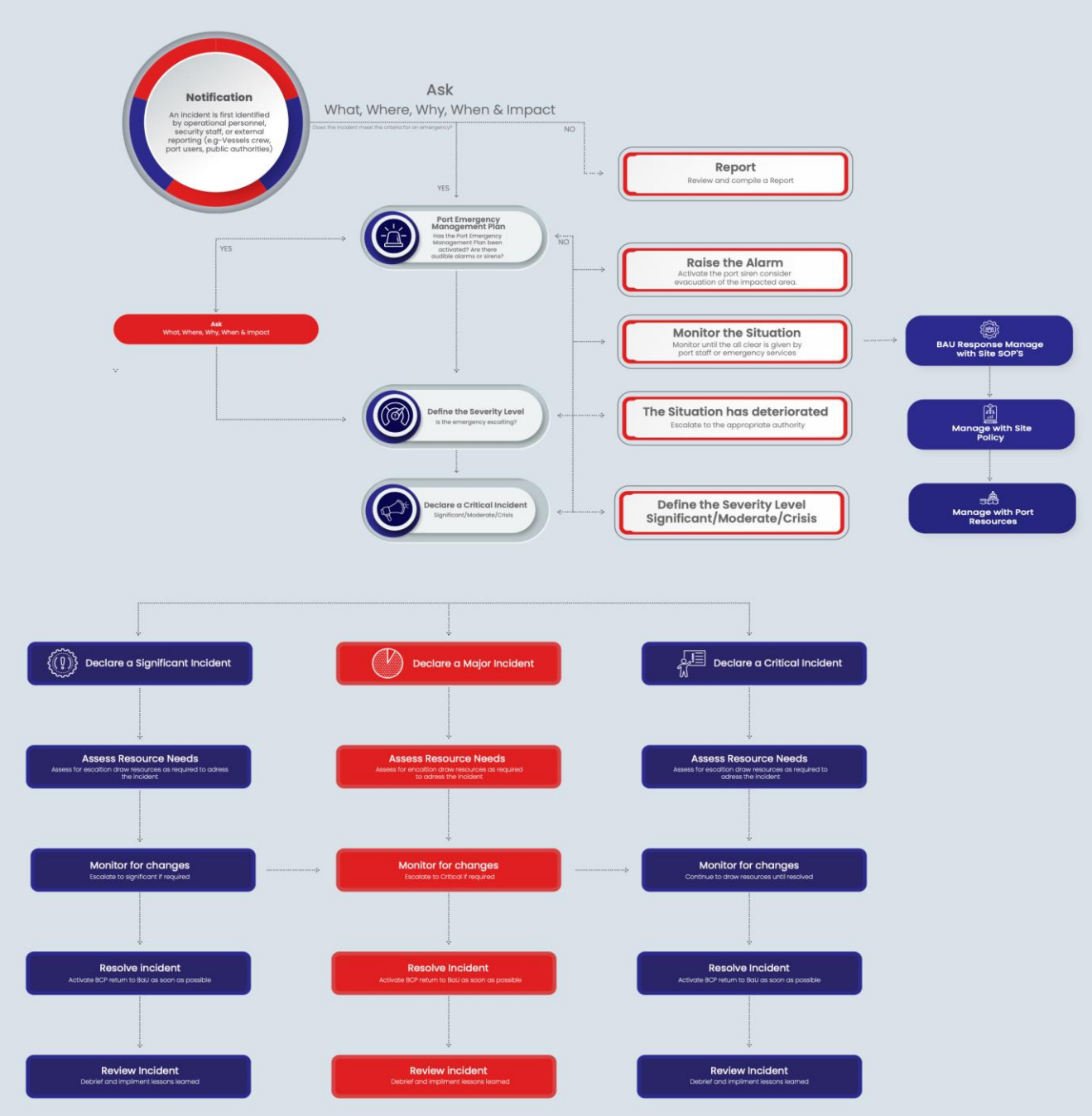


Figure 3

4.6 Critical Incident Team Operating Cycle

The Critical Incident management team operating cycle or “operational rhythm” is a systematic process designed to manage and resolve critical incidents efficiently. It begins with gathering essential information to understand the situation, using structured tools to collect facts, identify key stakeholders, and track infrastructure damage and casualties. This ensures a clear and accurate assessment of the incident.

Once the facts are established, the team prioritises issues based on their urgency and impact, using visual tools to focus efforts on the most critical concerns. From there, a tailored incident management strategy is developed and implemented, aligning actions with pre-established response plans and assigning responsibilities to ensure a coordinated and effective response. This process ensures that the incident is managed with clear direction, accountability, and a focus on minimising harm and restoring normal operations.

4.7 Critical Incident Decision Cycle

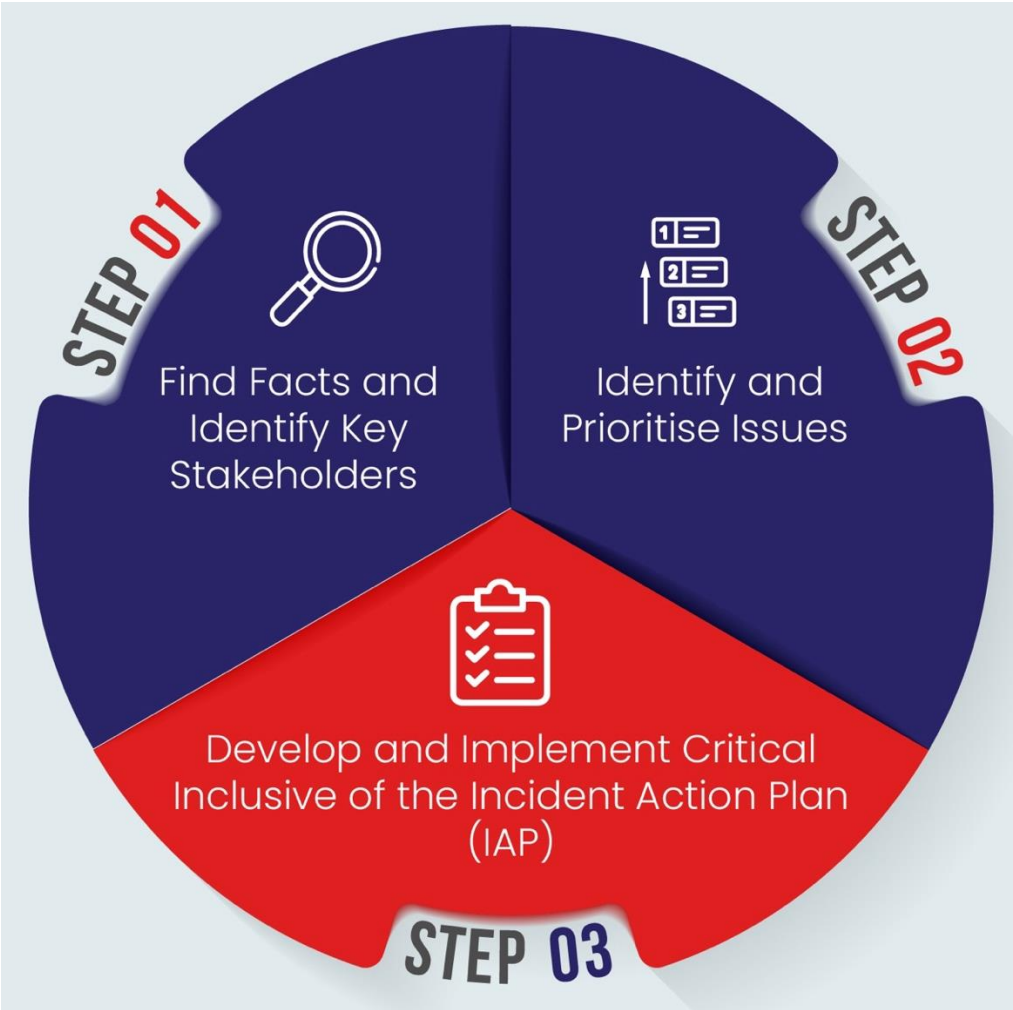


Figure 4

4.8 The SMEACS System

4.8.1 Situation, Mission, Execution, Administration, Command, and Safety

SMEACS is a useful acronym that stands for Situation, Mission, Execution, Administration, Command, and Safety. Here's a breakdown of how each element applies to with the Darwin Port Integrated Critical Incident Management Plan (CIMP):

4.8.1.1 Situation

Overview of the Incident: Describe the nature of the critical incident, including what has happened, where it occurred, and when it began.

Current Status: Provide information on the current status of the incident, including ongoing impacts, affected areas, and initial assessments.

Threat Assessment: Outline any potential threats or complications that may arise, including environmental factors or secondary hazards.

4.8.1.2 Mission

Objectives: Clearly define the primary goals of the CIMP, such as safeguarding lives, protecting property, and restoring normal operations.

Expected Outcomes: Specify the desired outcomes of the response, including timelines and measurable success criteria.

4.8.1.3 Execution

Actions and Strategies: Detail the specific actions to be taken by the response team, including resource deployment and operational tactics.

Roles and Responsibilities: Assign roles to team members and clarify their responsibilities in executing the plan.

Timeline: Outline key timelines for actions and responses, including any critical deadlines.

4.8.1.4 Administration

Resource Management: Describe how resources (human, financial, and material) will be managed, including procurement processes and logistics.

Documentation: Explain the documentation processes, including record-keeping, reporting requirements, and how information will be communicated to stakeholders.

Welfare and Support: Include provisions for the welfare of staff and responders, such as mental health support and rest periods.

4.8.1.5 Command

Command Structure: Define the command hierarchy, identifying key personnel and their roles within the incident management team.

Decision-Making Processes: Outline how decisions will be made, including who has the authority to approve actions and changes to the plan.

Coordination with Agencies: Specify how coordination will occur with external agencies and stakeholders involved in the response.

4.8.1.6 Safety

Safety Protocols: Establish clear safety protocols to protect personnel and stakeholders during the incident response.

Risk Assessment: Include ongoing assessments of safety risks associated with the incident and response activities.

Emergency Procedures: Detail emergency procedures for evacuations, medical assistance, and other safety measures.

By using the SMEACS framework in a CIMP, teams can ensure a structured, comprehensive approach to incident management, enhancing clarity and effectiveness in responding to critical situations while prioritising safety.

5 Section Five – Critical Incident Management Team Structure

5.1 ICIMT Structure Overview

The CIMT compromises of a core group of subject matter experts, who work in functional teams providing accurate, timely and in-depth guidance and advice to the CIMT Leader.

Aligning with the AIIMS structure, the CIMT members may work within one of a number of key areas, these areas may be supported by one or more person teams, each with a different functional role under the CIMT Leader.

Note: Due to the limited number of available staff, the Darwin Port ICIMP has activated the four (4) primary cells within the CIMT only.

5.2 Darwin Port ICIMT Structure

This provides for functional capability and considers the probability of extended periods of operation against fatigue and sustainability from within the Darwin Port management team.

