

RESPONSIBILITIES INCLUDE

- Management of Intelligence activities across the response, ensuring effective application of the Intelligence Cycle
- Provision of coordination, direction, support, and/or mentoring to regional level Intelligence leads
- Production and dissemination of intelligence products/outputs that support decision makers and key clients
- Provision of expert Intelligence advice to the Controller and other functions
- Ensure the Controller and wider IMT are informed of the Intelligence aspects of the response
- Ensure intelligence collection is informed by shared situational awareness and awareness of decisions for and from Cabinet and the National Security System (NSS)
- Ensure knowledge of the machinery of government and political dynamics are applied effectively to the Intelligence Cycle and collection process
- Ensure accuracy and usability of response information (verify and validate, correct format of data)
- Management and storage of documentation, including sensitive information
- Ensure the Intelligence Cycle and associated outputs and outcomes are culturally inclusive and reflect a Te Ao Māori worldview

KEY RELATIONSHIPS

- Controller (and deputy), Response Manager
- The IMT and other functions, particularly Planning and Iwi/Māori Representation
- Intelligence functions at other NCCs and at regional and all-of-government level (if applicable)
- Internal and external stakeholders, partners, and support agencies/organisations
- Iwi rūnanga and liaison staff

KEY OUTPUTS

- Situation and Intelligence Reports (e.g. profiles, intelligence summaries, implications of key decision)
- Intelligence visualisation and geospatial products such as maps, charts, and dashboards to support understanding and dissemination
- Information Collection Plan
- Forecasts (scenarios) and identification of emerging risks
- Intelligence Status Reports
- Input into the Action Plan

CONSIDERATIONS

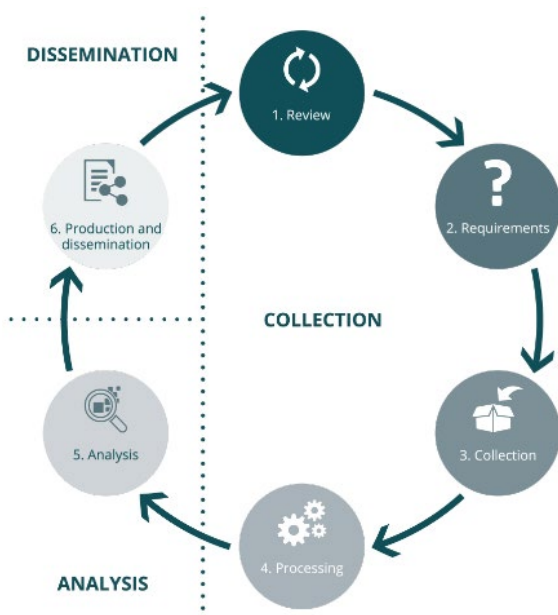
- **The intelligence audience:** Ensure intelligence products support the immediate, ongoing, and future needs of decision makers, key clients, other functions, agencies, and response levels
- The limitations of the information (time, accuracy, level of confidence, reliability of source)
- Information security requirements under Privacy Act and Official Information Act
- Analysis of impacts from decision making, shifting priorities, or emerging risks
- Consistent and systematic collection of data; ensuring formatting and curation allows for escalation of the data
- Collection Plan priorities - collection and distribution cycles
- Diversity of thought and perspectives during analysis, use of analytical tools and techniques
- Political, Governance, and security context and requirements
- How unified control may affect intelligence gathering and sharing
- Applying a holistic and integrated response and recovery approach across the recovery environments

INTELLIGENCE SUB-FUNCTIONS

- Collection
- Analysis
- Dissemination

INITIAL TASKS

- Obtain a briefing from the Controller to gain situational awareness / obtain Controller's intent
- Establish Intelligence function; appoint, brief, and task staff; ensure staff have had an induction (including a Health and Safety induction)
- Engage across functions to gain initial understanding
- Assess the incident, identify critical intelligence gaps and risks; determine immediate/critical intelligence requirements
- Participate in setting response objectives
- Contribute to development of (initial) Action Plan
- Develop a schedule for producing outputs that includes due dates/times for Status Reports from other functions and when drafts need to be ready and finalised
- Ensure workstream priorities for Intelligence are aligned with the Action Plan
- Set up logs (as required) to record decisions and actions
- Set up Information Collection Plan and processes (and cycle) for collecting information
- Log, prioritise, and process / action requests for information
- Determine internal and external stakeholders and political and stakeholder context; establish communication channels



ONGOING TASKS

- Maintain the integrity of the Intelligence Cycle
- Provide intelligence reports, briefings, situation updates, and visual information to meet decision maker and key client needs; continually review requirements and needs
- Contribute to the planning process and provide expert Intelligence advice to the response
- Manage, maintain, and monitor Information Collection Plans, logs, and a reference/repository to enable auditability
- Monitor progress of Intelligence tasks, requests for information, and collection activities; manage expectations and demands
- Forecast incident progression against the collected response information and identify emerging risks
- Contribute to the risks and issues register(s); identify commonalities and share information where relevant
- Conduct ongoing intelligence scanning to understand changes in the operating environment
- Ensure the Controller and wider IMT are informed of the Intelligence process and understand the collection and dissemination cycles
- Support the Controller to advise Governance/Policy/Cabinet
- Build strong relationships with internal and external stakeholders, including other Intelligence functions at regional, national, and all-of-government level (if applicable)
- Contribute strategic data/intelligence to Governance reporting
- Attend IMT meetings, National Security System (NSS), other national intelligence forums, and convene national Intelligence Manager teleconferences
- Maintain and communicate handover documents
- Manage demobilisation for Intelligence

DEMobilISATION

Refer to *Appendix F Demobilisation* in page 96 of the 3rd edition of the CIMS Manual for more information.