United Nations
Interregional Crime and Justice
Research Institute

TOOLKIT

on effective CBRN planning and response for policymakers and CBRN managers

TOOLKIT

on effective CBRN planning and response for policymakers and CBRN managers

DISCLAIMER

The opinions, findings, conclusions, and recommendations expressed in this publication are solely those of the authors and do not necessarily reflect the views or positions of the United Nations, UNICRI, or any other national, regional, or international entity involved.

The content of this publication may be quoted or reproduced, provided the source is acknowledged. Neither UNICRI nor the authors bear responsibility for any use of the information contained herein.

The designations used and the presentation of material in this publication do not imply any opinion on the part of the United Nations Secretariat or UNICRI regarding the legal status of any country, territory, city, or area, or its authorities, nor regarding the delimitation of its frontiers or boundaries. Mention of specific institutions, companies, or manufacturers' products does not constitute endorsement or recommendation by the United Nations Secretariat or UNICRI over others of a similar nature.

This publication was made possible with the financial support of the Bureau of International Security and Nonproliferation, U.S. Department of State.

ACKNOWLEDGMENT

This Toolkit has been prepared by the following UNICRI team: Mr. Francesco Marelli, Head of the CBRN Risk Mitigation and Security Governance Unit, Ms. Alice Rena, Programme Officer, Ms. Mariana Diaz Garcia, Associate Programme Officer, and Ms. Gabriela Coman-Enescu, Consultant.

UNICRI would like to express its appreciation to Mr. Stephane Huriet, Mr. Jerry Davydov, Ms. Heba Mariey, Ms. Rana Baydoun for their support. Antonella Bologna, UNICRI, for the expert graphic layout and design of this document.

UNICRI extend sincere gratitude to the Organization for the Prohibition of Chemical Weapons (OPCW) and the World Health Organization (WHO) for their support and expertise during the development of the Toolkit.

UNICRI extends its sincere appreciation to CBRN experts, Benjamín Ruiz Loyola, Jorge Mier y Terán Suárez, for generously sharing their expertise.

For more information:

UNICRI

Viale Maestri del Lavoro, 10

10127 Turin, Italy

Website: www.unicri.org

E-mail: unicri.publicinfo@un.org

FOREWORD

CBRN incidents, with their unpredictable and potentially catastrophic impacts, demand more than conventional emergency response mechanisms. Addressing these challenges requires advanced tools and frameworks that empower strategic-level decision-makers to navigate uncertainties and mitigate evolving risks. In this context, the *Toolkit on effective CBRN planning and response for policymakers and CBRN managers* emerges as an essential resource, offering a holistic and proactive approach rooted in advanced preparedness, strategic foresight, and collaborative action.

This comprehensive guide results from an extensive collaborative effort that brings together diverse expertise, rigorous research, field missions, and lessons learned from past incidents. Its development involved contributions from regional governments, international organizations such as WHO, IAEA, and OPCW, and local stakeholders across Southeast Asia and East Central Africa. Workshops held in Manila and Nairobi provided invaluable insights from practitioners in varied contexts, ensuring that the Toolkit addresses critical preparedness gaps and reflects the realities of managing CBRN risks on the ground.

What distinguishes this Toolkit is its recognition that effective CBRN management is not confined to rigid protocols but instead relies on the creation of dynamic, adaptive systems capable of responding to emerging and unpredictable challenges. Its two-part structure – first focusing on planning and then on response actions – underscores the critical importance of preparation as a foundation for effective crisis management. Successful CBRN management begins long before an incident occurs, involving strategic planning, training, and the establishment of governance frameworks that enable rapid and coordinated responses.

For policymakers, emergency managers, and CBRN professionals, this Toolkit serves as a strategic companion, offering actionable guidance while simplifying complex processes. It stands as a testament to the necessity of collective preparedness in addressing risks that transcend borders.

This Toolkit is more than a reference document; it is a call to action for leaders at all levels to collaborate toward a safer, more secure future. It is with great pride and confidence that I commend this document to you, trusting it will serve as a valuable resource in strengthening CBRN preparedness and response.

This initiative would not have been possible without the generous support and funding of the Bureau of International Security and Nonproliferation, Department of State of the United States of America. We extend our sincere gratitude for their invaluable contribution to this initiative.

Leif Villadsen
UNICRI Acting Director

TABLE OF CONTENTS

LIST OF ACRONYMS

AI:	Artificial intelligence
BWC:	Biological Weapons Convention
CBRN:	Chemical, Biological, Radiological and Nuclear
CDC:	Centre for Disease Prevention and Control
COVID-19:	Coronavirus disease of 2019
CWC:	Chemical Weapons Convention
ECDC:	European Centre for Disease Prevention and Control
EU CBRN CoE:	European Union CBRN Centres of Excellence
HazMat:	Hazardous materials
IAEA:	International Atomic Energy Agency
NGO:	Non-governmental organization
OSINT:	Open-source intelligence
OPCW:	Organisation for the Prohibition of Chemical Weapons
SOP:	Standard operating procedure
PPE:	Personal Protective Equipment
UAV:	Unmanned aerial vehicle
UCS:	Unified Command Structure
UNICRI:	United Nations Interregional Crime and Justice Research Institute
UNODA ISU:	Implementation Support Unit (ISU) for the Biological Weapons Convention (BWC) within the United Nations Office for Disarmament Affairs
WCO:	World Customs Organization
WHO:	World Health Organization
WMD:	Weapons of Mass Destruction

Introduction

Responding to chemical, biological, radiological, and nuclear (CBRN) incidents presents significant challenges due to their immediate impact, potentially far-reaching effects, and long-term consequences. These incidents may lead to public health emergencies, social disruption, psychological trauma, environmental degradation, and substantial economic losses. Furthermore, CBRN events frequently compromise essential services, critical infrastructure, and trade, thereby instilling fear and eroding trust within affected communities.

To effectively mitigate CBRN risks, it is crucial to develop and implement a comprehensive strategy that encompasses prevention, detection, planning, response, and recovery. This strategy should adopt a multidimensional approach, integrating risk assessment, policy development, resource allocation, technological advancements, specialized expertise, and coordinated efforts across relevant agencies. A robust legal framework is also essential, providing clear laws, policies, and procedures that define roles and responsibilities, authorize emergency actions, and justify the use of emergency powers to enable a timely and effective response.

The *Toolkit on Effective CBRN Planning and Response for Policymakers and CBRN Managers* has been developed to support efforts in strengthening planning and response capacities. It offers practical guidance for strategic-level decision-makers, including policymakers, emergency management officials, and CBRN managers tasked with planning and overseeing responses to CBRN incidents. The document promotes alignment with international best practices, thereby enhancing interoperability and cooperation at national, regional, and global levels.

The Toolkit is structured into two main sections. The first section focuses on CBRN planning,[1] while the second section addresses response. In both sections, complex processes are broken down into structured steps, outlining key actions, common challenges, and best practices—specifically designed to support strategic-level decision-making.

The **Planning Section** begins with risk and capability assessments, which are fundamental to the CBRN planning process. These assessments provide a critical foundation for identifying potential threats and vulnerabilities, while also evaluating the availability and adequacy of resources, expertise, and infrastructure necessary for an effective response. The insights gained from these assessments directly inform the development of CBRN response plans, ensuring that specific actions, procedures, and protocols are in place to address identified risks in a timely and coordinated manner.

Within this framework, resource management ensures the appropriate allocation of personnel, equipment, and financial support to implement response plans effectively.

CBRN training programmes and exercises are also key elements of the planning process, designed to prepare responders by simulating real-world scenarios, identifying potential weaknesses, and ensuring personnel are equipped to manage CBRN incidents. The review and evaluation phase assesses the effectiveness of response plans and identifies any gaps in resources, procedures, or training.

1 Since the Toolkit is designed for policymakers and CBRN managers, the term “CBRN planning” is used instead of “CBRN preparedness.” The Planning Section aims to guide the development of strategies, policies, and procedures to address potential CBRN threats, whereas “CBRN preparedness” focuses more on ensuring the readiness and capabilities necessary to effectively implement those plans during a CBRN incident.

Risk and capability assessments should be periodically updated, and response plans revised accordingly to incorporate new insights, emerging threats, or changes in available resources. This iterative process—encompassing assessment, planning, resource management, training, evaluation, and revision—ensures that CBRN planning remains dynamic and effective in addressing evolving threats and vulnerabilities.

The Planning Section also outlines key elements that should be incorporated into response plans, including the establishment of a Unified Command Structure, the development of public awareness and communication strategies for CBRN incidents, the clarification of emergency authorities and legal frameworks for declaring a state of emergency, the creation of mechanisms for international cooperation and assistance, and the implementation of a comprehensive CBRN training program.

Building on this foundation, the **Response Section** focuses on the effective execution of CBRN response plans, which are critical for managing CBRN incidents. It offers guidance on key actions, challenges, and best practices for establishing a Unified Command Structure, conducting CBRN situation assessments, mobilizing resources, maintaining effective communication with the public, and investigating the cause of the incident while collecting evidence for potential legal proceedings. Additionally, it outlines the necessary steps for declaring a state of emergency and requesting international assistance.

The Toolkit serves as both a practical framework and a reference document. As a framework, it provides a structured approach to proactive CBRN planning and response. Therefore, policymakers and CBRN managers can use it as a guide to develop and implement strategies and policies, and to coordinate the efforts of various agencies into a unified system, ensuring all aspects of CBRN management are aligned. As a reference document, the Toolkit supports the quick identification of potential gaps and priorities, and can be used to validate or adjust plans, actions, and tools.

The Toolkit concludes with a **Roadmap** that summarizes the key steps presented throughout the CBRN planning and response sections. Designed as a concise and practical tool, the Roadmap provides quick guidance for policymakers and responders in developing, implementing, and continuously improving CBRN strategies, fostering a coordinated and effective approach to managing potential CBRN incidents.

The development of the Toolkit was informed by three primary sources of information:

- Desk research: Extensive research was conducted, including an analysis of CBRN planning and response literature, lessons learned from past incidents, and the identification of gaps in existing planning and response frameworks at national, regional, and global levels.
- Field data collection: Targeted field missions were carried out in Southeast Asia and Eastern and Central Africa to gather insights from relevant agencies involved in CBRN response in key countries, including Ethiopia, Indonesia, Kenya, Lebanon, Malaysia, the Philippines, and Tanzania. A reference framework guided data collection on key topics such as resources, intelligence, communication, coordination, and international assistance.