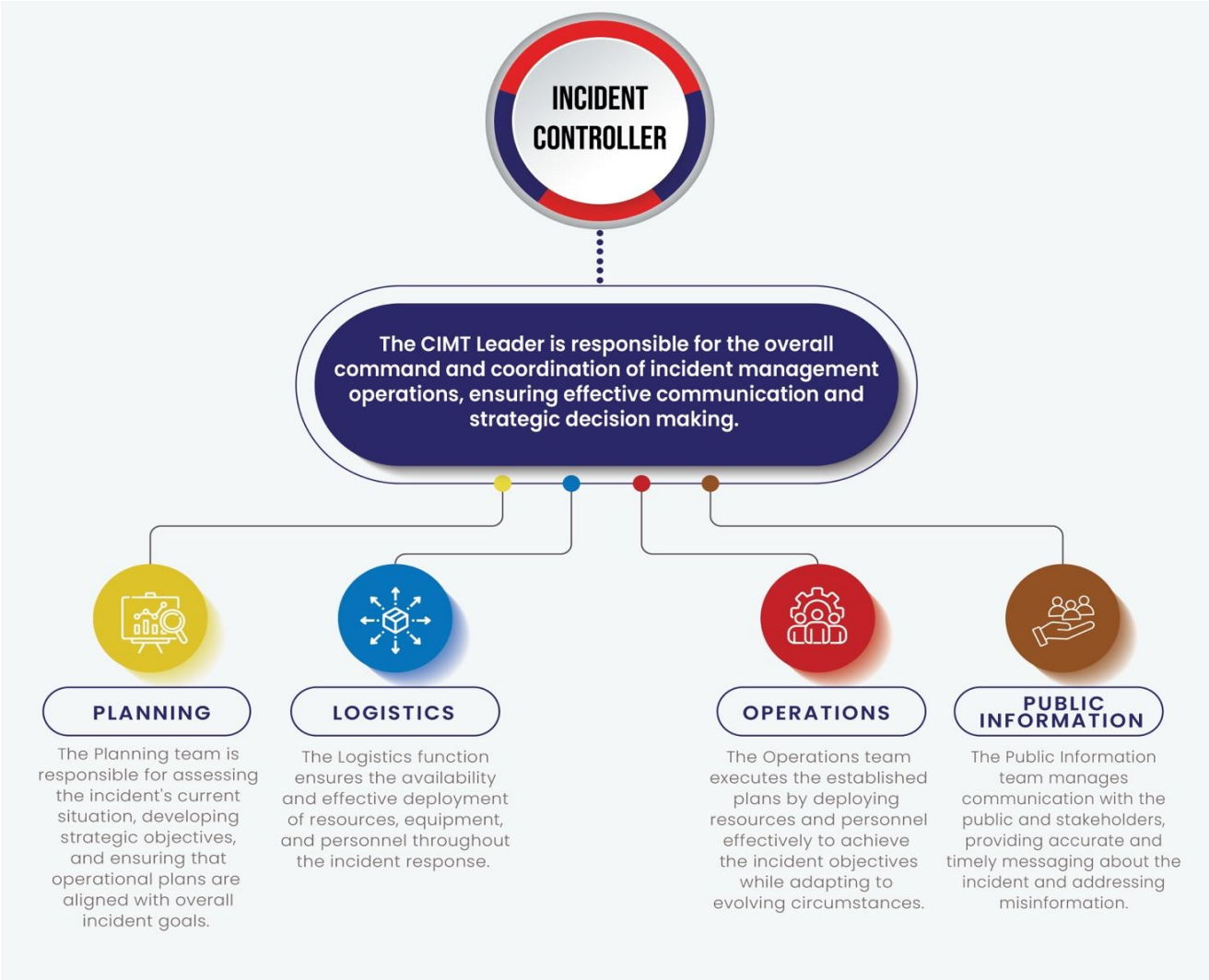


Figure 5

5.3 Critical Incident Management – Team Responsibilities

Darwin Port prepares for critical incident's, using a planned management structure, with defined roles and responsibilities.

The CIMT provides leadership and direction during a critical incident or business disruption. It is primarily responsible for the strategic direction and operational management of a critical incident affecting Darwin Port, clients and stakeholders, including the response and recovery of business unit functions other core responsibilities include:

- Evaluating in predicting the present and future extent and impact of the incident by continually assessing risk, identifying strategies, tools, interdependencies and associated resources and facilities required to recover the business accordingly.
- Determining recovery priorities for the Darwin Ports business unit and other related sites specific priorities.
- Ensuring employee welfare arrangements are in place during and after an incident.
- Managing resources, including materials, equipment, employees and funds.
- Communicating with relevant emergency response agencies in relation to the response to the incident.
- Overseeing all financial aspects of the response and providing advice across the CIMT to facilitate use of financial resources and tracking and managing incident related expenditure appropriately in line with Darwin Ports policy.
- Ensuring appropriate legal advisors are always in place for the Darwin Ports business units and the Port, managing liability, insurances and investigations.
- Ensuring the CIMT 's record keeping sits within an appropriate legal framework.
- Coordinating the recovery and restoration phases of the Darwin Ports' operations.
- Facilitating communications between recovery managers, the CIMT and other key stakeholders as part of the response and recovery phases.
- Updating Darwin Port on planned recovery actions, developments and other matters or actions taken by Darwin Port.

5.4 Functional Roles

The CIMT structure remains flexible so it can respond appropriately to situation-specific demands with staffing arrangements designed to ensure the Team has appropriate expertise and capacity to meet situational demands without compromising employee welfare. The CIMT Leader invokes these arrangements.

5.4.1 Critical Incident Management – Team Leader

The CIMT Leader' s functions and responsibilities include, but are not limited to:

- Overall responsibility for the management of all activities and personnel deployed to resolve the incident.
- Management of the interface with organisations and people working beyond the incident management structure especially with the Lead Combat Agency.
- Management of the interface with organisations, tenets, clients, communities, and people affected by, or likely to be affected by the incident.
- Actively direct and support the CIMT and ensure effective communication links across management teams. Other key responsibilities include continually assessing risk and ensuring employee welfare arrangements are in place during and after an incident.

5.4.2 Planning Officer

A Planning Officer, if necessary, may be appointed by the Incident Controller and delegated with the authority to:

- Take responsibility for preparation and delivery of the plans and strategies required to help control the incident.
- Undertake a risk assessment.
- Maintain a resource management system for all of the resources that have been allocated to the incident.
- Identify and locate Specialists and SMEs as required.
- Assemble, maintain and provide incident information.
- Establish and manage a planning section, if necessary, given the size and complexity of the incident.

5.4.3 Operations Officer

The Operations Officer acts as the operational and communication link between the Incident Commander(s) and the CIMT, supporting operational tasks to ensure the business can continue functioning during the critical incident. This role involves anticipating the incident's likely progression, assessing key risk exposures, and identifying the strategies, tools, interdependencies, and resources needed for business recovery.

The Operations Officer's duties and responsibilities include, but are not limited to:

- Implementing strategies to resolve the incident.

- Managing all activities undertaken to directly address the incident.
- Overseeing the resources, including personnel and equipment, assigned to the operations section.
- Establishing an operational structure and allocating resources to ensure safe work practices for personnel at the incident site.
- Implementing procedures for the welfare of operational personnel.
- Contributing to the development of the Incident Action Plan.

5.4.4 Logistics Officer

The Logistics Officer is responsible for acquiring and managing resources, facilities, services, and materials to support incident control. Key responsibilities include:

- Ensuring a safe environment for logistics personnel.
- Receiving briefings from the Incident Controller.
- Developing and Organising the Logistics Section's plan.
- Assigning tasks and managing resources, such as vehicles, food, accommodation, and PPE.
- Facilitating communication and cooperation with relevant parties.
- Providing logistical support updates and estimating future needs.
- Establishing staging areas if necessary.

The Logistics Officer should plan for up to 72 hours of CIMT activity, coordinating with HR for welfare and WHS issues, and ensuring continued support for business recovery and operations beyond this period if needed.

5.4.5 Public Information Officer – (Communications)

Public information plays a crucial role in managing any incident, focusing on gathering, organising, and disseminating timely and relevant information to stakeholders outside the incident management team. It supports incident management by:

- Providing warnings and information to potentially affected businesses, stakeholders, and the public.
- Liaising with the news media and handling media-related issues.
- Consulting and communicating with affected tenants.

The public information cell is responsible for safeguarding and enhancing the Organisation ’s reputation by managing all communications, both internally and externally, including media relations. This involves developing and implementing a Communication Plan that outlines key internal and external stakeholders, core messages, and communication channels.

5.5 Cell Functions

5.5.1 Planning Cell

The role of the Planning Cell within a Critical Incident Management Team is to support the response by anticipating resource needs, documenting ongoing operations, and developing action plans for current and future challenges. The Planning Cell gathers and analyses critical information to inform decision-making, forecasts incident development, and ensures all actions are coordinated with the broader response objectives. It also maintains situational awareness, prepares reports, and ensures resources, logistics, and personnel are optimally deployed to manage the incident effectively.

- Collect and analyse data to provide situational awareness and inform decision-making.
- Create and update incident action plans (IAPs) to address both immediate and long-term operational needs.
- Anticipate and plan for required resources, ensuring that personnel, equipment, and support are allocated efficiently.
- Ensure accurate and timely documentation of incident operations, decisions, and actions taken during the response.
- Facilitate communication and coordination between different sections of the incident management team, ensuring alignment with overall response objectives.

5.5.2 Operations Cell

The Operations Cell serves as the link between the Incident Commander(s) and the CIMT, facilitating operational communication. It supports tasking related to ongoing operations, including maintaining business continuity during the crisis. The Operations Cell also predicts the incident's development, assesses key risk exposures, and identifies strategies, tools, interdependencies, and resources required for business recovery. Its duties and responsibilities include, but are not limited to:

- Implementation of strategies to resolve the incident.
- Management of all activities that are undertaken directly to resolve the incident.
- Management of resources people and equipment assigned to the operations section.
- Establishing operational structure and allocating resources to enable safe work practices to be implemented by personnel on the incident ground.
- Implementing procedures for the welfare of operational personnel and;
- Contributing to the development of the Incident Action Plan.

5.5.3 Logistics Cell

At a small incident the Incident Controller may perform the logistics function. The Logistics Officer’s role and responsibilities are to obtain and maintain human and physical resources, facilities, services, and

materials in support of the control and resolution of the incident. The Logistics Officer's role and responsibilities include, but are not limited to:

- Provide a safe working environment for all Logistics personnel.
- Obtain a briefing from the Incident Controller.
- Develop the Logistics Section's component of the Incident Action Plan.
- Plan the organisation of the Logistics Section.
- Allocate tasks to Section personnel.
- Support control of the incident through the procurement and maintenance of human and physical resources, facilities, services and materials.
- Facilitate effective liaison and cooperation with all relevant persons.
- Provide progress reports on logistical support for the incident to the Incident Controller.
- Estimate future service and support requirements.
- Facilitate the establishment and maintenance of staging areas (if required) in support of the

5.5.4 Sustaining CIMT Operations

The Logistics Officer should consider planning cycles of up to 72 Hours in order to sustain CIMT activity and other business operations, with advice from a nominated HR SME about associated welfare and WHS issues and coordinate the people and other resources required to sustain CIMT activities, recover the business, and support business operations beyond 72 hours if required.

5.5.5 Public information Cell

Is Responsible for managing the communication and dissemination of information to the public, media, and stakeholders during a critical incident. This cell plays a vital role in ensuring that accurate, timely, and coordinated messages are delivered to prevent misinformation, manage public perception, and maintain trust. They work closely with the incident command team to align public messaging with the overall response strategy, ensuring that updates are clear and consistent across all communication platforms. Their tasks include managing media relations, handling inquiries, and providing updates on safety measures and incident progress.

Key responsibilities of the Public Information Cell include:

- Craft and release clear, accurate, and consistent information to the public and stakeholders.
- Act as the main point of contact for the media, providing regular updates and responding to media inquiries.
- Track public response and media coverage to ensure accurate information is being reported and adjust messaging if needed.

- Work closely with incident management teams to ensure that public messaging aligns with operational strategies and objectives.
- Regularly inform the public about safety measures, potential risks, and the progress of the incident response.

5.6 Additional Roles that May be Activated

5.6.1 Finance Cell

The finance cell has responsibility to oversee all financial aspects of organisation's crisis response and provide advice across the CIMT to facilitate use of financial resources and track and manage incident-related expenditure appropriately in line with Port policy.