- Regional workshops: Two regional workshops were organized to review and validate the Toolkit. The first was held in Manila, Philippines (17–19 October 2023), gathering over 30 participants from Cambodia, Indonesia, Malaysia, the Philippines, and Thailand, as well as representatives from the World Health Organization (WHO), academia, and NGOs. The second workshop took place in Nairobi, Kenya (22–24 April 2024), bringing together senior-level participants from Ethiopia, Kenya, Tanzania, and Uganda, alongside international organizations such as the Organisation for the Prohibition of Chemical Weapons (OPCW) and WHO, and local actors like the Kenyan Red Cross. Both workshops featured knowledge-sharing sessions, group exercises, and interactive discussions aimed at refining and validating the Toolkit. In addition, UNICRI conducted two national tabletop exercises in Indonesia (October 2024) and Seychelles (November 2024) to further test and validate the Toolkit's findings.

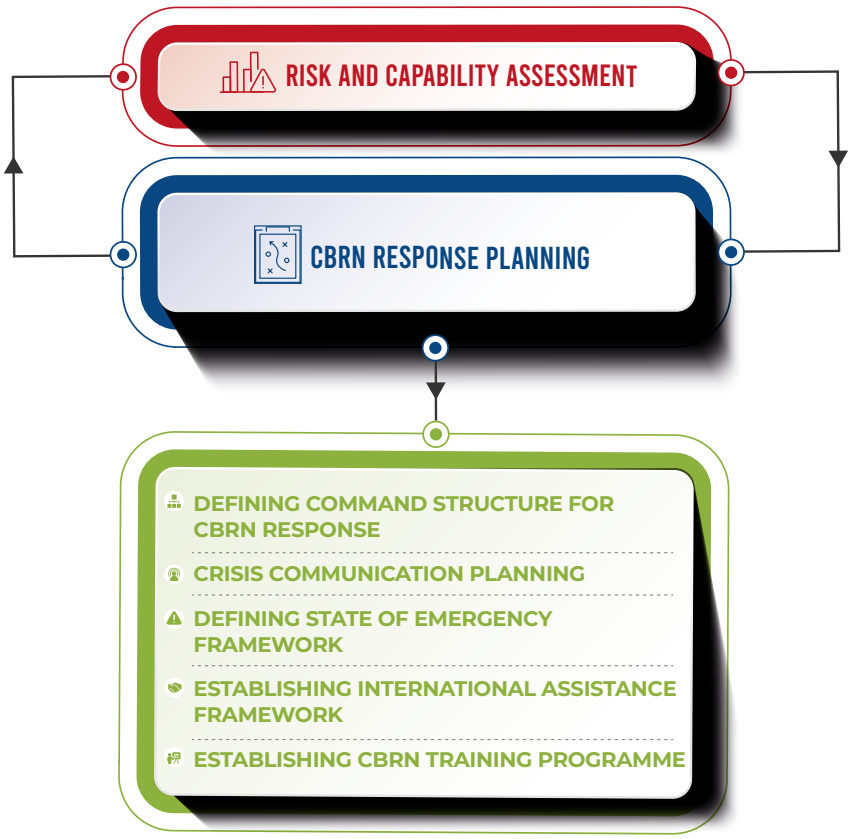
Section 1
Planning

Planning is a cornerstone of effective response to CBRN incidents, providing a structured and proactive approach to identifying risks, setting priorities, and developing the necessary capabilities to address a broad range of potential threats. Through comprehensive planning, policymakers, CBRN managers, and responders are equipped with the strategies, resources, and partnerships essential for mitigating the impact of CBRN incidents on public health, safety, and national security.

Central to the planning process are risk and capability assessments, which provide critical insight into CBRN threats and vulnerabilities, as well as the resources required for a timely and effective response. These assessments directly inform the development of tailored response plans, outlining specific actions, procedures, and protocols to address identified risks. The planning process also prioritizes the development of national capabilities, ensuring the appropriate allocation of vital resources such as trained personnel, equipment, medical supplies, and facilities. Regular reviews and evaluations are also integral to the planning process, ensuring that response capabilities remain aligned with national needs, priorities, and evolving threats. This ongoing evaluation ensures that response plans are consistent with both national and international standards, allowing for timely adjustments and continuous improvement of the overall preparedness framework.

This section provides an overview of these essential planning principles and includes dedicated subsections that focus on key elements that response plans should address. These subsections provide guidance on critical aspects such as establishing a Unified Command Structure, developing public awareness and communication strategies, clarifying emergency authorities and legal frameworks for declaring a state of emergency, and creating frameworks for international cooperation and assistance.

By integrating these elements into the planning process, a resilient and adaptive framework is established, ensuring a coordinated, swift response to CBRN incidents.



1. RISK ASSESSMENT

Risk assessment is one of the key elements of CBRN planning. By systematically identifying, analyzing, and prioritizing threats and vulnerabilities, the risk assessment ensures that planning efforts focus on the most credible and significant risks. It provides critical insights into the likelihood and impact of potential threats, enabling efficient resource allocation and proactive planning.

Risk assessment is also instrumental in developing effective CBRN response plans by identifying high-risk situations and locations, and outlining the actions required to address them. The assessment helps shape realistic plans that consider available resources while guiding training efforts to ensure personnel is adequately equipped to manage prioritized risks.

KEY ACTIONS

1) Threat identification

Threats include potential hazards, such as CBRN materials or hazardous substances, and the events or actors that could exploit, release, or cause their uncontrolled spread. These threats arise from three main sources: **intentional acts** like terrorism, industrial sabotage, or weaponization of hazardous materials; **accidental incidents** such as industrial spills, workplace accidents, transportation mishaps, or equipment failures; and **natural events** like earthquakes, extreme weather, or geological shifts that may damage containment systems or disperse dangerous substances.

Threat identification focuses on recognizing potential CBRN threats, their sources, areas of potential impact, and the events or mechanisms through which they could occur, all within the specific context of a country. Scenarios are often developed based on the country's current situation, historical data, past incidents, and expert analyses. Emerging threats, such as the malicious use of synthetic biology, unmanned aerial vehicles (UAVs), and artificial intelligence (AI), should also be considered to account for evolving risks.

Several mechanisms are employed in threat identification, including structured interviews, affinity grouping, risk source analysis, checklists, and scenario analysis, to collect relevant information. Characterizing these threats requires defining an appropriate scope, ensuring that it is neither too broad—making it difficult to develop actionable strategies—nor too narrow, which could lead to excessive detail that hinders effective prioritization. Data from intelligence reports, historical incidents, and expert judgment play a crucial role in characterizing threats, helping to assess both the likelihood of each threat and its potential consequences as part of the broader risk assessment process.

Example of CBRN threat identification

CHEMICAL THREAT

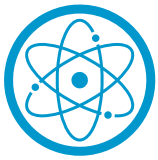
A deliberate release of chlorine gas in a populated urban area.

BIOLOGICAL THREAT

Deliberate release of anthrax spores in a major metropolitan area.

RADIOLOGICAL THREAT

Theft of radiological materials from medical or industrial facilities, or improper disposal leading to potential exposure or contamination.



NUCLEAR THREAT

Significant failure in the facility leading to a nuclear accident.

Key aspects to be considered when conducting threat identification include:

- Continuously monitor all available information sources, including news reports, scientific publications, intelligence briefings, social media, online forums and global CBRN incidents to stay informed about emerging threats, technological advancements, possible insider threats, trends in tactics and materials used by perpetrators, their capabilities, motivations, and potential targets, as well as industrial accidents, hazardous material spills, and natural threats.
- Implement a systematic process to identify and analyze potential CBRN threats, irrespective of source, and vulnerabilities within within the country.
- Collaboration with international intelligence agencies, international organizations, regional partners, and public health officials to leverage their expertise and gain insights into specific relevant threats.

2) Vulnerability assessment

While threat identification focuses on potential scenarios, analyzing the sources and nature of possible CBRN incidents, vulnerability assessment evaluates the weaknesses and susceptibilities within critical systems, infrastructure, and populations that could be exploited by these identified threats. Together, they form the foundation of a comprehensive risk assessment process. A combined register that aligns identified threats with corresponding vulnerabilities can be developed to facilitate the decision-making process, particularly by focusing resources on high-risk combinations of threats and vulnerabilities.

Assessing vulnerabilities involves identifying weak points in infrastructure, operational readiness, and human factors that could exacerbate the impact of a CBRN incident. Key aspects to consider, after defining the threat, include:

- **Identifying critical infrastructure and key populations:**
  - Map out high-risk locations such as industrial zones, hospitals, transportation hubs, and densely populated urban areas.
  - Assess vulnerable populations, including children, elderly individuals, and those with pre-existing health conditions and the relevance to consider them for the specific threat.
- **Evaluating structural and operational weaknesses:**
  - Examine the resilience of physical infrastructure (e.g., containment measures, security perimeters, air filtration systems).
  - Assess the ability of emergency response teams to access and operate within affected areas.
- **Assessing interdependence and cascading effects:**
  - Determine how failures in one sector (e.g., energy supply, transportation) could exacerbate vulnerabilities in another (e.g., hospital operations, communication networks).
  - Identify potential ripple effects that could hinder an effective response.
- **Analyzing environmental and geographic factors:**
  - Assess how weather conditions (e.g., wind patterns, rainfall) could impact on the spread of chemical or biological agents.
  - Consider the proximity of hazardous material storage sites to water bodies, residential areas, and food production facilities.

Examples of vulnerability assessments based on CBRN threats[2]

CHEMICAL THREAT

Deliberate release of chlorine gas in an urban area

- Population exposure: High-density residential areas, schools, and hospitals near the release site increase the risk of widespread casualties.
- Healthcare system readiness: Insufficient hospital capacity, lack of ventilators, and limited stockpiles of antidotes make treatment difficult.
- Emergency response: Limited access to trained hazardous materials (HAZMAT) teams, decontamination units, and protective equipment could hinder response efforts.
- Meteorological factors: Unpredictable wind conditions can spread the gas rapidly, increasing exposure.
- Public awareness and evacuation protocols: Inadequate public warning systems and evacuation plans may result in delayed protective actions.