5.6.2 Legal and Admin Cell

The Legal and Admin cell ensures appropriate legal advice is in place for the Port and the Board at all times and provides legal support for each team member individually depending on the severity of the crisis and personal liability.

Key responsibilities include, but are not limited to:

- Assessing risk and Managing liability.
- Insurance and investigation aspects at all levels.
- Ensuring the CIMT 's administrative support and record keeping sit within an appropriate legal framework.

5.6.3 Information, Communication and Technology (ICT) Cell

The Information, Communications and Technology (ICT) Cell provides support to the Incident Control Hub and to the Incident Control Cell, through Information, Communications and Technology support and advice.

5.6.4 Business Resiliency Team

The Business Resiliency Team can comprise of a number of elements depending upon the situation. These elements will be activated as required by the CIMT Leader and will be tasked with undertaking the direct work associated with the relief and recovery aspects of the Incident Action Plan and Recovery Plan. In addition, the business Resiliency team may undertake actions identified within the Ports Business Continuity Framework and Plan.

5.7 Notification and Activating the ICIMP

This plan can be activated by the following people:

The following Managers have the Authority to Activate the ICIMP on advisement to their respective Heads of Department
Darwin Ports CEO
General Manager – Operations.
Senior Manager Landside Operations
Duty Operations Manager.

Table 8

The authority activating the ICIMP, or their nominated representative, will be responsible for identifying a Critical Incident Management Team Leader and notifying Darwin Port clients and stakeholders of Darwin Port's intent to stand up the CIMT in response to a critical incident event.

The CIMT Leader is responsible for activating the CIMT. The CIMT Leader will decide which elements of the CIMT they require predicated upon the situation and the specific nature and impacts of the event on BaU operations.

5.8 CIMT Authority

The Critical Incident Management Team (CIMT) operates under the authority delegated by the port's governance framework to manage and respond to critical incidents. The CIMT ensures that decisions and actions are executed efficiently within predefined limits of authority. While the team is empowered to act decisively in real-time to mitigate risks and manage the incident's impact, it functions within the boundaries set by the port's operational and legal guidelines.

The CIMT leader holds ultimate responsibility for approving all strategic actions within the Critical Incident Management Team, ensuring alignment with the port's objectives and regulatory compliance.

This centralised approval ensures accountability while enabling the team to respond dynamically and effectively to unfolding crises.

5.9 Emergency Related Critical Incident

Notification of a Significant, Major or Critical Incident is to be a priority. Initial notification within Darwin Port is to be made to the appropriate senior manager. All necessary details (see the Incident Notification Checklist at Annex C). If unable to contact the appropriate senior manager., they are to contact the General Manager – Operations or delegate.

5.10 Notification Timing

The criticality of the incident will drive the speed and level of notification. Although common sense will generally guide the speed of notification, the chart below provides the minimum requirements expected.

Impact Level		Notification Timeframes	
		Port to General Manager Operations or Delegate	**General Manager Operations to Executive**
	Emergency	45 Mins	60 Mins
	Level 1 – Significant	45 Mins	60 Mins
	Level 2 – Major	30 Mins	45 mins
	Level 3 – Critical	10 Mins	20 Mins

Table 9

5.11 Communication Flow

- **Incident Discovery**: Staff or monitoring systems detect an incident.
- **Initial Assessment**: Duty Manager assesses the severity and assigns an initial escalation level.
- **Notification**: Communication follows the notification protocols.
- **Escalation**: If unresolved or escalates in severity, move to the next level of escalation.
- **Resolution**: Once the incident is resolved, a debrief and incident report are prepared.

5.12 Communication to Key Stakeholders

See Key Stakeholders List Attachment C.

6 Section Six – Critical Incident Management Centre (CIMC)

6.1 Establishing the CIMC

When the authorised person responsible activates this ICIMP, an appropriate predesignated location is selected to establish a management centre for the relevant team, (as seen in the table below). If the primary locations are unavailable (e.g. due to the critical incident event), the alternate location shall be utilised. In making this decision and based on the event circumstances, the authorised person must consider the following:

- The current and future threat.
- Accessibility functionality of the secondary location; and
- Location of CIMT members.

The authorised person responsible for activating this plan nominates the location in the initial notification message. Team members assemble at the given location, which becomes the central point for that team's communication and management activities.

The predesignated locations below have been established with the equipment, resources and configuration necessary to support management functions, so the team can command, control, coordinate and communicate Darwin Ports response efficiently and effectively.

CIMC Priority	**Cyclone Location**
Primary	Meeting Room 3
Secondary	Meeting Room 2
Tertiary	Remote With GMO In Attendance with at NTG Emergency Centre as Part of a Whole of NT Response.
CIMC Priority	**Non – Cyclone Location**
Primary	Meeting Room 3
Secondary	Fort Hill Wharf
Tertiary	Remote and GMO To Discuss with NTC as Part of Ongoing Emergency Response Discussions.

Table 10

6.2 Critical Incident Management Centre – Infrastructure Requirements

The site will be established to allow the CIMT to Command Control and Communicate (Darwin Ports response and recovery actions. The site will contain the following infrastructure as a minimum, including the Darwin Port ICIMP "Go Box":

Information	**Tech**
• Building and wharf site plan, including the location of electricity, water and gas shut off points. • Access to electronic CIM documentation. • Printed copies of all Incident Management forms and duty statement. • A list of employees at each site, their contact details (including next of kin). • Insurance company contact details. • List of clients, tenants, subcontractors and supplier details (this should be provided from existing systems e.g. Salesforce, ensure hardcopies are printed). • Emergency Service point of contact details.	• Spare mobile phones and Prepaid sim cards and chargers. • Low frequency 2-way radios with spare batteries and chargers. • Laptops & chargers. • Printer and printer paper. • Extension cords and power boards (tagged and tested). • Power – multiple power outlets. • Internet – wireless and hardline (if available). • Video conferences capability (if available). • Access to a TV for viewing free to air media.
Stationary	**Other**
• General stationary (pens, white board markers, staples, highlighters, blue tac, magnets). • Whiteboard/Smartboard. • Butchers paper/Flip Charts. • Spare batteries for torches.	• Spare key security codes or proximity cards. • First aid kit. • Torch. • Drinking water. • Table for at least ten (10) people. • Small break out tables x 3 (could be in adjacent Rooms). • Access to bathrooms.

Table 11

6.3 Alternate CIMC – Activation Procedure

The activation procedure is as follows:

- Contact alternative site to advise of incident and activation of alternative premises.
- Confirm available resources at alternative site.
- Confirm phone numbers and alternate site for phone diversions.
- Confirm with site contact, relocation numbers an estimated time of arrival.
- Provide key staff with contact numbers and relocation address. Key staff to relocate using private vehicles and or taxis; and,
- Liaise with site contact provide further resources as required.

7 Section Seven – Document Management

7.1 Document Ownership and Accuracy

The General Manager – Operations or Delegate maintains this plan. Their responsibilities include the following, but are not limited to:

7.2 Document Currency:

Liaise with appropriate people to ensure the document content is current.

7.3 Distribution and Access

Provide identified members with the current copy of the ICIMP and ensure the document is accessible to all staff.

7.4 Application and Training

Coordinate appropriate training for any Darwin Ports employees reasonably expected to have responsibilities detailed with this ICIMP.

7.5 Continuous Improvement:

Responsible for the plan's compliance and improvement.

Note: The General Manager -Operations or Delegate is responsible for ensuring staff and contact details are correct within this document. To ensure this plan is accordance with relevant legislation and business expectations an annual plan review will be undertaken.

7.6 Plan Review

The ICIMP will be reviewed regularly and updated to ensure the Darwin Port managers, staff and key stakeholders are familiar with the ICIMP and that it reflects Darwin Ports changing operational and business needs.

7.7 Plan Rehearsal

It is critical that Darwin Port Exercises this ICIMP to ensure that it remains valid, relevant and useful. This is done as part of an ongoing training program and is a key factor in the successful implementation of the recovery strategies. Darwin Port will seek to rehearse this plan in part or full at least once per year and if possible, in conjunction with other relevant emergency and security management plan.

7.8 Induction and Training

7.8.1 Integrated Critical Incident Management Plan Familiarisation

As soon as they are listed as a CIMT member or alternate, it is mandatory for such staff to obtain and keep an accessible copy of the current ICIMP. Darwin Port will provide identified managers and staff with relevant training, which includes employees' roles within this plan. Darwin Port will provide annual refresher training or as required training to support skills retention. Darwin Port requires all employees with an identified role in this plan to acknowledge in writing that they have attended training, understood their roles and responsibilities and had access to a copy of the plan.

7.8.2 Training and Exercise Schedule

The training requirements for the Darwin Port Integrated Critical Incident Management Plan (ICIMP) are designed to ensure that all personnel are equipped with the necessary skills and knowledge to effectively respond to critical incidents. This comprehensive training program will cover key areas, including incident response protocols, risk assessment, communication strategies, and the use of relevant technologies. Participants will engage in practical exercises and simulations to reinforce their understanding of the ICIMP framework, enhance coordination among teams, and improve decision-making in high-pressure situations. Continuous training and assessment will be implemented to keep staff updated on best practices and emerging threats, fostering a culture of preparedness and resilience within Darwin Ports operational environment. Please see Annex B – Training and Exercise Schedule for more details.

7.9 Record Keeping

7.9.1 Legal Record Keeping Requirements

Meticulous record-keeping is vital to the Darwin Port Strategic Business Resiliency Framework (SBRF) and critical event response. The ICIMT maintains detailed records to ensure effective communication, coordination, and evidence-based learning. This documentation supports legal proceedings, cost recovery, and inquiries post-event. Templates and tools are provided to streamline the record-keeping process for CIMT members.

7.9.2 Record Keeping Protocol

Members must adhere to strict record-keeping protocols, saving digital copies of completed templates, notes, images, emails, and text messages, and uploading them to the Darwin Port Electronic File System.

- Upon activation, members should start recording information using the designated templates and tools and continue using these formats throughout the event.

- The primary method is to input notes directly into digital templates; printed templates can be used as a backup for handwritten notes.
- Handwritten records must be transferred to digital templates as soon as possible and before leaving the site. These should be scanned and uploaded to an agreed location.
- All incident records and data should be catalogued in digital files using the approved file name format.

7.10 Staff Welfare

Darwin Port commits to ensure that its absolute priority during and after any event that has triggered this plan, is the welfare and safety of its employees, contractors and others who may be adversely affected by an incident.

The CIMT is responsible for managing the effective welfare response during and after an event. At a high level, CIMT members identify, analyse and address welfare risks continually throughout Response and Recovery phases.

As part of the Incident Action Plan, the CIMT Leader initiates immediate and ongoing actions to address welfare requirements with advice from the nominated Human Resources representative.

7.10.1 All Staff Welfare Checks

The CIMT Leader ensures that an All-Staff Welfare Check is coordinated through the nominated Human Resources representative within 30 minutes of CIMT activation, or as soon as practicable, depending on the incident type and at regular intervals during the event.

7.10.2 Next of Kin Contact Protocol

If a Darwin Port employee is seriously injured or dies, the CIMT Leader takes advice from the nominated Human Resources representative who implements Darwin Ports “Next of Kin” notification procedure”. Death notifications may be required to be undertaken by the relevant state Police Service.

7.11 Sustained Operations Protocol

7.11.1 Strategic and Operational Risk Context

The CIMT Leader is accountable for their respective Teams' composition throughout the incident and preserving employees' welfare is their paramount concern.

The CIMT Leader assesses the situation to determine any specialist demands and the duration for which their Team is likely to be active. Accordingly, he/she will implement a two or three shift rotation for incidents requiring sustained CIMT operation over a prolonged period.

The shifts will consist of equally qualified and experienced personnel and be capable of acting autonomously over the shift period.

7.12 Handover Procedures

As a person completes their shift in one of the CIMT roles, they must conduct a handover to the incoming person that is relieving them. The handover is a structured briefing process encompassing the following:

- The current and predicted situation.
- Goals and activity objectives.
- Execution – how the goals and objectives will be achieved.
- Administration
- Organisational and Structural Communications
- Team members begin preparing for an upcoming handover as soon as the CIMT Leader announces a shift rotation or if the shift rotation is detailed on a CIMT roster. Shift lengths are to be determined in line with existing Darwin Port employment agreements, contracts or arrangements.

7.13 Internal Reporting

The CIMT Leader is responsible for keeping Darwin Port Executive Leadership Group up to date and highlighting any risks that may impact the Port's major stakeholders, or reputation.

7.14 Social Media and News Media

Modern media, particularly social media, has accelerated the speed that information about a critical incident can spread. The viral effect of social networks, such as Facebook and X, means that stakeholders can break news faster than traditional media – making managing a critical incident even harder.

To mitigate this, Darwin Port has a planned approach to releasing information to the media in the event of a critical incident that includes a media reaction plan. This plan will seek to protect Darwin Port and more broadly Darwin Ports reputation by overseeing all communication from Darwin Port to key internal and external stakeholder groups.

All attempts will be made to ensure that a Port media representative is part of the CIMT, but in those situations where this is not possible the CIMT leader will act as the Port spokesperson.

All attempts should be made to align any media releases with those being published by any responding emergency service. The Public Information Officer is responsible for ensuring relationships with emergency service media personnel is established early in any incident

8 Section Eight (8) – Risk Management

8.1 Risk Context

An underpinning element of Darwin Port SBRF, and this ICIMP, is Darwin Ports Risk Management Principles. As part of the Risk Management process, Darwin Port has identified Key Strategic Risks across Security Risk and Emergency Risk which have been used to define the Risk Context. These risks are contained within the relevant reference documents. Please see internal reference Documents – Table 5.

8.2 Business and Operational Risk Context

Darwin Port has undertaken Risk Assessments that consider several key risk areas including, but not limited to:

8.2.1 People

This area focuses on the risks associated with personnel, including employee safety, health, training, and compliance with labour laws. It also encompasses the management of human resources, including recruitment, retention, and ensuring a safe work environment.

8.2.2 Property

This includes risks related to physical assets such as buildings, equipment, and inventory. Effective property risk management involves assessing vulnerabilities, ensuring adequate insurance coverage, and implementing security measures to protect assets from theft, damage, or natural disasters.

8.2.3 Processes

This area addresses the risks associated with operational processes, including inefficiencies, compliance failures, and disruptions. Effective process management involves identifying potential operational risks, implementing controls, and continually monitoring processes for improvement.

8.2.4 Reputation

This encompasses risks that can impact an Organisation ’s reputation and brand value. It includes public perception, customer satisfaction, and the potential fallout from negative incidents, such as data breaches or poor service. Managing reputation risk involves proactive communication strategies, stakeholder engagement, and crisis management planning.

A direct result of this work is the identification and construction of several recovery plans designed to guide and support the rapid return to Business-as-Usual operations. Darwin Port maintains this detailed business risk register with ongoing reviews undertaken annually.

8.3 Incident Recovery

8.3.1 Recovery Management

When the immediate aspects of the critical incident are addressed, and when considered appropriate, the CIMT Leader, with support from the appropriate CIMT representatives activates the Recovery Plan (under the Incident Action Plan) to guide a phased Recovery and business continuity. The CIMT continue to operate post-critical incident through any "clean-up" and "return-to-work" operations. Should, the incident or event be of a great scale involving state and/or federal government intervention, Darwin Port recovery processes will dovetail into the Local, Regional and or State arrangements under the coordination of a recovery coordinator.

If it is a local event the recovery coordinator will be supported by the Municipal Recovery Manager. Regional level support will be by Department of Health and Human Services, and State level will be provided by the state Emergency Management Organisation. It is an expectation that the CIMT Leader will liaise closely with the designated recovery agency.

8.3.2 Recovery Plan

The Recovery Plan outlines the tools, interdependencies, utilities and facilities required to transition back to normal business, including estimated or target timelines. It addresses areas including:

- Closing incident operations and supporting or resolving logistical demands.
- Continuity of financial control measures.
- Meeting the welfare needs of three key groups:
  - Darwin Port employees or contractors who have been involved in managing the event.
  - Employees who have been affected by the event, but were not involved in managing the event and;
  - Members of the public who have been affected by the event.
- Monitoring and triaging risks:
  - Continuing or closing established communications and conducting a recovery communications program (internal and external).
  - Standing Down the CIMT.

8.4 Post Incident Actions

8.4.1 Stand Down

When the CIMT has recovered the situation to the point it can be controlled through normal channels and procedures, the CIMT stands down. The CIMT Leader stands down the CIMT officially with verbal and text/email notifications and ensures this direction is noted within the records. The CIMT Leader is responsible for directing the CIMT stand down process which includes the following:

- Ensure the Recovery Plan accounts for all relevant elements of the transition back to BaU
- Collate records/evidence and save files to the agreed directory.
- Standing down any support staff.
- Notify all CIMT members/alternates of stand down.
- Advise any stakeholders that the CIMT has engaged with that the CIMT is closing and the transition back to business as usual has occurred.
- Continuing or closing established communications.
- Continuity of any financial control measures.
- Monitoring and triaging residual risks.
- Provide a closing brief to the Board/others.
- Pack away equipment and resources at location(s).
- Schedule any subsequent meetings and follow-up and nominates personnel to manage/ attend.
- Ensure employees understand arrangements for routine stress debriefing/trauma counselling and that they have a safe means of transport home.
- Meeting the welfare needs of stakeholders; and,
- Facilitate a Hot Debrief.

8.4.2 Extended Support

Some select support may still be required from certain elements of the CIMT to assist the Site Manager and operational and shift teams as they fully return to normal operations and functioning. The CIMT Leader will coordinate this with the relevant mangers and staff.

8.4.3 Psychological First Aid

Depending on the nature and severity of the incident, Darwin Port may arrange stress debriefing/trauma counselling as part of the stand down procedure for identified staff or stakeholders.

Human relations representatives should coordinate with appropriate counselling and psychological services.

Members of the public/victims who have been affected by the incident will be directed to publicly available services by the relevant emergency.

8.4.4 Debriefing – (Hot)

The CIMT Leader conducts a Hot Debrief with CIMT members and key stakeholders to capture key learnings and issues, highlight sensitivities and restricted information, detail expected media interest and Darwin Ports position, close discussion and summarise next steps before formally standing down personnel and sending them home/back to work safely.

Consider what worked well and what could be done differently next time.

8.4.5 Improvement Cycle – Post Incident Review (PIR)

Darwin Port will ensure post-event knowledge is attained to continue to develop this ICIMP and build upon its resilience.

When a BCP or critical incident is resolved, the CIMT Leader schedules and directs a follow up 'Learning Phase', where Darwin Port management and staff collectively come together to undertake a Post Incident Review (PIR). The PIR seeks to identify ways in which to improve the plans, systems and people that contribute to this ICIMP, Critical incident Management capability and preparedness and then detail actions required to implement these.

The scope of the Learning Phase, and the associated PIR, may include reviewing the incident, evaluating the effectiveness of the overall response or select elements of the response, the application of the plans and the CIMT 's performance. The scale of the phase will depend on the significance and impact of the event and may result in a single meeting or an extended program of interviews and meetings, that may include support staff and external agencies.

A PIR should be conducted at a suitable time shortly after the event to identify gaps, follow-up actions, key impacts and future prevention strategies. When conducting a PIR:

- Focus on the three 'W's';
    - What happened?
    - What went well?
    - What can we do differently next time?
- A PIR should be timely, accurate, interactive, objective and constructive, but not personal.
- Different techniques can be used to collect information including surveys, workshops and/or interviews.

- Consider who the best person is to facilitate a PIR (e.g. good rapport with staff, excellent communication skills).

Note: The greatest learnings are usually realised through observations and enhancements identified through the detail and data captured within the records kept during the event. As such, it is imperative that record keeping is of an extremely high standard.

LANDBRIDGE DARWIN PORT

Partnering in growth, connecting people and supporting potential

ICIMP Attachment One (1)

Critical Incident Management

Team Leader - Duty Statements

Duty Statements
Duty Card (1) – Critical Incident Management - Team Leader
Duty Card (2) – Planning Cell - Team Leader
Duty Card (3) – Logistics Cell - Team Leader
Duty Card (4) – Operations Cell - Team Leader
Duty Card (5) – Public Information Cell - Team Leader

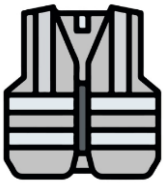
Published June 2025

Partnering in growth, connecting people and supporting potential

Duty Card One (1)

Critical Incident Management Team Leader

Position filled by	P: S:



CIMT Leader

Team Leader Role Purpose & Function

- Takes on the role of Incident Controller until relieved by Lead Combat Agency.
- Responsible for taking charge and exercising leadership of the response.
- Leads the activities of the CIMT members.
- Develops strategies & objectives.
- Establishes effective relationships with stakeholders.
- Approves plans.
- Ensures that the response is carried out safely, efficiently and in collaboration with any response agencies.

Role	Expectation
Experience or Qualifications	Relevant experience in a leadership role plus experience managing incident response or incident management qualifications. Seniority that allows the ability to make key decisions for the incident response without further approval needing to be sought.
Leadership	Ability to lead a team on demand, demonstrate sound judgement and remain calm under pressure. Ability to influence others to achieve their best. Ability to take responsibility for outcomes and implement changes for improvement.
Collaboration & Negotiation	Ability to collaborate with others to achieve outcomes, ability to negotiate with a wide range of stakeholders including senior members of response agencies.
Problem Solving	Ability to identify risks/issues, consequences, options, provide recommendations and implement solutions with ease.

Table 1

Key Interface	
Darwin Port Management	Provide updates on the situation.
CIMT Members	Provide guidance, direction and feedback.
Combat Agency Incident Controller	Keep advised, provide advice and assistance, obtain regular updates.
Key external stakeholders	Provide updates on the situation and impacts to the stakeholder.

Table 2

Duty Card One (1)

Team Leader Responsibility Checklist

Activations and Assembly

Immediate Action	
Obtain a situation update on the incident.	☐
Review incident severity and determine level of activation required.	☐
Activate relevant CIMT personnel.	☐
Start an Incident Action Log and proceed to the Critical Incident Management Centre.	☐
Set the briefing and reporting schedule (briefings should be no longer than 15-20 mins).	☐

Table 3

Initial CIMT Briefing

Immediate Action	
Conduct an initial team brief detailing response priorities, objectives and risks (SMEAC).	☐
Advise team of briefing and reporting schedule.	☐
Allocate tasks to relevant team members.	☐

Table 4

Incident Control

Immediate Action	
Lead the CIMT and manage its strategic response priorities.	☐
Review the response by convening CIMT update briefings at regular intervals.	☐
Set recovery and business resumption goals and provide ongoing advice during planning.	☐
Consider insurance and legal aspects of situation.	☐
Keep the CEO informed via regular updates.	☐
Update staff when required.	☐
Ensure active and ongoing engagement with all stakeholders, in consultation with the Communication Manager.	☐
Authorise all communication materials for release internally and externally.	☐
Continually review the actions completed.	☐
Document all personal actions and decisions in a personal log.	☐
Decide when the Critical Incident is over in conjunction with the CEO.	☐

Table 5

Duty Card One (1)

Post Incident Control

Immediate Action	
Lead the CIMT and manage its strategic response priorities.	☐
Review the response by convening CIMT update briefings at regular intervals.	☐
Set recovery and business resumption goals and provide ongoing advice during planning.	☐
Consider insurance and legal aspects of situation.	☐
Keep the CEO informed via regular updates.	☐
Update staff when required.	☐

Table 6

Duty Card Two (2)

Planning Cell - Team Leader

Planning

Position filled by	P: S:

Team Leader Role Purpose & Function

- Reports to the CIMT Leader Managers members of the Planning Team.
- Responsible for forward planning for response and recovery operations.
- Evaluates and analyses intelligence on current and forecast situation.
- Develops objectives, strategies & options.
- Undertake risk assessments.
- Prepares and disseminate plans.
- Provides technical advice and collects and maintains information regarding resources allocated to the incident.
- Planning team provides management support and administration services to the CIMT.