BIOLOGICAL THREAT

Deliberate release of anthrax spores in a major metropolitan area

- Healthcare system exposure: Hospitals may have limited ability to diagnose and treat anthrax exposure due to inadequate laboratory capacity or lack of specialized medical personnel.
- Public health surveillance deficiencies: Weak disease detection and monitoring systems may delay outbreak identification and response.
- Supply chain fragility: Critical shortages of antibiotics, vaccines, and biohazard containment materials could hinder an effective medical response.
- Inefficient public communication: A lack of coordinated messaging could lead to misinformation, panic, and improper self-medication.

2 The vulnerability assessment is closely related to the broader capability assessment. This comparison is further explained in the next chapter. While vulnerability assessment focuses on weaknesses—such as inadequate infrastructure, lack of emergency response plans, or high population density—capability assessment measures the strengths and preparedness of a country's response mechanisms.

RADIOLOGICAL THREAT

Theft or improper disposal of radiological materials

- Security weaknesses: Inadequate physical security at radiological storage facilities may increase the risk of theft or loss of hazardous materials.
- Tracking and recovery gaps: Lack of comprehensive tracking systems could delay detection of missing materials.
- Public exposure risks: Improper disposal or accidental exposure could endanger communities living near radiological sites.
- Regulatory oversight issues: Weak enforcement of radiation safety protocols may allow for improper handling and transportation.

NUCLEAR THREAT

Significant failure at a nuclear facility leading to a radiation leak

- Geographical exposure risks: Proximity of key infrastructure (such as water supplies, agricultural land, and transportation networks) to the facility increases the potential for widespread contamination.
- Emergency preparedness gaps: Weak or outdated evacuation and shelter-in-place plans may leave populations vulnerable to radiation exposure.
- Limited response capacity: A shortage of radiation detection equipment, protective suits, and decontamination stations could slow response efforts.
- Long-term health risks: A lack of radiation exposure tracking and medical monitoring systems may hinder long-term health assessments and interventions.

An adequate vulnerability assessment ensures that response plans prioritize the most critical risks, aligning mitigation efforts with real-world constraints. Regular updates, scenario-based planning, and cross-sector coordination are key aspects to enhancing national preparedness and resilience against CBRN threats.

3) Impact assessment

Once threats and vulnerabilities are identified, the impact assessment evaluates the potential consequences of these threats in relation to the vulnerabilities. This involves analyzing the magnitude and scope of likely outcomes of an event (e.g., damage to infrastructure, restricted access, or compromised services), as well as the availability of backup resources. The process is deterministic, simulating the sequence of failures and their timing until a stable state is reached, thereby providing an understanding of how impacts unfold over time. The impact can be classified into five distinct levels, ranging from minimal (least severe) to catastrophic (most severe).

Impact rating scale (1-5)

IMPACT LEVEL	DESCRIPTION	SCORE
Minimal	Limited impact, easily recoverable	1
Minor	Short-term, manageable effects	2
Moderate	Significant impact, requiring resources to recover	3
Major	Severe impact, with widespread, long-lasting consequences	4
Catastrophic	Devastating, unrecoverable or irreversible impact	5

The impact level can be assessed in the following manner:

IMPACT LEVEL	DESCRIPTION	EXAMPLE: DELIBERATE RELEASE OF CHLORINE GAS IN A POPULATED URBAN AREA
Minimal (1)	No injuries, no environmental damage, minimal or no service disruption, negligible economic impact.	Small, contained chlorine gas leak with no injuries or environmental damage. Immediate containment prevents further consequences.
Minor (2)	Minor injuries, minimal environmental impact, brief service interruption, limited economic effects.	Minor exposure causing mild respiratory irritation to a small number of people. Minimal environmental impact with quick service restoration.
Moderate (3)	Serious injuries, localized environmental effects, temporary service disruption, significant local economic impact.	Serious injuries requiring hospitalization, localized environmental contamination, and temporary evacuation of the affected area.
Major (4)	Single or multiple fatalities, significant environmental damage, major service disruption, substantial economic impact.	Multiple fatalities, significant respiratory injuries, extensive environmental contamination, and disruption of critical services like transportation and healthcare in the area.
Catastrophic (5)	Multiple fatalities, severe environmental damage, permanent disruption of critical services, massive economic loss.	Widespread fatalities, irreversible environmental damage, permanent displacement of affected populations, and collapse of critical urban services such as water and power supply.

Explanation for the scenarios in the previous example

Minimal (1): Represents a scenario where a chlorine gas leak is quickly detected, contained, and mitigated before it spreads or causes harm.

Minor (2): Indicates short-term exposure with manageable health impacts and minimal disruption to public life.

Moderate (3): Demonstrates localized harm, including serious injuries and environmental contamination, requiring additional resources to recover and restore normalcy.

Major (4): Reflects a severe scenario with loss of life, extensive contamination, and prolonged service interruptions affecting large areas.

Catastrophic (5): Represents the worst-case scenario with devastating human, environmental, and economic consequences, leading to long-term or permanent disruption.

Key aspects to be considered when assessing the impact of a CBRN incident include:

- Evaluate the timeline of impacts to understand immediate, short-term, and long-term consequences.
- Align impact assessments with previously identified threats and vulnerabilities to provide a holistic risk profile.
- Use scenarios and simulations to test the interaction between threats, vulnerabilities, and potential impacts.
- Highlight gaps in resources or capabilities that could worsen the consequences of a CBRN event.

4) Likelihood assessment

Once the threats, vulnerabilities, and their potential impacts are assessed, the likelihood of these events occurring can be incorporated into the analysis to provide a comprehensive risk assessment. A likelihood assessment evaluates the probability of each threat materializing, regardless of its cause (whether intentional, accidental, or natural). This process leverages intelligence, historical data, and trends to estimate event frequency, while also considering emerging technologies, geographic factors, and human error to refine probabilities. The assessment aims to provide actionable insights that inform risk prioritization. Regular updates ensure that likelihood estimates remain aligned with evolving threats, vulnerabilities, and mitigation capabilities.

Likelihood rating scale

LIKELIHOOD LEVEL	DESCRIPTION	SCORE
Very low	Extremely unlikely to occur, with minimal historical precedent or evidence to support its potential occurrence.	1
Low	Unlikely to occur or occurs infrequently.	2
Medium	Possible to occur, with some historical precedent.	3
High	Likely to occur or has occurred previously.	4
Very high	Almost certain to occur, with substantial historical data and evidence supporting its potential occurrence. The chance of this event happening is very close to 100%.	5

The likelihood level can be assessed in the following manner:

LIKELIHOOD LEVEL	DESCRIPTION	EXAMPLE: DELIBERATE RELEASE OF CHLORINE GAS IN A POPULATED URBAN AREA
Very low (1)	Extremely unlikely to occur, with minimal historical precedent or evidence to support its occurrence.	No credible threats, effective security measures at facilities, and robust detection systems in place.
Low (2)	Unlikely to occur or occurs infrequently.	Chlorine is securely stored, but some minor vulnerabilities in facility access controls exist.
Medium (3)	Possible to occur, with some historical precedent.	Historical data shows occasional incidents of theft or unauthorized access to chlorine in nearby industrial facilities.
High (4)	Likely to occur or has occurred previously.	Intelligence reports indicate active interest by threat actors in acquiring chlorine, coupled with known security lapses.
Very high (5)	Almost certain to occur, with substantial historical data and evidence supporting its potential occurrence.	Recent credible threats, significant vulnerabilities in storage facilities, and active adversarial capabilities indicate imminent risk.

5) Risk calculation

IDENTIFICATION OF THREAT		EVALUATION OF THE RISK	
Threat	**Vulnerability**	**Impact**	**Likelihood**
What are the specific threats?	What critical weaknesses, systemic gaps, or susceptibilities exist that could be exploited or compromised by the identified threats?	What are the potential consequences if the threat materializes? (use CBRN Risk Matrix – see below).	What is the probability of occurrence of this threat? (use CBRN Risk Matrix – see below).

Risk calculation is the final step in the assessment process, integrating the previously identified threats, vulnerabilities, and the likelihood of each threat materializing to determine the overall level of risk. This process is tipically conducted using a risk matrix, a tool that evaluates both the likelihood of a threat occurring and the severity of its impact. By combining these two factors, the risk matrix provides a structured basis for decision-making, enabling the development of adequate response plans and the effective allocation of resources to address the most critical risks.

The calculation begins by defining clear scales for likelihood and impact, assigning numerical values to each level to enable quantitative analysis. A risk score is then derived by multiplying the likelihood rating by the impact rating. Higher scores indicate greater levels of risk, enabling decision-makers to prioritize the threats and vulnerabilities that pose the most significant challenges.

Risk calculation is not a static process but rather a dynamic one. Regular reviews are essential to account for changes in the threat landscape or vulnerabilities. The risk matrix should be updated as new information becomes available, ensuring its continued relevance and accuracy. Additionally, scenario planning can be conducted using the matrix to explore potential vulnerabilities and prepare response plans for high-risk scenarios.

Example of the risk matrix for various CBRN threats

THREAT	LIKELIHOOD (1–5)	IMPACT (1–5)	RISK SCORE (LIKELIHOOD X IMPACT)	DESCRIPTION
Chemical spill in a populated area	**4**	**4**	**16**	A spill of industrial chemicals (e.g., chlorine gas) due to equipment failure or sabotage in a densely populated urban area. Likely occurrence with major health and environmental impacts.
Theft of radiological material	**3**	**3**	**9**	Theft of radiological materials from poorly secured facilities. Moderate likelihood with localized health risks and potential public panic.
Biological attack with anthrax	**2**	**5**	**10**	Deliberate release of anthrax spores in a metropolitan area. Unlikely but catastrophic impact if it occurs, causing widespread fatalities and public health crises.
Improper disposal of radiological waste	**2**	**3**	**6**	Negligent disposal of radiological waste causing limited exposure in a rural area. Low likelihood and moderate localized impact.
Nuclear plant failure	**1**	**5**	**5**	Significant accident at a nuclear plant causing widespread radiation exposure. Very low likelihood due to stringent safety measures but catastrophic impact if it happens.

Considering the first example in the table above - chemical spill in a populated area, the following analysis was done:

- Likelihood (4): A chemical spill in a populated area has a high likelihood due to the common use of hazardous chemicals in industrial and urban areas. Equipment failures, accidents, or intentional acts such as sabotage contribute to this risk.
- Impact (4): The impact is major, involving potential fatalities, respiratory injuries, environmental contamination, and the disruption of critical services like healthcare and transportation.
- The risk score of 16 (4 likelihood × 4 impact) indicates a high priority threat, warranting significant resources for mitigation and response planning.

Risk assessment: challenges and good practices

CHALLENGES	GOOD PRACTICES
Failing to address comprehensive threats, including emerging risks such as UAVs and synthetic biology, can be challenging and may lead to critical gaps in preparedness and response efforts.	▸ Use **systematic approaches** such as structured interviews, affinity grouping, and scenario analysis to ensure broad threat identification. ▸ Establish a **dynamic threat monitoring process** that regularly reviews emerging technologies, geopolitical developments, and scientific advancements to keep CBRN risk assessments up to date.
Incomplete assessments can lead to the risk of **missing critical threat-vulnerability combinations.**	▸ Create a **combined threat-vulnerability register** to integrate and align threats with corresponding vulnerabilities for clarity. ▸ Regularly **update the threat-vulnerability register** through iterative assessments to capture emerging threats and evolving vulnerabilities, ensuring that the register remains relevant and comprehensive.
Assessments **are not realistic** and are grounded in theoretical or overly generalized scenarios rather than real challenges.	▸ Use **realistic scenarios,** such as past incidents, current threats, and country-specific hazards. ▸ Use **tools, methodologies and guidance documents** to realistically assess risks. For example, IAEA developed a Design Basis Threat (DBT) guidance to facilitate the development of physical protection on the basis of a State's evaluation of the threat (see IAEA, Development, Use and Maintenance of the Design Basis Threat, 2009).
Failing to **balance the scope in assessments,** particularly when they are overly broad or narrow, can complicate prioritization and resource allocation.	▸ Define **clear criteria for threat characterization,** balancing breadth and specificity to maintain actionable outcomes. ▸ Engage **interdisciplinary teams** to review and validate the scope of assessments, ensuring diverse perspectives contribute to a balanced and practical prioritization process.

CHALLENGES	GOOD PRACTICES
Not **estimating the likelihood accurately** due to limited historical data or evolving threats can reduce reliability of likelihood ratings.	▸ **Leverage** intelligence, historical data, expert judgment, and sensitivity analysis to refine likelihood assessments dynamically. ▸ Incorporate **scenario-based modeling** to simulate potential threat trajectories, allowing for more informed likelihood estimations despite limited historical data.
Incorrectly assessing long-term impacts, especially when cumulative and cascading effects are overlooked, can pose significant challenges such as difficulty to predict interactions accurately, data uncertainty, or difficulty in quantifying impacts (e.g., social and psychological impacts).	▸ **Simulate event sequences** and analyze cascading effects using scenario planning to assess impacts comprehensively. ▸ **Engage stakeholders** across sectors to identify potential long-term and cascading effects, leveraging diverse expertise to enhance the impact assessment.
Relying solely on numerical calculations without integrating qualitative data can lead to oversimplification and a misunderstanding of complex scenarios.	▸ **Combine quantitative data with qualitative** insights from subject matter experts for a holistic evaluation of risks. ▸ Use **case studies and historical examples** to complement data analysis, providing context and depth to the assessment of complex scenarios.
Since threats and vulnerabilities evolve rapidly, the dynamic threat landscape can render **static assessments outdated.**	▸ **Regularly update assessments** to reflect new intelligence, geopolitical shifts, technological advancements, and past lessons. ▸ Establish a **continuous monitoring system** to track emerging threats and vulnerabilities, ensuring assessments remain current and relevant.
Geographic and infrastructural differences create uneven vulnerabilities and variability in preparedness across regions.	▸ **Tailor assessments** to regional contexts, considering local population density, infrastructure, and socio-economic factors. ▸ Collaborate with **regional stakeholders** to gather localized data and insights, ensuring assessments address specific regional needs and challenges.
Resource constraints in risk mitigation make it challenging to address all high-priority risks effectively.	▸ Focus on **high-risk threat-vulnerability pairs** with cascading potential, optimizing resource allocation for maximum impact. ▸ Implement a **phased approach** to risk mitigation, prioritizing actions based on resource availability and potential effectiveness over time.

2. CAPABILITY ASSESSMENT IN CBRN RISK MANAGEMENT

A capability assessment evaluates a country's ability to respond to and recover from a CBRN incident. It examines the availability of trained personnel, specialized equipment, operational plans, and infrastructure required for an effective response. A comprehensive assessment helps identify gaps, ensuring a coordinated approach to mitigating CBRN risks. Key components of a capability assessment include:

- **Human resources and training**
  - Availability of first responders, including firefighters, hazmat teams, medical personnel, and law enforcement.
  - Level of preparedness through training programs, including joint exercises and emergency response drills.
  - Proficiency in handling specialized CBRN equipment and adherence to established response protocols.
- **Equipment and technology**
  - PPE for first responders and medical staff.
  - Detection devices for CBRN threats.
  - Decontamination facilities for affected individuals and environments.
  - Medical countermeasures, including antidotes, vaccines, and pharmaceuticals.
- **Healthcare system and emergency medical response**
  - Hospital preparedness for mass casualty events, including isolation rooms for infectious agents.
  - Coordination between public health authorities and emergency responders.
  - Stockpiling and distribution of CBRN-specific medications and equipment.
- **Operational plans and communication systems**
  - Clear SOPs aligned with national and internati onal response frameworks.
  - Public safety measures, including evacuation strategies and risk communication.
  - Inter-agency coordination mechanisms for rapid decision-making.
- **Infrastructure and logistics**
  - Availability of emergency shelters and transportation for affected populations.
  - Supply chain resilience to ensure continuous access to medical supplies and protective gear.
  - Critical infrastructure protection, including security at hazardous material storage sites.
- **Legal and regulatory framework**
  - Compliance with international treaties, including the Biological Weapons Convention (BWC), Chemical Weapons Convention (CWC), and International Atomic Energy Agency (IAEA) regulations.

- National laws governing CBRN preparedness, response, and recovery.

An adequate capability assessment ensures that vulnerabilities identified in risk assessments are addressed through improved preparedness and response mechanisms. By systematically evaluating human resources, technology, healthcare capacity, infrastructure, and legal frameworks, countries can enhance resilience to CBRN threats, ensuring a more effective and coordinated national response.

Bridging risk and capability assessments

Risk assessment, including threat identification and vulnerability assessment, determines the likelihood and potential impact of CBRN incidents. While **vulnerability assessment** focuses on weaknesses—such as inadequate infrastructure, lack of emergency response plans, or high population density—**capability assessment** measures the strengths and preparedness of a country's response mechanisms.

By linking the results of these assessments, decision-makers can:

- Prioritize resource allocation to address critical vulnerabilities.
- Improve response mechanisms where existing capabilities are insufficient.
- Enhance national resilience through targeted training, investment, and policy development.

A vulnerability assessment might reveal that a city's hospitals lack decontamination facilities for chemical exposure, while a capability assessment would determine whether the healthcare system has the expertise, protocols, and equipment to manage such cases effectively. For example:.

Vulnerability in the risk assessment focuses on weaknesses and susceptibilities in infrastructure, systems, and populations that could either be exploited by or exacerbate the impact of a CBRN event. It identifies **what is at risk and why.**

- **Chemical threat example:** A city's vulnerability to a chlorine gas attack may include high population density, lack of decontamination stations, and poor air circulation in subway systems.

Capability assessment evaluates the existing resources, capacities, and readiness of a system to respond to and mitigate a CBRN incident. It identifies **what is available** to reduce risks and how effective these resources are.

- **Chemical threat example:** The same city's capability assessment would examine the number of trained HAZMAT teams, stockpiles of antidotes, emergency evacuation plans, and the effectiveness of public warning systems.

A vulnerability assessment shows where the risks are, while a capability assessment determines whether the response mechanisms are adequate to address those risks. The results of both assessments guide decision-making for strengthening preparedness and response strategies

Capability assessment: challenges and good practices

CHALLENGES	GOOD PRACTICES
Lack of standardized methodology to conduct an assessment. Without a clear and consistent framework, assessments may vary in scope, quality, and reliability.	▸ Use **internationally recognized assessment frameworks** to ensure consistency. ▸ Develop **a step-by-step assessment procedure** to guide evaluators systematically.
Limited key stakeholder engagement can lead to gaps in assessment findings.	▸ Establish a **multi-agency working group** to ensure all relevant sectors contribute to the assessment. ▸ Conduct **stakeholder consultations and workshops** to validate findings and recommendations.
Inadequate data collection and analysis (e.g. poorly designed data collection materials, lack of access to classified information, and inconsistent data sources) can compromise the accuracy of the assessment.	▸ Develop **structured data collection tools** (e.g., surveys, checklists, and interview guides) to ensure comprehensive information gathering. ▸ Use **data analytics and scenario modeling** to enhance the accuracy of capability assessments.
Failure to integrate risk and capability assessments since assessments may focus too much on either risks or capabilities rather than linking them effectively.	▸ Use a **risk-informed capability assessment approach** that evaluates threats alongside available response capacities. ▸ Regularly **update assessments to** reflect evolving risks, technological advancements, and changes in national security priorities.
Lack of follow-up and implementation mechanisms since many assessments result in reports that are not acted upon due to unclear accountability or resource constraints.	▸ Develop an **actionable roadmap** with clear responsibilities, timelines, and budgetary considerations for capacity-building measures. ▸ Establish **a monitoring and evaluation (M&E) framework** to track progress on addressing identified gaps.
Overlooking cross-border cooperation, including failing to consider regional/international collaboration in assessments, can limit preparedness.	▸ Engage **regional organizations and international partners** to exchange best practices and harmonize capability assessments. ▸ Conduct **joint exercises and bilateral/ multilateral assessments** to address transnational threats.
Resource constraints and funding limitations since financial and logistical barriers can restrict the scope and effectiveness of capability assessments.	▸ Identify **alternative funding sources**, including international donors and public-private partnerships. ▸ Optimize resource allocation by prioritizing **high-impact capability gaps** and leveraging existing infrastructure.

3. CBRN RESPONSE PLANNING

CBRN planning is a critical component of national and community preparedness, ensuring an effective response to incidents that pose significant risks to public health, safety, and the environment. Effective CBRN planning encompasses the development of comprehensive response plans that outline clear roles and responsibilities, standard operating procedures, and coordination mechanisms among stakeholders. It emphasizes robust resource management, including the identification, allocation, and deployment of specialized equipment, trained personnel, and logistical support systems.