Role	Expectation
Experience or Qualifications	Relevant experience in the strategic management of planning functions or incident management qualifications.
Leadership	Ability to lead a team on demand, demonstrate sound judgement and remain calm under pressure.
Develop Outputs	Ability to perform consistently, efficiently, professionally with quality and detail. Ability to produce detailed documents with ease.
Collaboration & Negotiation	Ability to collaborate with others to achieve outcomes, ability to negotiate with a wide range of stakeholders.
Problem Solving	Ability to identify risks/issues, consequences, options, provide recommendations and implement resolutions.

Table 1

Key Interface	
CIMT Leader	Provide updates on the situation.
CIMT Cell Leaders	Keep advised and provide feedback.
Combat Agency Incident Controller	Keep advised, provide advice and assistance, obtain regular updates.
Team Members	Provide guidance and advice on tasks and activities to be undertaken.

Table 2

Duty Card Two (2)

Team Leader Responsibility Checklist

Activations and Assembly

Immediate Action	
Proceed to the Critical Incident Management Centre (CIMC) and start an Incident Action Log.	☐
Gather resources needed to set up the CIMC (Office Supplies, IT equipment, maps/charts etc).	☐
Display CCTV feed of incident scene within CIMC (if available).	☐
Start an Incident Action Log for your cell and proceed to the CIMC.	☐

Table 3

Initial CIMT Briefing

Immediate Action	
Attend CIMT briefings which will detail response priorities, objectives and risks.	☐
Advise CIMT Leader of additional resources required and raise any concerns regarding the response.	☐
Maintain a record of the briefing minutes.	☐

Table 4

Incident Control

Immediate Action	
Ensure all actions, TX and RX is recorded in the Incident Action Log.	☐
Publicise the briefing and reporting schedule (set by CIMT Leader) to CIMT members.	☐
Maintain any displayed information (on whiteboards or walls) to ensure currency.	☐
Analyse information on the current and projected incident situation.	☐
Identify new and emerging risks for the incident.	☐
Seek input from other CIMT members on their incident response planning needs.	☐
Develop the Incident Action Plan (IAP), include any contingency planning.	☐
Seek approval of the IAP from the CIMT Leader.	☐
Continually review IAP to ensure currency and makes updates as required (seek CIMT approval).	☐
Liaise with Logistics to identify resource requirements.	☐
Liaise with Operations to identify any response requirements.	☐
Maintain a register of resources available, including their location and status.	☐
Collect, collate and store incident records.	☐

Table 5

Duty Card Two (2)

Post Incident Control – Stand down

Immediate Action	
The CIMT Leader will advise once the incident response is to be ceased and the CIMT stood down, this will trigger a transition to recovery.	☐
Develop a demobilisation plan, consider surplus resources, logistics capabilities & release priorities.	☐
Develop recovery plans if needed.	☐
Submit recovery and/or demobilisation plans to CIMT Leader for approval.	☐
Disseminate recovery and/or demobilisation plans to CIMT following approval.	☐
Continue to work with CIMT on their needs during demobilisation and recovery.	☐
Complete any outstanding actions or obligations.	☐
Conduct debriefs with Planning personnel to capture opportunities for improvement.	☐
Attend CIMT debrief to capture opportunities for improvement.	☐
Close the CIMC and collect all documentation.	☐
Ensure all documentation or records are filed.	☐
Reprint any documentation and set up resources ready for the next incident.	☐

Table 6

Partnering in growth, connecting people and supporting potential

Duty Card Three (3)

Logistics Cell - Team Leader

Position Filled By	P: S:

Logistics

Team Leader Role Purpose & Function

- Reports to the CIMT Leader.
- Manages members of the Logistics Team.
- Responsible for acquiring and distributing equipment, materials and infrastructure in support of the operational response including human resources, facilities and services.
- Manages finances/budgets for the response.
- Manages storage of equipment, sourcing suppliers & providing catering (can also include travel arrangements for responding personnel including accommodation etc).

Role	Expectation
Experience or Qualifications	Relevant experience in the logistics operations, procurement or incident management qualifications in Logistics.
Leadership	Ability to lead a team on demand, demonstrate sound judgement and remain calm under pressure.
Develop Outputs	Ability to perform consistently, efficiently, professionally with quality and detail. Ability to influence others or have existing relationships with suppliers.
Collaboration & Negotiation	Ability to collaborate with others to achieve outcomes, ability to negotiate with a wide range of stakeholders.
Problem Solving	Ability to identify risks/issues, consequences, options and provide recommendations.

Table 1

Key Interface	
CIMT Leader	Provide updates on the situation.
CIMT Members	Keep advised and provide feedback.
Team Members	Provide guidance and advice on tasks and activities to be undertaken.
Suppliers	Maintain good relationships and communications.

Table 2

Duty Card Three (3)

Team Leader Responsibility Checklist

Activations and Assembly

Immediate Action	
Proceed to the Critical Incident Management Centre (CIMC) and start a Logistics Log.	☐

Table 3

Initial CIMT Briefing

Immediate Action	
Attend CIMT briefings which will detail response priorities, objectives and risks.	☐
Advise CIMT Leader of any logistics concerns or risks regarding the response.	☐
Maintain a record of the briefing minutes.	☐

Table 4

Incident Control

Immediate Action	
Ensure all actions, discussions, decisions, information received or given is recorded in the Incident/Logistics Action Log.	☐
Determine structure of Logistics team and resources required to fulfil roles.	☐
Liaise with Operations and Planning on equipment needs.	☐
Identify logistics needs and issues to support response planning (See below Table).	☐
Distribute equipment and resources to the relevant locations.	☐
Contribute to the develop of the Incident Action Plan.	☐
Liaise with other CIMT members to inform strategic and operational decisions.	☐
Provide advice to Planning on shortfalls in equipment availability.	☐
Prioritise and manage all resources assigned to the function.	☐
Identify and communicate current or emerging risks to the logistics function.	☐
Ensure Logistics Personnel are assessing risks prior to undertaking tasks.	☐
Ensure Logistics Personnel are briefed and debriefed on current situation and strategies.	☐
Provide advice & recommendations to the CIMT Leader regarding Logistics.	☐

Table 5

Duty Card Three (3)

Post Incident Control - Standdown

Immediate Action	
Contribute to the development of the demobilisation & recovery plans & strategies.	☐
Brief Logistics personnel on demobilisation plans and strategies.	☐
Implement demobilisation plan for the logistics function.	☐
Ensure team is available to assist with the implementation of recovery plan.	☐
Complete any outstanding actions or obligations.	☐
Conduct debriefs with Logistics Personnel to capture opportunities for improvement.	☐
Attend CIMT debrief to capture opportunities for improvement.	☐
Provide all documentation to Planning for filing.	☐

Table 6

Partnering in growth, connecting people and supporting potential

Duty Card Four (4)

Operations Cell - Team Leader

Position Filled By	P: S:

Team Leader Role Purpose & Function

- Reports to the CIMT Leader.
- Manages members of the Operations Team.
- Is responsible for leading the operations response to the incident.
- Ensures effective, timely, efficient and consistent actions are taken to resolve the incident.
- Facilitates the implementation of the Incident Action Plan (IAP) and any other operational plans.

Role	Expectation
Experience or Qualifications	Relevant experience in the strategic management of operational functions or incident management qualifications.
Leadership	Ability to lead a team on demand, demonstrate sound judgement and remain calm under pressure.
Develop Outputs	Ability to perform consistently, efficiently, professionally with quality and detail.
Collaboration & Negotiation	Ability to collaborate with others to achieve outcomes, ability to negotiate with a wide range of stakeholders.
Problem Solving	Ability to identify risks/issues, consequences, options, provide recommendations and implement resolutions.

Table 1

Key Interface	
CIMT Leader	Provide updates on the situation.
CIMT Cell Leaders	Keep advised and provide feedback.
Combat Agency Incident Controller	Keep advised, provide advice and assistance, obtain regular updates.
Team Members	Provide guidance and advice on tasks and activities to be undertaken.

Table 2

Duty Card Four (4)

Team Leader Responsibility Checklist

Activations and Assembly

Immediate Action	
Proceed to the Incident Management Centre and start an Incident Action Log.	☐
Make contact with the affected site and seek a Situation Report (SitRep) on the incident.	☐
Mobilise any additional resources required immediately.	☐

Table 3

Initial CIMT Briefing

Immediate Action	
Attend CIMT Briefings which will detail response priorities, objectives and risks.	☐
Advise CIMT Leader of additional resources required and raise any concerns regarding the response.	☐
Maintain a record of the Briefing minutes.	☐

Table 4

Incident Control

Immediate Action	
Ensure all actions, discussions, decisions, information received or given is recorded in the Incident Action Log.	☐
Determine structure of operations team and resources required to fulfil roles.	☐
Provide incident updates to Planning (planning will update the SitRep accordingly).	☐
Discuss equipment needs with Planning.	☐
Establish access to any equipment needed (once provided by Logistics).	☐
Liaise with other CIMT members to inform strategic and operational decisions.	☐
Manage and coordinate all field or site-based response operations.	☐
Priorities and allocate tasks and manages all resources (people and equipment) assigned to the function.	☐
Identify and communicate current or emerging risks.	☐
Ensure operations Personnel are assessing risks prior to undertaking tasks (Take 5).	☐
Ensure Operations Personnel are briefed and debriefed on current situation and strategies.	☐
Ensure Operations personnel are advised of their roles once combat agency has arrived on scene and how they can assist.	☐
Provide advice & recommendations to the CIMT Leader.	☐

Table 5

Duty Card Four (4)

Post Incident Control – Stand down

Immediate Action	
The CIMT Leader will advise once the incident response is to be ceased and the CIMT stood down, this will trigger a transition to recovery.	☐
Contribute to the development of the demobilisation & recovery plans & strategies.	☐
Brief Operations personnel on demobilisation plans and strategies.	☐
Implement demobilisation plan.	☐
Ensure team is available to assist with the implementation of recovery plan (recovery is a process of assisting individuals, businesses or the community to achieve an effective level of functioning.	☐
Complete any outstanding actions or obligations.	☐
Conduct debriefs with Operations Personnel to capture opportunities for improvement.	☐
The CIMT Leader will advise once the incident response is to be ceased and the CIMT stood down, this will trigger a transition to recovery.	☐
Attend CIMT debrief to capture opportunities for improvement.	☐
Provide all documentation to Planning for filing.	☐

Table 6

Partnering in growth, connecting people and supporting potential

Duty Card Five (5)

Public Information Cell - Team Leader

Position Filled By	P: S:

Team Leader Role Purpose & Function

- Reports to the CIMT Leader.
- Leads and manages the production and dissemination of relevant, timely, informative and action based public information to the public and media.
- Manages social media posts.
- Manages media response and interviews.
- Collates any on site footage.
- Does not manage internal communications between teams or contractors or communications with response agencies.