KEY ACTIONS

1) CBRN response plans development

CBRN response plans provide an overarching structure for managing CBRN incidents. They establish clear roles and responsibilities among stakeholders, enhance interagency coordination, and enable swift resource mobilization. By integrating risk assessments, fostering interagency collaboration, and ensuring resource readiness, these plans aim to mitigate the impacts of incidents, safeguard lives, and enhance resilience in the face of complex, high-consequence emergencies.

Critically, these plans define specific actions and protocols for each response phase, establishing clear decision-making pathways and operational procedures. This includes detailed guidance on initial threat assessment, containment strategies, decontamination procedures, medical response, evacuation protocols, and communication strategies. By pre-defining these actions, response teams can react more quickly and systematically, reducing uncertainty and minimizing potential escalation of the incident.

Additionally, CBRN response plans should be adaptable to evolving threats and incorporate measures for long-term recovery and resilience-building to restore normalcy after an event. Serving as a foundational tool, these plans align strategic objectives with tactical approaches to comprehensive emergency management.

Creating effective CBRN response plans is a critical first step in ensuring preparedness for such events.

Response plans should include the following:

- **Objective:** Clearly define the overarching goals of the response, such as protecting lives, mitigating harm and ensuring rapid recovery.
- **Roles and responsibilities:** Establish clear roles and responsibilities for stakeholders, including incident management structures, so that every individual involved in the response to an incident has a clear understanding of his/her role and how that role integrates with others.
- **Specific actions and SOPs:** Outline the specific actions to be taken during all critical stages of responding to a CBRN incident, contingencies, and timelines.
- **Resource requirements:** Define the resources needed to support effective response efforts, including personnel, equipment, facilities, and financial resources.
- **Unified Command Structure (UCS):** Ensure seamless coordination among multiple agencies and jurisdictions to achieve a cohesive and effective response.

Key considerations for the development of response plans include:

- **Alignment** across various plans to ensure that the plans share common goals (e.g. minimizing casualties, ensuring rapid response, etc.) and there are no conflicting procedures, especially when plans address overlapping responsibilities.
- **Standardized terminology** to reduce confusion.
- Promote **scalability and flexibility,** ensuring that aligned plans can be scaled to address incidents of varying magnitudes, from localized spills to large-scale attacks.
- Promote **interoperability,** ensuring that response plans can adapt to joint operations with other jurisdictions, organizations, or international partners.
- Facilitate **legal and regulatory compliance,** ensuring that the plans comply with national and international laws governing CBRN incidents. This includes adherence to domestic regulations, international treaties and conventions (such as the Chemical Weapons Convention or the Biological Weapons Convention), and human rights standards and obligations.
- Ensure **continuity of operations (COOP)** to maintain essential functions and services in organizations, including emergency responders, healthcare providers, and critical infrastructure operators. This includes the identification of essential functions and critical operations, the designation of backup locations to establish redundant communication and IT systems to support uninterrupted operations, and the development of protocols for delegating responsibilities to other personnel or facilities when primary assets are unavailable.
- Ensure **continuity of government (COG)** during a CBRN incident including sustained functioning of governmental leadership and decision-making processes. This includes the establishment of clear lines of succession for leadership at all levels

of government to avoid decision-making gaps, the safeguard essential documents and data to support decision-making and recovery efforts, and the implementation of robust and redundant communication systems for government leaders to ensure uninterrupted coordination.

The following list privides examples of CBRN response plans that can be developed. The specific type, content, and structure of CBRN response plans may vary depending on the national or regional context, the identified CBRN threats, and the available resources and capabilities.

General Plans – Focus on overall frameworks, geographic areas, and specific response capabilities.

- **National CBRN response plan:** Outlines the overall framework for responding to CBRN incidents at a national level. Addresses all types of CBRN threats and includes provisions for preparedness, response, recovery, and mitigation.
- **Regional CBRN response plan:** Covers specific geographic areas with shared vulnerabilities or threats.
- **Urban CBRN response plan:** Focuses on response capabilities within metropolitan areas.

Agent-specific plans – Focus on the unique characteristics of different CBRN agents or materials.

- **Chemical incident response plan:** Addresses the specific hazards posed by various chemical agents.
- **Biological incident response plan:** Outlines response actions for different types of biological agents.
- **Radiological incident response plan:** Covers procedures for handling radioactive materials and contamination.
- **Nuclear incident response plan:** Addresses the unique challenges of nuclear accidents or attacks.

Incident-based plans – Focus on specific scenarios or locations.

- **Public gathering plan:** Outlines the response to a CBRN incident at a large public event, such as a concert, sporting event, or festival.
- **Transportation plan:** Addresses CBRN incidents involving transportation systems, such as airports, train stations, or ports.
- **Infrastructure plan:** Focuses on the response to CBRN incidents at critical infrastructure, such as power plants, water treatment facilities, or chemical facilities.
- **Workplace plan:** Outlines the response to CBRN incidents in workplaces, such as factories, offices, or schools.
- **Community plan:** Addresses the response to CBRN incidents at the community level, including evacuation procedures, public health measures, and social support services.

Functional plans – Address specific aspects of CBRN response.

- **Incident response plan:** Outlines the immediate actions, roles, and responsibilities for responding to a CBRN incident, including detection, notification, evacuation, decontamination, and initial treatment.
- **Operations plan:** Details the operational procedures and resource deployment strategies for managing the various phases of a CBRN incident, such as containment, mitigation, and recovery.
- **Medical response plan:** Outlines protocols for medical treatment, triage, and patient management.
- **Communication plan:** Details communication strategies for informing the public during a CBRN event.
- **Decontamination plan:** Provides guidance on cleaning up contaminated areas and personnel.
- **Transportation plan:** Addresses the logistics of moving people, equipment, and hazardous materials.
- **Environmental response plan:** Addresses the monitoring, decontamination, and remediation of affected environments, such as air, water, and soil.
- **Command and control plan:** Specifies that the CBRN response would operate under a Unified Command Structure to ensure effective coordination among multiple agencies and will be activated immediately upon confirmation of a CBRN incident. Defines organizational structure and decision-making processes to ensure a rapid and cohesive response when a CBRN incident occurs.
- **CBRN situation assessment process plan:** Defines the purpose and scope of CBRN situation assessment, roles and responsibilities of the multi-agency assessment group; activation protocols; data collection methodologies and sources; analysis and interpretation; reporting structures and timelines; integration with decision-making processes; continuous reassessment and updating protocols; training and exercise requirements for assessment team members.
- **Continuity of operations plan:** Focuses on ensuring the continued performance of essential government functions during and after a crisis. It involves maintaining critical operations, preserving records, and restoring services, and FEMA's Continuity Guidance Circular establishes a unified framework for continuity planning and implementation nationwide.
- **Continuity of government plan:** Focuses on the preservation of the government itself and includes plans for leadership succession, emergency decision-making, and maintaining constitutional government.
- **Demobilization plan:** Addresses in either a standalone plan or as a component of a broader CBRN response plan (general or event-specific response plans). The best approach depends on specific needs and resources. In many cases, a combination of both approaches may be most effective, with a detailed demobilization plan integrated into a broader CBRN response plan.

- **Recovery plan:** Outlines strategies for restoring essential services, rebuilding infrastructure, and supporting affected communities following a CBRN incident. Addresses public health and safety, environmental remediation; economic recovery, infrastructure repair, building the capacity of communities to withstand future crises, cleaning up contaminated areas and restoring ecosystems.
- **Waste management plan:** Details actions to be taken to despose of contaminated materials in a safe and secure manner, ensuring the safety of the public, environment, and the economy.

2) Resource management

The next step in planning is to ensure the availability and effective allocation of resources, guided by the findings of the risk assessment and aligned with the specific needs identified and detailed in the response plans.

Resource management includes aspects such as:

Resource identification, in particular the identification of:

- **Personnel:** Individuals with the appropriate range of knowledge, skills, behavioral traits, physical fitness, and values to effectively respond to CBRN incidents.
- **Equipment and supplies:** Essential items such as Personal Protective Equipment (PPE) for responders, detection and identification devices (e.g., chemical sensors, radiation monitors), decontamination equipment and supplies (e.g., neutralizing agents, cleaning materials, specialized protective gear), and medical countermeasures (e.g., antidotes, vaccines, antibiotics, potassium iodide tablets).
- **Facilities:** Designated locations for the Unified Command Structure, temporary medical facilities, decontamination stations, safe shelters, or evacuation centers.

Resources prioritization. This involves prioritizing resources for high-risk areas and critical capabilities. For example:

- **High-risk areas** (receive most resources):
  - Focus on areas with highest threat likelihood and potential impact
  - Prioritize critical infrastructure and densely populated regions
- **Medium-risk areas** (receive a moderate level of resources):
  - Address moderate-threat scenarios and vulnerabilities
  - Support preparedness in areas adjacent to high-risk zones
- **Low-risk areas** (receive a smaller portion of resources):
  - Maintain basic preparedness capabilities
  - Enable surge capacity and support functions

Stockpiling and distribution, including:

- **Strategic storage:** Maintain reserves of essential supplies at strategic locations for rapid access during emergencies.
- **Supply chain management:** Establish reliable supply chains for replenishment during prolonged responses.
- **Distribution strategies:** Ensure rapid deployment of resources.

Maintenance and readiness of equipment, including:

- **Equipment maintenance:** Conduct regular inspections and service of equipment to ensure operational readiness (e.g., calibration of sensors, replacement of expired medical stock).
- **Inventory management:** Maintain accurate and centralized records of resource availability and usage. Utilize inventory tracking systems for real-time updates.

Multi-agency resource coordination, including:

- **Resource sharing agreements:** Establish agreements between local, national, and international agencies to ensure an effective sharing of resources during large-scale incidents. These agreements should also include private-sector entities, such as hospitals, pharmaceutical companies, and transport providers.
- **Mutual aid agreements:** Collaborate with neighboring countries and international organizations for shared access to equipment, personnel, and facilities during emergencies.

Allocation of financial resources. To support necessary activities and investments, it is recommended that long-term financial plans are developed to ensure the sustainability of CBRN preparedness and response efforts, including:

- **Budget allocation:** Allocate sufficient funding specifically for CBRN planning, training, and response activities to ensure effective operational readiness.
- **Diversified funding strategies:** Explore multiple funding sources, such as government budgets, international aid, and private donations, to enhance financial resilience.
- **Emergency funding mechanisms:** Establish mechanisms for accessing emergency funds to facilitate rapid response in the event of a CBRN incident.
- **Cost-benefit analysis for major investments:** Conduct regular reviews of CBRN investments to ensure value and effectiveness. These analyses should assess procurement strategies in terms of threat mitigation, operational efficiency, and optimal resource use.

Consolidated interagency database of CBRN resources:

It is crucial to develop and maintain a comprehensive interagency database that collects information on available resources, including personnel, equipment, supplies and facilities. Such a database can be vital during a CBRN incident, particularly when CBRN decision-makers at strategic-level need to quickly assess CBRN capabilities across different agencies and jurisdictions (see Chapter 3 Allocation and mobilization of strategic resources of the Response Section).

Critical infrastructure management: This plays a vital role in maintaining societal functions and ensuring public safety during CBRN incidents, encompassing utilities, transportation networks, healthcare facilities, and communication systems. This includes:

- **Regular assessments:** Conduct vulnerability assessments to identify weaknesses in critical infrastructure and prioritize enhancements.
- **Training and drills:** Implement training programs and simulation exercises for personnel to prepare for potential CBRN scenarios.
- **Investments in technology:** Upgrade monitoring systems and implement advanced technologies to improve detection and response capabilities.
- **Establishing partnerships:** Foster collaboration between public and private sectors to enhance resource sharing and support during emergencies.

3) Capacity building

Another key action of CBRN planning is to ensure that staff and agencies are prepared to respond effectively to CBRN incidents. The focus is on building capacity, testing plans, and addressing personnel needs.

The comprehensive personnel strategy includes the following key components:

- **Specialized training:** Regular and ad-hoc training ensures that responders are familiar with specific elements of response plans, equipment, and protocols. It also serves to assess the physical and mental health of personnel, helping to maintain sustained performance during incidents.
- **Inter-agency training:** Regular and ad-hoc training to ensure that different stakeholders (e.g., first responders, public health officials, and military personnel) understand each other's roles and responsibilities. These trainings during planning are essential for enhancing operational compatibility, ensuring equipment interoperability, minimizing errors, fostering collaboration, and optimizing resource utilization.
- **Competency assessment:** Regular assessments to ensure that personnel maintain the required skills, knowledge, and readiness to effectively respond to CBRN threats.
- **Leadership development:** Regular and ad-hoc training focused on developing leadership skills to manage crisis situations, make critical decisions under pressure, and lead teams during complex emergencies.

- **Personnel well-being and professional support:** Ongoing, or as needed, support for the mental and physical well-being of responders, ensuring that they have access to counseling services, recovery support, and the resources needed to perform at their best.
- **Surge capacity planning:** Ensuring availability of sufficient personnel and resources to quickly scale efforts in response to large-scale emergencies, with contingency plans in place to manage a surge in demand.
- **Public awareness training:** Regular and ad-hoc training to educate community members on recognizing CBRN threats, reporting suspicious activities, and following evacuation or shelter-in-place orders.

To know more about training, competencies, surge capacity and personnel well-being see Chapter 3.5 Establishing a CBRN training programme of the Planning Section.

4) Review and evaluation

The final step in the CBRN planning cycle is to ensure that the CBRN response plans remain effective, relevant and adaptable to evolving threats and circumstances. Plans are living documents and require frequent updates and revisions based on lessons learned during actual incidents, exercises, or drills. This step involves continuous analysis of the plans' components, performance during incidents or exercises, and ongoing improvements.

Main elements for an effective review and evaluation include:

- Definition of **clear objectives** for the review and evaluation process, such as ensuring readiness, identifying gaps, or improving interagency coordination.
- Use of **key performance indicators (KPIs)** to measure success, such as response times, resource deployment efficiency, percentage of affected individuals effectively treated etc. It also includes the use of **benchmarking** to compare the outcomes of the response plans to international standards (e.g., IAEA, OPCW, WHO) and best practice from other countries.
- Comprehensive **data collection** through CBRN situation assessments, after-action reports (e.g., what worked well? what did not work? what can be improved?), and feedback mechanisms (surveys, interviews, or debriefings with stakeholders), etc.
- Engagement of **all relevant stakeholders,** including first responders, law enforcement, intelligence, health officials, policymakers, and community leaders.
- Testing of the plans against **real-world scenarios** (based on past incidents), **hypothetical scenarios** (emerging or potential threats) and **worst-case scenarios** (plan's ability to handle large-scale or high-impact incidents).
- Engagement of **independent or third-party evaluation** for unbiased reviews or fresh perspectives.
- Maintenance of **detailed documentation** of review findings and changes.
- **Frequency of review and evaluation** though routine reviews (e.g. plan reviews on an annual or biannual basis), post-incident evaluations (immediate review actions taken after any real incident to derive lessons learned.) and exercise-based evaluation (evaluation of the plans implementation after each exercise, incorporating feedback from all stakeholders).

CBRN response planning: challenges and good practices

CHALLENGES	GOOD PRACTICES
Ensuring **active engagement of all stakeholders** during the development of response plans and achieving clarity on their respective roles and responsibilities.	▸ Designate a **lead agency** responsible for plan development and implementation. This agency must have the authority, expertise, and resources to coordinate CBRN response efforts effectively. ▸ Identify **supporting agencies** based on their expertise, capabilities and resources relevant to CBRN response. Involve private sector partners, community representatives, and subject matter experts. ▸ Establish **clear roles and responsibilities** through **formal written documents.** The lead agency's authority should be explicitly defined, including decision-making powers and accountability requirements. ▸ Formalize the engagement process through the establishment of **planning committees** that oversee various aspects of plan development and maintenance. ▸ Develop plans through **scenario-based workshops** or **planning seminars/workshops.**
Ensuring **SOPs are clearly written,** comprehensive, and easily understood by all responders.	▸ Ensure SOPs are **comprehensive, consistent, and compliant** with relevant standards and regulations. ▸ Use a **clear and concise structure,** for easy reference during high-pressure situations. ▸ Include **flowcharts, checklists, and decision trees** to enhance usability. ▸ Implement **quality control measures** to verify the accuracy, clarity, and practicality of SOPs through peer reviews or pilot testing. ▸ **Align SOPs with training programs** to ensure personnel are familiar with the procedures. ▸ Ensure SOPs **align with national and international standards,** such as those provided by the WHO, OPCW, IAEA, and other relevant bodies. ▸ Incorporate **legal and regulatory requirements** related to CBRN response. ▸ Follow a **structured review and approval process,** engaging stakeholders and subject matter experts to ensure operational alignment and regulatory compliance. ▸ Develop **clear update procedures** to regularly revise SOPs, incorporating evolving best practices, technological advancements, and insights gained from operational experiences.

CHALLENGES	GOOD PRACTICES
Ensuring that the **plans and SOPs align with national and international laws** while providing responders with the authority to act decisively during incidents and mitigating potential legal challenges during or after an incident (such as liability issues, jurisdictional disputes, or challenges related to privacy and data sharing).	▸ Reviewing **relevant laws and regulations,** including the review of domestic legislation (such as public health laws, emergency powers, and environmental regulations) and the alignment of response procedures with international treaties and conventions. ▸ Ensure that responders, including military, police and civilian agencies have the **legal authority** to implement necessary actions such as quarantine, evacuation, and restricted area enforcement. ▸ Address **legal gaps or ambiguities** through consultations and legislative updates. ▸ Create SOPs for handling **legal requirements during responses,** such as reporting incidents to international bodies, managing evidence, and maintaining accountability for actions taken. ▸ Train response teams on **applicable laws and regulations** to ensure they understand their rights, responsibilities, and limitations during operations. ▸ Establish mechanisms for **continuous legal review** and consultation to adapt to evolving legal standards and emerging scenarios.
Insufficient **well-trained personnel** to handle CBRN large-scale or prolonged emergencies.	▸ Define **roles and responsibilities** of personnel involved in CBRN response, referencing the specific requirements outlined in the CBRN response plan, such as: CBRN managers (event commanders, planners), first responders (medical, fire, hazmat, law enforcement), scientific CBRN experts, public health officials, logisticians, legal and regulatory specialists, engineers, environmental specialists, public information officers, mental health professionals, support and administrative staff. ▸ Establish **capability levels** within each role, reflecting increasing levels of knowledge, skills, and experience. For example, first responders might have basic (awareness), intermediate (operational), and advanced (specialist) capability levels. ▸ Define **core competencies** outlining the necessary skills, knowledge, behavioral traits, and physical requirements for each role and capability level involved in CBRN response. This approach can guide recruitment, training, and ongoing performance assessments. ▸ Ensure **standardized competencies,** such as developing competency assessment tools and establishing certification requirements, recognizing individuals.

CHALLENGES	GOOD PRACTICES
	▸ Develop **leadership and sustainability:** › **Identify and train personnel** who will manage response operations at all levels, from event commanders to evacuation zone managers. › Ensure **cross-functional capabilities** where appropriate. › Build s**ustainable training capability** by investing in Train-the-Trainer programs. ▸ Promote **collaboration between different agencies** involved in CBRN response through joint training exercises and planning sessions, and by establishing clear communication protocols. ▸ Plan for **surge capacity needs** by, for example, maintaining a trained reserve personnel roster, supporting staff who can be reallocated during emergencies, cross-training personnel from related departments, and establishing mutual aid agreements for personnel sharing. ▸ Implement **personnel support and well-being:** establish comprehensive health monitoring programs, provide regular psychological support and counselling services, implement stress management and resilience training, create work-life balance policies for sustained operations, develop family support programs, implement health monitoring and support programs. ▸ Implement **staff retention strategies** such as: professional development and career growth, recognition and reward systems, comprehensive benefits package, work environment and support. ▸ Implement **standardized training programs** and monitor training **effectiveness.**
Addressing **resource constraints,** which can hinder effective preparedness and response efforts.	▸ Prioritize **monitoring and evaluation activities,** which allow assessing the effectiveness of preparedness and response efforts, identify gaps, and make informed decisions to optimize resource allocation and enhance overall readiness for CBRN incidents. ▸ Utilize **existing data sources and information systems,** which involves leveraging available information to enhance decision-making, streamline operations, and improve situational awareness. ▸ Seek **funding and technical assistance** from international organizations.