Role	Expectation
Experience or Qualifications	Relevant experience in a leadership role plus experience in managing external communications and media or incident management qualifications in Public Information. Understanding of stakeholder expectations for public information.
Leadership	Ability to lead a team on demand, demonstrate sound judgement and remain calm under pressure.
Develop Outputs	Ability to perform consistently, efficiently, professionally with quality and detail. Ability to produce public facing documents/communications with ease.
Collaboration & Negotiation	Ability to collaborate with others to achieve outcomes, communicates clearly & concisely across diverse groups, ability to negotiate with a wide range of stakeholders.
Problem Solving	Ability to identify risks/issues, consequences, options, provide options & recommendations.

Table 1

Key Interface	
CIMT Leader	Provide updates on the situation.
CIMT Members	Provide guidance, direction and feedback.
Key external stakeholders	Provide updates on the situation and impacts to the stakeholder.
Lead Combat Agency Media	Align messaging.
Media	Provide updates as required.

Table 2

Duty Card Five (5)

Team Leader Responsibility Checklist

Activations and Assembly

Immediate Action	
Proceed to the Critical Incident Management Centre (CIMC) and start a Media Information Log.	☐

Table 3

Initial CIMT Briefing

Immediate Action	
Attend CIMT briefings which will detail response priorities, objectives and risks.	☐
Advise CIMT Leader of additional resources required and raise any concerns regarding the response.	☐
Maintain a record of the briefing minutes.	☐

Table 4

Incident Control

Immediate Action	
Ensure all actions, discussions, decisions, information received or given is recorded in the Incident/Media.	☐
Determine structure of Public Information team and resources required to fulfil roles.	☐
Work with Lead Combat Agency Media team to ensure messaging is aligned across agencies.	☐
Disseminate warnings, information, advice and safety messages to affected stakeholders.	☐
Answer enquiries from the public regarding the incident.	☐
Liaise with Planning to inform decision making process regarding information that needs to be disseminated.	☐
Maintain information on the current and projected incident situation to ensure disseminated information is current.	☐
Use all available sources of information to ensure a broad picture of the incident situation, including social media, media outlets, community networks and the community.	☐
Coordinate any formal media briefings.	☐
Collection of on the ground footage.	☐
Maintaining consistent messaging across all stakeholders to maintain a ‘single point of truth’.	☐
Coordinate any community stakeholder meetings or any other public engagement activities.	☐
Be proactive with dissemination of information.	☐

Table 5

Duty Card Five (5)

Post Incident Control – Stand down

Immediate Action	
The CIMT Leader will advise once the incident response is to be ceased and the CIMT stood down, this will trigger a transition to recovery.	☐
Continue to provide public information to stakeholders regarding any recovery operations relevant to them.	☐
Continue to work with CIMT on their needs during demobilisation and recovery.	☐
Complete any outstanding actions or obligations.	☐
Conduct debriefs with Public Information personnel to capture opportunities for improvement.	☐
Attend CIMT debrief to capture opportunities for improvement.	☐
Provide all documentation is filed.	☐

Table 6

End

DARWIN PORT
LANDBRIDGE

Partnering in growth, connecting people and supporting potential

ICIMP - Attachment Two (2) –

Critical Incident Management Centre - Sign in Sheet

Name	Title/Position	Phone	Email	Time In	Time Out

Table 1

All persons entering the CIMC must sign in/out. (**NO Exceptions**)(Print as Required)

Partnering in growth, connecting people and supporting potential

ICIMP - Attachment Three (3) -

Incident Action Log - (IAL)

Each person filling any CIMT role must maintain an Incident Action Log.

Record all information regarding the response below including who Darwin Port spoken to, phone conversations, directions given, directions received, decisions made, information received etc. Any relieving person must start a new page.

Logs should be printed, and handwritten notes taken, this eliminates technical issues during an incident.

Full Name:		**Date:**	
Cell		**Incident Level** **Critical/Major/Significant**	
Incident:			

Time	**Activity/Action** (who you spoke with, directions given, information received etc.)	**Action Required (Y/N)**	**Action Completed**
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐

(Print as Required)

Time	**Activity/Action** (who you spoke with, directions given, information received etc.)	**Action Required (Y/N)**	**Action Completed**
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐

Table 1 (Print As Required)

Partnering in growth, connecting people and supporting potential

ICIMP - Attachment Four (4) -

Incident Action Plan - (IAP)

Objectives & Strategies

Incident Name:			
Date		**Time:**	
Plan for the period from:		**Plan for the period to:**	
Plan Status	☐ Draft ☐ Approved	**Plan Prepared By:**	
Estimated Staff Involved		**Injured/Casualty (if Known)**	

Table 1

Environmental								
Tide	High:	Low:	**Wind**	Direction:	Speed	**Light**	Sunset:	Sun Rise:

CIMT Structure			
Role	**Current Position – Full Name**	**Relieving Position – Full Name**	**Phone of Relieving Position**
CIMT Leader			
Planning Cell Team Leader			
Logistics Cell Team Leader			
Operations Cell Team Leader			
Public Information Cell Team leader			

Table 2

Partnering in growth, connecting people and supporting potential

What is happening?
The Situation report should detail what has happened, where, and when; identifying who or what has been impacted; estimating the problem's size, scope, area, numbers, and potential secondary hazards; summarising any Work Health and Safety (WHS) concerns, including injuries or fatalities; and ensuring that if this is a subsequent Incident Action Plan (IAP), any outdated information is removed.
Situation:
What are the objectives?
Setting clear objectives within an Incident Action Plan (IAP) is vital for effective incident management. Objectives should be specific, measurable, achievable, relevant, and time-bound (SMART) to ensure all team members understand their roles. Each objective must address immediate needs, such as safeguarding lives and protecting property, while being regularly reviewed and adjusted as the situation evolves. Involving key stakeholders in this process enhances collaboration and improves the overall effectiveness of the response efforts.
Objective:

Objective by Priority	**Strategies:** Means of accomplishing objectives.
1.	
2.	
3.	
4.	

Table 3

Partnering in growth, connecting people and supporting potential

Predicted Situation	
When predicting changes in a critical incident for an Incident Action Plan (IAP), assess factors like the incident's evolving nature, resource availability, stakeholder impacts, and environmental conditions. Look for signs of escalation or de-escalation, including shifts in public sentiment and emerging hazards. Analysing situational reports and on-ground feedback helps ensure timely adjustments to strategies and objectives, maintaining an effective and adaptable response	
Infrastructure at Risk	
Critical	**Non - critical**
Resources at Risk	
Critical	**Non - critical**
Resources	
Ordered	**Deployed**

Table 4

How will assets and resources be deployed?
In an Incident Action Plan (IAP), assets and resources will be deployed based on the incident's needs and established objectives. This involves identifying critical resources and determining their optimal allocation for an effective response. Deployment strategies will consider factors like location, availability, and urgency, with clear communication channels for coordination. Regular assessments will guide adjustments to ensure efficient and targeted response efforts as the situation evolves.
What administration functions are currently in use or require establishment?
In the Incident Action Plan (IAP), current administration functions include documentation management, resource allocation, and communication protocols. Establishing functions such as incident tracking, personnel accountability, and financial oversight is essential for effective management. These processes ensure smooth information flow, efficient resource use, and accountability, with regular reviews identifying gaps to enhance operational effectiveness.
Additional information relevant to the IAP.
Communication of the IAP.
Effective communication is vital during a critical incident, necessitating a clear list of communication methods and key contacts. This includes using email for formal correspondence, a landline for the Critical Incident Management Centre , mobile phones for real-time updates among CIMT members, and radio for immediate communication with ground crews. The IMR landline number should be specified, along with phone numbers and email addresses for all CIMT members. Additionally, contacts for emergency agencies, ground crews, key contractors (security, maintenance, trades), tenants, and utility providers (power, water, gas, network) must be included to ensure efficient coordination and response efforts.

Table 5

Safety Assessment.
Safety management during the critical incident response is vital and will be incorporated into all operations. A risk assessment or "Take 5" process will be required before activities, with safety information recorded in designated logs. Fatigue management protocols will establish maximum shift durations for field and CIMT teams. Responders must have the appropriate training and skills, while a designated safety officer will oversee compliance and personnel wellbeing. A clear process for accessing medical treatment will be in place, and existing business processes will be adapted as needed to ensure all safety measures are documented.
List any attached document here.
Ie, Maps schematics drawings or plans.
1. 2. 3. 4. 5.

Table 6

Authorisation.		
NOTE: The IAP must be Signed by the CMT Leader.		
Prepared By: Planning Officer	Name:	
Approved By: CIMT Leader	Name:	Sign:
Date:		

Table 7

(Print As Required)

End

ICIMP -Attachment Five (5) -
CIMT Situation Report

SitRep No#:

Date	
Incident	
Location	
Your Name	
CIMT Leader	

Note: Information detailed below should be factual and largely without interpretation and speculation. Information should cover the period between the last SitRep and the next scheduled SitRep.
SitReps should be numbered in order, starting at 1.

Situation

Detail:

- What has happened, where and when?
- Who or what has been impacted?
- Estimate of the problem (size, scope, area, numbers, secondary hazards).
- WHS summary (any injuries or fatalities, extent of WHS issues).
- If this is a subsequent SitRep, remove old information that is no longer relevant.

Insert the details of the situation here:

Table 1

Impact

"What are impacts have occurred to structures, people, community"?

Consider:

- What are the impacts to the built environment
- How has the incident impacted people
- How has the incident impacted stakeholders or tenants
- How has the incident impacted the surrounding areas

Insert details of impact here:

Table 2

Resources

"What resources are being used, needed or not available"?

Consider:

- Personnel
- Contractors
- Tools, equipment and,
- Vehicles etc.

Insert resources here:

Table 3

Executions

"Detail what has been done, what is being done, and what needs to be done, refer to IAP for guidance"

Consider:

- What personnel are responding on site
- What equipment is being used
- What activities are being undertaken
- What interactions are occurring with emergency services
- What is the prognosis based on current progress
- Any outstanding actions and any additional resources required to close out

Insert actions here

Table 4

Emerging Issues

"Are there any emerging issues that have not already been considered"

Consider:

- Any emerging community, media or political issues
- Any threats/hazards likely to cause secondary issues

Insert emerging issues here:

Table 5

Prognosis

"Detail how the response is being administered"

Consider:

- What is likely to occur if IAP strategies are successful
- What could happen to stop the strategies from working, what do you need?
- Future expectations both internal and external
- Influences on completion e.g. lack of resources, weather, WHS issues etc.

Insert prognosis here:

Table 6

Safety

"Insert any known hazards/threats or any emerging safety issues"

Consider:

- Any requirements for risk assessment or Take 5 prior to response activities.
- Where safety information should be recorded.
- Fatigue management for both field and CMT teams, can include maximum shift times.
- Requirements for training or specific skills for responders.
- Who is managing/overseeing safety in relation to the response.
- Process for any medical treatment for responders if needed.
- Existing business processes can be used or modified for the response as needed, don't reinvent the wheel, just ensure it is detailed in this section.

Insert safety concerns here:

Table 7

Reporting

SitRep frequency should be determined by the CMT Leader in consultation with the CMT and Combat Agency. The frequency will reduce as the crisis recovery progresses. The frequency will be detailed in the IAP

Next SitRep is due:

Table 8

Authorisation

Prepared By:	Name:
Approved By:	Name:

Table 9

(Print as Required)

ICIMP - Attachment Six (6)

Incident Summary Display Board

This is a snapshot of the incident response; it should reflect the most current IAP and SitRep. It should be displayed on a wall within the IMR.