CHALLENGES	GOOD PRACTICES
	▸ Use a **hybrid approach,** which involves maintaining stockpiles of critical equipment to ensure immediate availability during emergencies while simultaneously utilizing just-in-time procurement for non-critical resources. This approach balances preparedness and cost-efficiency, ensuring that essential supplies are readily accessible when needed while minimizing waste and storage costs for less critical items. ▸ Advocate for **risk-based financial planning** and leverage **multi-source funding,** including government budgets, international aid, and public-private partnerships.
Ensuring the **availability and readiness of essential supplies** during large-scale CBRN incidents.	▸ Maintain comprehensive **resource inventories.** Use databases to track the availability, status, and location of resources, and have a clear understanding of assets at all times. ▸ Store resources under conditions that **preserve their usability** (e.g., temperature-controlled environments for medical supplies). ▸ Introduce **rotational stockpiles** and enforce regular inspection, maintenance, and environmental control systems to ensure operational readiness. ▸ Establish **surge capacity frameworks and agreements** with suppliers for emergency procurement and personnel reinforcements. Implement **strategic geographic distribution.** ▸ **Balance accessibility** with security requirements. ▸ Combine **stockpiling for critical items with just-in-time procurement** for non-critical resources. ▸ Implement **multi-modal transportation** options and ensure pre-arranged transport agreements (e.g., trucks, airlifts) for rapid deployment. ▸ Ensure availability of **redundant communication channels,** including satellite phones, digital radios, and secure apps, to maintain operational coordination. ▸ Conduct **gap analyses** to identify resource shortfalls, implement strategic stockpiling in geographically distributed locations, and establish real-time inventory tracking systems. ▸ Develop **protocols for distributing resources** to affected areas based on incident severity and population density.
Establishing **resilient and adaptable supply chains** to ensure the continuous availability of critical resources and uninterrupted operations during emergencies.	▸ Establish **pre-negotiated partnerships and agreements** with suppliers to ensure rapid procurement during emergencies, with agreed-upon terms for expedited deliveries and flexibility. ▸ Identify and establish relationships with **alternative suppliers** to mitigate the risk of single-source dependency and ensure continuity of supply in case primary suppliers are unavailable. ▸ Develop and implement **contingency plans for alternative transportation and delivery methods.** This includes identifying backup routes, distribution centers, and transport providers to mitigate potential disruptions to logistics during a crisis.

CHALLENGES	GOOD PRACTICES
Ensuring **response plans are regularly reviewed**, updated, and tested for effectiveness.	▸ Conduct regular exercises, drills, and simulations to test response plans in realistic scenarios. Incorporate **lessons learned** to improve effectiveness and adaptability. ▸ **Engage all relevant stakeholders,** including government agencies, private sector partners, and community organizations, to ensure plans address diverse perspectives and requirements. ▸ Following every exercise or real-world incident, perform comprehensive **after-action reviews** to identify strengths, weaknesses, and areas for improvement. ▸ Continuously **monitor and adapt plans** to address new threats, technologies, and evolving risk landscapes. ▸ Maintain clear, updated, and **accessible documentation** of response plans to ensure all responders are familiar with protocols.
Balancing the need for comprehensive response plans with the requirement for simplicity, ensuring that **plans are thorough yet practical,** and avoiding unnecessary complexity that could hinder clarity and execution.	▸ Focus on the **most critical components** of the response plan, such as roles, responsibilities, communication protocols, and key response actions, ensuring they are easy to understand and implement. ▸ Use clear, **concise language,** avoiding jargon and overly technical terms. ▸ Create **adaptable and scalable plans** that can accommodate different levels of incidents, from minor events to major catastrophes. ▸ Break down complex plans into **manageable sections** or modules, allowing for flexibility and easy updates without overwhelming responders with excessive detail. ▸ Conduct exercises to **test the clarity and practicality** of the plans, identifying areas where complexity may be hindering effective response.
Resistance to change in response practices or adoption of new technologies.	▸ **Implement the changes gradually** in multiple phases. ▸ Conduct change **management workshops** and showcase the benefits of new technologies and practices through hands-on demonstrations and pilot projects. ▸ **Involve multiple stakeholders** in the planning or development of plans to ensure there is enough consensus to adapt the new practices.

3.1 DEFINING A COMMAND STRUCTURE FOR CBRN RESPONSE

A clear command structure with effective inter-agency collaboration, clear communication protocols, and a unified strategic approach is essential for managing CBRN incidents.

While various incident management systems exist for incident response, the Unified Command Structure (UCS) is particularly well-suited for CBRN incidents. The UCS is a collaborative management system that enables coordinated, multi-agency decision-making and operational control during complex CBRN incidents. It enables agencies with different legal, geographic, and functional authorities and responsibilities to work together effectively under coordinated leadership without affecting individual agency authority, responsibility, or accountability. The UCS ensures streamlined decision-making, efficient resource allocation, and seamless communication – elements that are vital for addressing the scale and complexity of CBRN incidents, which often require integration across local and national levels. Aligned with national risk assessments and tailored to a country's specific CBRN threat landscape, the UCS should be proactively planned, with clearly defined structures, roles, responsibilities, and decision-making processes reflected in CBRN response plans.

KEY ACTIONS

1) Define the UCS structure, roles and responsibilities of stakeholders

Despite its integrated nature, the UCS carefully preserves the individual authority, responsibility, and accountability of each participating agency. The UCS is led by senior representatives from key agencies who share the responsibility for providing overall direction and making critical decisions. This leadership is supported by the Command Staff, responsible for advisory roles and communication functions, and the General Staff Sections, which handle operations, planning, logistics, and financial management. Clear reporting lines ensure that each section operates efficiently and contributes to the broader response effort.

To ensure effective coordination and address specific needs, the UCS should incorporate specialized groups tailored to various aspects of a CBRN response, activated as needed for the specific tasks under their purview. These may include situation assessment teams to analyze incident impacts and forecast scenarios, resource management teams to allocate essential materials and personnel, and international coordination teams to integrate foreign assistance when required. Decision-making groups, composed of senior officials and subject matter experts, also play a key role in determining the need for emergency declarations and strategic adjustments. These groups operate under the unified structure while leveraging specialized expertise to address diverse response requirements.

The UCS operates at three incident management levels – strategic, tactical, and operational – based on the scale and complexity of the incident. This tiered approach enables a dynamic response structure that adapts to both large-scale and localized incidents. While the basic structure of the UCS remains consistent across all levels, the focus and scope vary, with each level tailored to specific needs and timeframes:

- **Strategic level:** Oversees overall emergency management, sets policy and strategic frameworks and direction, and coordinates high-level resources to guide the entire response effort.
- **Tactical level:** Implements strategic decisions and coordinates the response efforts at the operational-level, bridging the gap between strategic decisions and on-scene operations.
- **Operational level:** Manages immediate response at the incident site, such as containment, decontamination, and public safety measures, and adapts plans based on real-time conditions.

The UCS is designed to be scalable, adapting to the magnitude and complexity of the CBRN incident, thus enabling a seamless transition between localized and large-scale responses. In the planning phase, this adaptability is addressed by establishing predefined thresholds for scaling operations.

The table below shows an example of scalability:

 **Large-scale incident**	▸ Full activation of all components of Unified Command across strategic, tactical, and operational-levels ▸ Distinct groups for each specialized function ▸ Various operational periods ▸ International coordination
 **Small-scale incident**	▸ Unified Command may be handled by a single agency, potentially combining strategic and tactical-levels ▸ Specialized functions integrated into broader organizational units ▸ Shorter operational periods ▸ Primarily local agency resources

As an incident grows in size and complexity, the UCS can further expand its organizational structure by adding specialized sections (e.g., operations, planning, logistics, and finance/administration), branches, divisions, and groups. These components manage specific operational areas or functions (e.g., containment, decontamination, medical treatment, etc.) while maintaining clear reporting lines within the UCS leadership. This systematic expansion enables complex operations to be divided into manageable components, ensuring that each function is effectively coordinated while maintaining overall unity of command and strategic oversight.

2) Set activation thresholds for CBRN incidents

Activation thresholds are critical for determining when to implement the UCS in response to CBRN incidents. These thresholds may include specific risk-based indicators, such as the presence of threat indicators, detection of CBRN agents or materials exceeding predefined concentration levels, confirmed or suspected releases of hazardous substances, and the potential for widespread contamination.

Other common trigger mechanisms can include credible intelligence reports, health surveillance data indicating exposure, multiple casualty reports with consistent symptoms, or breaches of containment in high-risk facilities. By pre-establishing these activation thresholds within the planning process, agencies can ensure timely and coordinated responses, enabling more effective management of CBRN incidents.

3) Pre-identify potential incident commanders

Incident Commanders are senior representatives from key agencies who are part of the leadership team. They are not positioned above the UCS leadership but are integral to it, participating in collective strategic decision-making.

Incident Commanders are selected based on the specific incident type and their agency's expertise, and they maintain their agency-specific responsibilities while contributing to the coordinated response effort. During the planning phase, potential incident commanders (and their successors) can be pre-identified based on factors such as the scale and complexity of potential incidents, the nature of the CBRN threat, geographic considerations, and the expertise required for specific response functions. This ensures that individuals with the appropriate qualifications and authority are ready to assume leadership roles tailored to the unique demands of various scenarios.

4) Define communication protocols

Effective communication allows exchanging real-time information, situational updates, and directives during an incident using secure, redundant communication channels to prevent disruptions and standardized terminology and predefined reporting formats to minimize misunderstandings and improve operational efficiency.

5) Define inter-agency collaboration mechanisms

The UCS is built on robust inter-agency coordination mechanisms that integrate resources, expertise, and capabilities from multiple stakeholders. These mechanisms include pre-established agreements, such as Memorandums of Understanding (MOUs) or mutual aid agreements, that define roles, responsibilities, and resource-sharing arrangements. Regular joint training, simulations, and shared planning activities strengthen interoperability.

6) Assessment and revision

Regular assessment and revision of UCS plans are essential to maintaining their effectiveness in addressing evolving threats, incorporating advancements in technology, and adapting to updates in inter-agency protocols. Periodic reviews ensure that the UCS remains aligned with current risk landscapes, operational capabilities, and stakeholder needs, fostering a resilient and adaptive response framework for CBRN incidents. Moreover, evaluation and continuous improvement are essential to

maintaining an effective UCS. After each incident or exercise, a comprehensive review should be conducted to assess the performance of the UCS, identify lessons learned, and pinpoint areas for improvement.