INCIDENT SUMMARY – DISPLAY BOARD					
Date:		**Incident Location:**			
Incident Name/description:					
Mission/Objective:	*(Copy from IAP)*				
Incident Impacts					
Impact on Personnel (Deceased, injured, missing, uninjured)			**Impact on Assets**		
Impact on Stakeholders			**Impact on Community**		
Impact on the Environment			**Other Impacts**		

Table 1

Key Contacts								
Stakeholder	**Name**	**Position**		**Phone**				**Email**
Fire & Rescue								
Police								
Site Managers								
Incident Controller								
Tenants	**Name**	**Company**	**Contact No**	**Email**	**Name**	**Company**	**Contact No**	**Email**

Table 2

(Print as Required)

Partnering in growth, connecting people and supporting potential

Annex A – Darwin Port ICIMP CIMT Contact Details

Team Leader/ Title	Name	Phone	Email
CMT Leader - Primary			
CMT Leader - Secondary			
Planning Cell Leader - Primary			
Planning Cell Leader - Secondary			
Operations Cell Leader - Primary			
Operations Cell Leader - Secondary			
Logistics Cell Leader - Primary			
Logistics Cell Leader - Secondary			
Public Information Cell Leader - Primary			
Public Information Cell Leader - Secondary			

Table 1

Update as required

Annex B – Darwin Port ICIMP Training and Exercise Schedule

#	Exercise Type	Scenario/Focus Area	Objectives	Frequency	Responsible Party	Output/Documentation	Post Ex Report Title Number
Drills							
1	*Tabletop Exercise*	*Bomb threat and evacuation scenario*	• *Test decision-making under pressure* • *Validate notification escalation paths* • *Review chain of command*	*Annually*	*ICIMT Lead*	• *Exercise summary report* • *Debrief notes*	Ex Runaway Voltage 2025 v1.0
2							
3							
4							
5							
6							
Exercises							
1							
2							
3							
4							
5							

Table 1

Update as required

Annex C – Notification and Escalation Checklist

Notification & Escalation Framework

The ICIMP establishes a three-tiered escalation structure for Critical Incidents, and a flat response model for Emergencies. Notification responsibilities scale proportionally to the severity of the incident.

Emergency events are managed using SOPs and port staff. Critical incidents require a formal activation of the ICIMP and Critical Incident Management Team (CIMT), with notifications to stakeholders, senior managers, and emergency agencies.

Who can activate the ICIMP?

- CEO
- General Manager – Operations
- Senior Manager Landside Operations
- Duty Operations Manager

Response timeframes for notification (per ICIMP Table 9):

The criticality of the incident will drive the speed and level of notification. Although common sense will generally guide the speed of notification, the chart below provides the minimum requirements expected.

Impact Level		**Notification Timeframes**	
		Port to General Manager Operations or Delegate	**General Manager Operations to Executive**
	**Emergency**	45 Mins	60 Mins
	**Level 1 – Significant**	45 Mins	60 Mins
	**Level 2 – Major**	30 Mins	45 mins
	**Level 3 – Critical**	10 Mins	20 Mins

Table 1

Note: *All incidents must be logged, assessed, and escalated using the pathway in Figure 3, page 35 of the ICIMP. Use the SMEACS model for situational awareness, execution, and communication.*

Partnering in growth, connecting people and supporting potential

Escalation Roles and Trigger Guidance

Impact Level		Trigger	Responsibility	Action Summary
	Emergency	Localised event contained with SOPs	Port Duty Manager	Notify GM Ops; log incident; consider escalation
	Level 1 – Significant	Minor operational disruption; no external agency	General Manager	Activate ICIMP partially; internal coordination
	Level 2 – Major	Cross-functional impact; risk to assets or operations	General Manager + CIMT	Full CIMT activation; notify stakeholders and emergency responders
	Level 3 – Critical	Severe, multi-agency crisis; high reputational risk	CIMT Leader + Exec	Activate full crisis structure; report to Exec + regulators; initiate full recovery planning

Table 2

Checklist Item	Applies to Level	Responsible Party	Completed By	Time Completed	Complete
Incident logged in CIMT system	All Levels	First Responder			☐
Initial severity assessment completed	All Levels	CMT Leader/Duty manager			☐
Notification to General Manager	All Levels	CMT Leader/Duty manager			☐
Notification to Executive (if required)	L1–L3	GM Operations			☐
Incident declared as Critical Incident	L1–L3	CMT Leader/GM Operations			☐
Activation of ICIMP and team notification	L1–L3	CMT Leader or Delegate			☐
MARSEC level assessed and updated (if applicable)	L3	Port Security Officer			☐
SitRep and escalation logs initiated	L2–L3	Planning Officer			
SMEACS briefing framework initiated	L2–L3	CMT Leader/Planning officer			
Communication with lead combat agency confirmed	L2–L3	Logistics Officer			

Integrated Critical Incident Management Plan (ICIMP)

Rev 4.2 – June 2025

Appendix D

EMT/CMT Emergency Contact Directory

Revision History

REVISION	DATE	DESCRIPTION	AUTHOR	REVIEWER	APPROVAL
A – E	2015/1016	Compilation & DP review	Jim Morrison (**add energy**)	DP GMO & PMG	
0	8 April 2016	Authorisation for issue	Jim Morrison (**add energy**)	DP GMO	DP CEO
1	30 January 2018	Update logo, DP contacts & DP roles	Alleen Breward - Executive Assistant	DP GMO	DP CEO
1.1	12 June 2018	Content Review	Ian Niblock	GMO	
1.2	19 June 2018	PMG Review		PMG	
1.3	26 June 2018	Staff Review		DP Personnel	
1.4	27 June 2018	Content Approval	Ian Niblock	GMO	
2.0	27 June 2018	Authorisation for Issue	Terry O'Connor	CEO	CEO
2.1	14 June 2019	Annual Content Review	Gary Bawden	DOM	
2.2	14 June 2019	Content Approval	Ian Niblock	GMO	
3.0	14 June 2019	Authorisation for Issue	Terry O'Connor	CEO	CEO
3.1	15 January 2020	Contacts Updated Only –Approval Not Required	Alleen Breward	EA	N/A
3.2	17 June 2020	Contacts Updated Only – Approval Not Required	Amanda McCourt	GMO	N/A
3.3	23 June 2020	Update Distribution List only – Approval not required	Ian Niblock	GMO	N/A
3.4	23 June 2023	Contacts Updated Only –Approval Not Required	Annah Stacpoole	AAO	GMO
4.0	23 June 2023	Authorisation to Issue	Peter Dummett	CEO	CEO
4.1	24 June 2024	Updated contacts and annual review	David Power	GMO	N/A
4.2	24 June 2025	Updated contacts and re branding to match new ICIMP	Carleen Mitchell/Kylie Williams		

APPENDIX D – DP EMT / CMT EMERGENCY CONTACT DIRECTORY

CATEGORY	COMPANY	NAME	POSITION	MOBILE	OFFICE	EMAIL
Aviation	Air Services Australia Canberra				1300 301 120 02 6268 5555 Int'l - 1800 801 960	Servicedesk.airways@airservicesaustralia.com
Aviation	Airborne Solutions			0429 775 555		info@airbornesolutions.com.au
Aviation	North Australian Helicopters	Kevin Holden	Chief Pilot	0428 432 666	08 8978 9203	accounts.nah@bigpond.com admin@Northaustralianhelicopters.com.au
	Amateur Fishermens Association of the NT (AFANT)	David Ciaravolo	CEO	0415 471 600	08 8945 6455	research@afant.com.au office@afant.com.au ceo@afant.com.au
Fuel Provider	Ampol				1800 033 111	
DMSB	ASCO	Kylie Arnel John Cowan	DMSB Manager DWSB Manager	0418 533 048 0448 148 957	08 8985 9508 08 8922 9562	kylie.arnel@ascoworld.com john.cowan@ascoworld.com
Fuel Provider	AusFuel	Andrew Swart Paul Zerafa	Darwin Operations Manager General Manager	0448 886 939 0407 974 564	08 8984 0840 08 8935 1888	a.swart@directhaul.com.au p.zerafa@directhaul.com.au
Commonwealth Gov	AusSAR - Search & Rescue (also AMSA)	Joint Rescue Division	AMSA Connect phone number Aviation 24H phone number Maritime 24H Phone number		02 6279 5000 1800 815 257 1800 641 792	
Commonwealth Gov	Australian Maritime Safety Authority (AMSA)	Joint Rescue Coordination Centre	First Contact Head Office Switchboard Oil Spill Greg Witherall - Operations		1800 641 792 07 3110 6800 02 6279 5000 02 6230 6811	rccaus@amsa.gov.au greg.witherall@amsa.gov.au
ABF National	Department of Home Affairs		Switchboard National Security	AH -1300 484 987 24/7 manned	02 6264 1111 National Switchboard	security @homeaffairs.gov.au
ABF	Australian Border Force Marine Logistics Darwin		Marine Logisitics	0419 515 859 On Call mobile		marine.logistics@homeaffairs.gov.au
AEP	Australian Energy Producers (AEP)				02 6247 0960	contact@energyproducers.au

CATEGORY	COMPANY	NAME	POSITION	MOBILE	OFFICE	EMAIL
Commonwealth Gov	Australian Transport Safety Bureau (ATSB)		24/7 Aviation, Marine, Rail Accident/Incident Notifications		1800 011 034	atsbinfo@atsb.gov.au atsbasir@atsb.gov.au
Marine Service Provider	Auriga Marine	Cindy Holden Kim Head Vaughan Poynter Leilani Gosschalk	Operations Manager General Manager Vessell Manager Marine Administrator	0409 067 274 0427 190 364 0418 719 787 0447 889 493	08 8947 4960	Cindy.holden@auriga.com.au Kim.head@auriga.com.au Vaughan.paynter@auriga.com.au Laeilani.gosschalk@auriga.com.au
Misc	Baker Hughes	Jason Mackellar	Darwin Plant Manager	0447 933 224	08 8943 5603	Jason.mackellar@bakerhughes.com
Marina	Bayview Marina	John Ludbrook Louise Ludbrook	Bayview Manager and LockMaster	0477 661 130		marinamanager@bayviewmarina.com.au
Marine Service Provider	Bhagwan Marine	Luke Morand Callum Gambell Lee Fitch	NT Manager Marine Superintendent Marine Superintendent	0407 664 266 0499 939 080 0458 939 812	08 8982 0600	luke.morand@bhagwanmarine.com operationsdarwin@bhagwanmarine.com
BOM	Bureau of Meteorology (BOM)	Offices	Casuarina Alice Springs Gove Airport		08 8920 3800 08 8987 2477	weatherquestion@bom.gov.au
BOM	Bureau of Meteorology (BOM)	Telephone Weather	NT Services Darwin Temps & Weather Obs NT Tropical Cyclone Information NT Coastal & Land Weather Warnings		1300 659 210 1300 659 211 1300 659 214	rdnt@bom.gov.au
Emergency Services	Bushfires				08 8922 0844	BushfiresNT@nt.gov.au
Aviation	Civil Aviation Safety Authority (CASA)		Switchboard Confidential Hotline (For at risk report)		131 757 (option 5)	oar@casa.gov.au darwin.emergencies@casa.gov.au
Environmental Services	Cleanaway		Office number Emergency Spills Hotline		08 8935 1111 1800 774 557	
Environmental Services	Cleanaway Waste Solutions				08 8947 3388 131 339	darwin.scheduling@cleanaway.com.au

CATEGORY	COMPANY	NAME	POSITION	MOBILE	OFFICE	EMAIL
ADF	Coonawarra Tower (Navy)	Port Services North James Burkett	Duty Phone Wharf Manager	0408 625 370 0437 590 654		postservicesnorth@defence.gov.au
	Coroner's Office	Dave Gregory	On - Call	0417 875 624		nt.coroner@nt.gov.au
Commonwealth Gov	CSIRO				1300 363 400	csiroenquiries@csiro.au
Marina	Cullen Bay Marina Manager	Gadian Dixon Clay Fredericks Lockmaster on Duty	Estate Manager General Manager Lockmaster (Radio CH - VHF 11)	0409 885 891 0499 177 323 0419 421 363	08 8942 0400	estate.manager@cullenbaymarina.com.au manager@cullenbaymarina.com.au admin@cullenbaymarina.com.au
Local Gov	Darwin City Council	Andrew Thompson	Manager, Security and Emergency Planning	0474 014 519	08 8930 0300 Customer Service	emergency.management@darwin.nt.gov.au darwin@darwin.nt.gov.au
Commercial Divers	Darwin Dive Co.	Drew Pearce	Manager	0428 438 527		drew@darwindiveco.com info@darwindiveco.com
DMSB	Darwin Marine Supply Base (DMSB)	Kylie Arnel	DMSB Manager	0418 533 048	08 8985 9508	kylie.arnel@ascoworld.com
Darwin Port	Darwin Port	Peter Dummett	Chief Executive Officer	0401 117 056	08 8919 0880	peter.dummett@darwinport.com.au
Darwin Port	Darwin Port	David Power	General Manager Operations	0417 867 886	08 8919 0801	David.power@darwinport.com.au
Darwin Port	Darwin Port	Rhys Jones	General Manager, Strategy & Growth	0400 872 554	08 8919 0805	rhys.jones@darwinport.com.au
Darwin Port	Darwin Port	Sarah-Jane Archdale	Group Company Secretary & Chief Corporate Governance Officer	0436 014 587	08 8919 0823	sarahjane.archdale@darwinport.com.au
Darwin Port	Darwin Port	Peter Sedgwick	Senior Manager Marine Ops	0497 199 726	08 8919 0818	Peter.sedgwick@darwinport.com.au
Darwin Port	Darwin Port	Ryan Akers	Senior Manager Maintenance & Engineering	0408 270 919	08 8919 0830	ryan.akers@darwinport.com.au
Darwin Port	Darwin Port	Wayne Bodkin	Senior Manager, Landside Operations and security	0448 658 652	08 8919 0886	wayne.bodkin@darwinport.com.au
Darwin Port	Darwin Port	Security Gatehouse		0401 110 320	08 8919 0816	security@darwinport.com.au
Darwin Port	Darwin Port	Harbour Control	Duty Harbour Control Officer		08 8919 0821 08 8919 0822	harbourcontrol@darwinport.com.au
Darwin Port	Darwin Port	Landside Operations	Duty Landside Officer	0408 465 063	08 8919 0856	cargo@darwinport.com.au

CATEGORY	COMPANY	NAME	POSITION	MOBILE	OFFICE	EMAIL
Darwin Port	Darwin Port	Vacant	Senior Manager Operations			
Darwin Port	Darwin Port	Joel Kevan Promad Mishira	Manager, Maintenance & Wharf Services	0436 105 010 0401 117 064	08 8919 0837	joel.kevan@darwinport.com.au Promad.mishira@darwinport.com.au
Darwin Port	Darwin Port	Carleen Mitchell	Executive Assistant & Cruise Facilitation Coordinator	0430 548 743	08 8919 0881	carleen.mitchell@darwinport.com.au
Darwin Port	Darwin Port	David Cairns	Manager Port Logistics	0401 319 706	08 8919 0857	david.cairns@darwinport.com.au
Darwin Port	Darwin Port	Jeremy Wu	IT Service Deliver Manager	0401 117 050	08 8919 0810	jeremy.wu@darwinport.com.au
Darwin Port	Darwin Port	Kristy Bellas	Head of Technology and Systems	0438 415 189	08 8919 0808	kristy.bellas@darwinport.com.au
Medical	Darwin Private Hospital				08 8920 6011	
Recreation Marine	Darwin Sailing Club	Steven Green	General Manager		08 8981 1700	gm@dwnsail.com.au
Recreation Marine	Darwin Trailer Boat Club	Angela Zidda	General Manager		08 8981 6749	admin@dtbc.com.au
Marine Service Provider	Darwin Tug & Line	Peter West	General Manager Duty Phone on call	0417 886 048 0457 433 329		info@dtls.com.au bookings@dtls.com.au
NT Government	Darwin Waterfront	Aaron Dunn Ralph Dsouza	Acting Manager Parking and Security Chief Operations Officer - DWC	0409 706 602 0428 710 061	08 8999 5155	darwinwaterfront@nt.gov.au dwcoperations@nt.gov.au ralph.dsouza@nt.gov.au
Federal Government	Department of Agriculture, Fisheries and Forestry		DAFF – hotline Biosecurity – exotic plant pest hotline		1800 900 090 1800 084 881	
NT Government	Department of Agriculture and Fisheries	Brett Herbert	Manager Fish Watch Hotline Fisheries – compliance	0413 381 094	1800 891 136 08 8999 2126 08 8999 2372	aquaticbiosecurity@nt.gov.au
NT Government	Department of logistics and Infrastructure	Cindy McDonald	Executive Director Transport, Safety & Services Marine Safety	0488 936 480	08 8924 7598 08 8924 7100	cindy-lee.mcdonald@nt.gov.au

CATEGORY	COMPANY	NAME	POSITION	MOBILE	OFFICE	EMAIL
NT Government	Department of Mining and Energy	Louis Gomatos	Senior Director Petroleum Operations - Gas	0447 046 435 1300 935 250 A/H	08 8999 6030 08 8999 5396	louis.gomatos@nt.gov.au petroleumoperations@nt.gov.au
NT Government	Department of Lands Planning and Environment	Kathleen Davis	Mining Division Executive director of Mining	0437 715 276	08 8999 6528	Mineralinfo.dlpe@nt.gov.au
Recreation Marine	Dinah Beach Cruising Yacht Club	Wendy McCallum	General Manager	0499 346 242	08 8981 7816	manager@dbcya.com.au
Marine Service Provider	DOF Subsea	Carole Cartledge Khann Sinclair	Base Manager Regional HSEQ Manager	0437 158 614 0414 498 207	08 9278 8779 08 9278 7800	carole.cartledge@dof.com khann.sinclair@dof.com
NT Government	Emergency Services (Police/Fire/ Ambulance)		Emergency Non-Emergency		000 131 444 (112 from mobile)	
Marina	Frances Bay Marina (Duck Pond) Lock	Angela Printz Greg Hocking Thalia Puckett	Business Manager Wharf Supervisor Smallship Scheduler	0438 924 274 0428 207 612	8924 7509 8922 0617	angela.prinz@nt.gov.au gregory.hocking@nt.gov.au smallships.scheduler@nt.gov.au
Marina	Frances Bay Mooring Basin Dept Lands Planning and Environment	Greg Hocking	Lock Operations A/H	0427 910 220 A/hours		FBMB.DLPE@nt.gov.au
Marine Service Provider	Hall Contracting	Mark McCurdy	General Manager	0417 240 407		mail@hallcontracting.com.au markmccurdy@hallcontracting.com.au
NT Government	Harbourmaster	Anil Chadha Jon Abbey	Regional Harbourmaster Deputy Regional Harbourmaster	0428 181 480 0417 549 023	08 8999 3867 08 8924 7101	anil.chadha@nt.gov.au jon.abbey@nt.gov.au
LNG Terminal	INPEX	Hajime Nakama	Terminal Ops Coordinator LNG1 Panel – LNG Loading (24Hr) LNG2 Panel -LPG Loading (24Hr) Utilities Panel – Condensate Loading (24Hr)	0458 688 825	8983 8110 8983 8050/8983 8051 8983 8070/8983 8071 8983 8060	hajime.nakama@inpex.com.au
Aviation	Nautilus Aviation				08 8945 0944	slightf@nautilusavaiation.com.au
Transport & Logistics	Linx	Eddie Wilson Phil Brewster	Darwin Stevedore Manager Senior Shift Manager	0429 159 464 0418 898 164		e.wilson@linxcc.com.au p.brewster@linxcc.com.au

CATEGORY	COMPANY	NAME	POSITION	MOBILE	OFFICE	EMAIL
						darwinops@linxcc.com.au
Shipping Agent	Monson Offshore	Dion Robinson	Senior Shipping Operations	0448 850 006	08 8947 2570	darwin@monsonoffshore.com.au
NT Government	NT Emergency Services		Duty Officer	0408 896 245	08 8922 3630	territorydutyofficer.ntes@pfes.nt.gov.au
Environmental Services	NT EPA	Nicole Civitarese	Marine Pollution hotline	1800 064 567	08 8924 4218 08 8924 4553	pollution@nt.gov.au
Emergency Services	NT Fire & Rescue	Mark Spain	Headquarters Chief Fire Officer	08 8999 3473 24/7	08 8946 4133 08 8946 4105	mark.spain@pfes.nt.gov.au
Emergency Services	NT Police				08 8999 0800	
Volunteer group	Wildlife Volunteers		WildCare Rescue 7am – 9pm	0408 885 341	08 8988 6121	wildcaredarwin@gmail.com
Engineering	Pearl Marine Engineering	Cameron Paice Nico Noppen	Operations Manager General Manager	0447 792 962 0428 948 896	08 8901 2000	c.paice@pearlmarineengineering.com.au n.noppen@pearlmarineengineering.com.au admin@pearlmarineengineering.com.au
Poisons Information	Poisons Information Centre				13 11 26	
NT Government	Pollution Hotline		(24x7)		1800 064 567	pollution.epa@nt.gov.au
Transport & Logistics	Qube	Scott Sims	Operations Manager	0401 542 089	08 8922 2300	scott.sims@qube.com.au
Transport & Logistics	Rentco	Jarrod Dennis	Branch Manager	0427 158 053	08 8947 4187	jarrod.dennis@rentco.com.au darwinadmin@rentco.com.au
Medical	Royal Darwin Hospital				08 8922 8888	
LNG Terminal	Santos	Neel Sud	Marine Superintendent	0409 029 173		neel.sud@santos.com
Marine Service Provider	Sealink NT (Mandorah Ferry)	Murray Barker?? Or Henry Masel	Operations Manager	0429 105 301	1300 130 679	murray.barker@sealink.com.au
Marine Service Provider	Seaswift	Todd Pemble Keith De Saram	Operations Manager Operations Support	0409 328 131 0456 857 157	08 8935 2414	toddp@seaswift.com.au keithd@seaswift.com.au
Marine Service Provider	Serco		Operations Manager			dmms.coonawarra@serco-ap.com

CATEGORY	COMPANY	NAME	POSITION	MOBILE	OFFICE	EMAIL
Marine Service Provider	Shorelands Shorebarge	Daniel Field Richard Chandler	Operations Manager Barge Manager	0419 036 425 0477 878 128	08 8932 3344	cranes@shorelands.com.au supervisor@shorebarge.com.au
Emergency Services	St Johns Ambulance		General Enquiries		08 8922 6200	
Marine Service Provider	Svitzer Tugs	Ben Ross Tug Control	Port Manager 24/7	0408 822 728	1800 451 129	audar.info@svitzer.com
Marina	Tipperary Waters Marina	Robbie Standaloft	Lockmaster	0407 075 077		lockmaster@tpperarywatersmarina.com
Transport & Logistics	Toll Remote Logistics	Melanie Brady	Port Manager On-Call contact	0428 094 298 0429 380 850		melanie.brady@tollgroup.com
Environmental Services	Veolia Environmental	Angela Maisey	Commercials	0409 328 052	08 8947 8947	angela.maisey@veolia.com nt.service@veolia.com
Misc	Vopak	Shaun Stewart Matthew Jeffree	Operations Manager Darwin Safety Co-Ordinator	0419 180 057 0437 839 789	08 8999 9121 08 8999 9104	shaun.stewart@vopak.com matthew.jeffree@vopak.com
Environmental Services	VTG	Yaz Cooper	Operations Supervisor	0456 224 117	08 7909 8888	admin@vtgwaste.com.au
Emergency Services	Water Police				131 444	
NT Government	WorkSafe	Workplace Health & Safety	For all accident notification, general enquiries & complaints		1800 019 115	ntworksafe@nt.gov.au