Defining a command structures for CBRN response: challenges and good practices

CHALLENGES	GOOD PRACTICES
Identifying the lead agency can be challenging, especially when conflicting mandates, protocols, and priorities among agencies can create confusion during the response.	▸ Establish **clear roles and responsibilities** ahead of a CBRN incident, including CBRN incident SOPs that were agreed at the inter-agency level. ▸ Ensure that **SOPs and protocols** clearly identify which agency is in charge for every type of CBRN incident. ▸ Conduct joint **training** and **table-top and field exercises.**
Political considerations and legal constraints, such as state versus federal authority or civilian versus military command, can delay the appointment of a strategic commander, limit certain agencies' leadership roles, and hinder decision-making in rapidly evolving situations.	▸ Develop **pre-approved action plans** and frameworks to ensure that decision-making authority is clearly delineated. ▸ Provide field commanders with **clear operational guidelines.** ▸ Consider the possibility of needing to declare **state of emergency.**
Unclear **lines of authority** across different jurisdictions can delay response and lead to valuable time lost.	▸ Pre-establish **cooperation and collaboration agreements.** ▸ Clearly **define jurisdictional boundaries** in plans.
Cultural and organizational differences among the agencies that are part of the UCS (e.g. between military and civilian agencies) can lead to disagreement on effective response.	▸ Organize **cultural competency training** to help individuals and organizations develop the knowledge, skills, and attitudes necessary to effectively interact with agencies from diverse backgrounds. The goal is to increase awareness of cultural differences, reduce biases, and enhance cross-cultural communication to improve relationships and outcomes in multicultural settings. ▸ Create a **joint task force** for CBRN responses which can help blending different organizations into a functional unit.

3.2 CRISIS COMMUNICATION PLANNING

Public awareness and education are essential for fostering community resilience against CBRN threats. An informed public is better prepared to respond to emergencies, follow safety protocols, and support mitigation efforts. Education initiatives reduce the impact of misinformation and disinformation, alleviate public fear, and enhance cooperation with authorities during a CBRN event.

KEY ACTIONS

1) Assess the existing communication structure

Using a checklist of various indicators can be useful for identifying the gaps that need to be addressed to ensure effective communication with the public. For example[3], multiple checklists can be developed to assess different aspects related to the communication strategies:

Planning, research, training, and evaluation		
☐ Yes	☐ No	Does your organization have an emergency response/crisis communication operational plan for public information and media, partner, and stakeholder relations?
☐ Yes	☐ No	Have you coordinated your planning with the community or state emergency operation center?
☐ Yes	☐ No	Have you coordinated your planning with other response organizations or competitors?
☐ Yes	☐ No	Have designated spokespersons received media training and risk communication training?
☐ Yes	☐ No	Do they understand emergency crisis/risk communication principles to build trust and credibility?

3 Alabama Public Health (n.d). Checklist4–6. Needs Assessment for Crisis and Emergency Risk Communication. https://www.alabamapublichealth.gov/riskcommunication/assets/needsassessment1.pdf

If your organization has a plan, does the plan have the following elements?		
☐ Yes	☐ No	Designated line and staff responsibilities for the public information team.
☐ Yes	☐ No	Information verification and clearance/approval procedures.
☐ Yes	☐ No	Agreements on information release authorities (who releases what/when/how).
☐ Yes	☐ No	Regional and local media contact list (including after-hours news desks).
☐ Yes	☐ No	Procedures to coordinate with the public health organization response teams.
☐ Yes	☐ No	Designated spokespersons for public health issues in an emergency.
☐ Yes	☐ No	Public health organization emergency response team after-hours contact numbers.
☐ Yes	☐ No	Contact numbers for emergency information partners (e.g., Governor's public affairs officer, local FBI public information special agent in charge, local or regional department of agriculture or veterinarian public information officers, Red Cross and other nongovernment organizations).
☐ Yes	☐ No	Agreements/procedures to join the joint information center of the emergency operations center (if activated).
☐ Yes	☐ No	Procedures to secure needed resources (space, equipment, people) to operate the public information operation during a public health emergency 24 hours a day/7 days a week, if needed.

2) Develop a CBRN communication plan

Having a CBRN communication plan in place can help save valuable time during a crisis. It is an operational document, which should be seamlessly integrated into the organization's overall response plan, as well as into local, state, or national response framework. An effective plan outlines the resources available and the procedures to follow in an emergency, while also providing sample key messages to communicate to the different target audiences. For example, the Centers for Disease Control and Prevention (CDC)[4] recommends including at least the following elements:

- **Designated responsibilities:** Clearly defined roles and responsibilities for the personnel who are involved in the processes related to communication with the public.
- **Verification and clearance procedures:** Elaborated internal processes for verifying information and expediting clearance.
- **Information-release authorities:** Pre-determined agreements on who releases what information, when, and how.

4 Centers for Disease Control and Prevention (2018). Crisis & Emergency Risk Communication (CERC).

- **Media contacts:** Established regional and local media contact lists, including after-hours news desks.
- **Coordination procedures:** Pre-determined procedures for coordinating with public health and other response teams.
- **Joint information center:** Establish a joint information center as a centralized hub where public information officers from multiple agencies work together to manage and coordinate the release of information to the public, media, and other stakeholders. The primary role of the center is to ensure that all communication is clear, accurate, and consistent, minimizing confusion during the event. By bringing together various responding agencies, the center facilitates unified messaging to ensure that the public receives information from a single authoritative source. This is crucial in preventing the spread of conflicting information that could lead to unnecessary panic. In addition to its role in unifying communication, the center manages media relations, coordinates press briefings and responds to inquiries. It plays an active role in controlling rumors and correcting misinformation and disinformation quickly to maintain public trust and ensure that safety instructions are followed. Whether providing evacuation details, decontamination procedures, or shelter-in-place directives, the center ensures a continuous and verified flow of information to the public, government entities, and international partners, if needed.
- **Spokespersons:** Designated public spokespersons and third-party validators for emergencies.
- **Emergency contact numbers:** Regularly update after-hours contact numbers for emergency response team members.
- **Emergency response information partners:** Foster alliances and partnerships to ensure that officials and experts speak with one voice and that resources are available and shared (including Red Cross and other NGOs).
- **Joint information center procedures:** Exercise procedures and agreements to join the center within the Unified Command Structure if activated.
- **Resource procedures:** Pre-established procedures to secure necessary resources (space, equipment, personnel) for 24/7 public information operations during an emergency.
- **Information dissemination methods:** Exercise methodologies to communicate with the public, stakeholders, and partners, including websites, social media channels, press releases, etc.
- **Stakeholder lists:** Pre-developed lists of key stakeholders, methods to reach them, and background descriptions.

3) Raise awareness

Effective communication is essential in helping at-risk communities understand potential risks and contribute to building resilience. Raising public awareness about CBRN incidents enhances community preparedness, encourages timely and informed actions, and reduces the spread of misinformation and disinformation. This ultimately facilitates a more coordinated and effective response.

Communication elements to consider include:

- **Engaging community leaders:** Involve trusted community figures in spreading awareness and educating the public, leveraging their influence to enhance message credibility.
- **Conducting regular drills and simulations:** Organize community-wide and national drills and simulations to practice response actions and reinforce the importance of preparedness.
- **Providing accessible educational materials:** Develop and distribute easy-to-understand educational and awareness materials, including brochures, videos, and interactive content. CBRN incidents might require specific basic knowledge from the population, which can be provided in an awareness-raising strategy (e.g., IFRCS CBRN public awareness)[5]. Make sure that the materials provided are available in different languages if needed. Remember that for messages to be credible and impactful within communities, they must be tailored to local hazards, cultures, and contexts. Establishing an overall culture of safety and resilience necessitates unified messaging. For example[6], the International Federation of Red Cross and Red Crescent Societies recommends considering the following aspects:

STEP-BY-STEP GUIDE FOR ADAPTING AND ADOPTING KEY MESSAGES

Step 1: Meet with the national disaster risk management office to make a preliminary plan.

Step 2: Prepare the key messages for review – translate the messages into the local language where necessary and format in line with nationally disseminated key messages.

Step 3: Plan a two-day workshop, set an agenda, send invitations to the authorities that represent different sectors and areas of expertise and share the review package with the subject-matter experts.

5 International Federation of Red Cross (2018). Public awareness and public education for disaster risk reduction: Chemical, Biological, Radiological and Nuclear Hazards, https://www.ifrc.org/sites/default/files/2021-06/20-CBRN-HR.pdf

6 International Federation of Red Cross and Red Crescent Societies and Save the Children (2018). Public awareness and public education for disaster risk reduction: Action-oriented key messages for households and schools. https://www.ifrc.org/sites/default/files/PAPE-2.0-English.pdf

Step 4: Prepare for the national key messages workshop.

Step 5: Conduct the national key messages workshop.

Step 6: Compile and edit inputs and circulate draft for final review.

Step 7: Finalize, publish and disseminate the key messages.

Step 8: Make use of the nationally adopted key messages for household risk reduction and to build resilience.

Step 9: Review the key messages periodically.

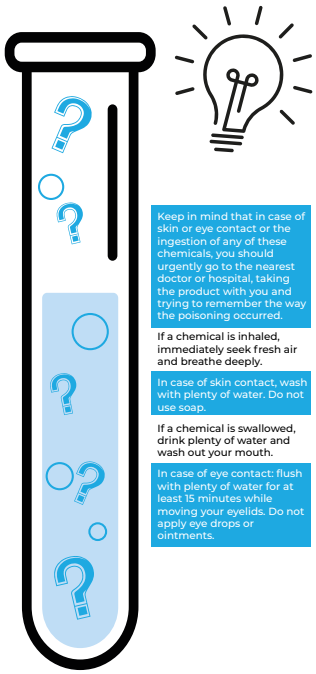
- **Fostering two-way communication:** Establish feedback mechanisms such as hotlines, surveys, and public meetings to address public concerns and gather input on communication strategies.
- **Implementing school programs and community awareness campaigns:** Integrate CBRN awareness into primary, secondary, and tertiary school curricula to educate children and adolescents, ensuring long-term community preparedness. Furthermore, continuous targeted campaigns can become an effective way to familiarize the population with CBRN related issues before an event occurs. For example, the government of Colombia developed a campaign[7] to promote proper practices for the use, handling, and storage of chemical substances. The campaign encourages surveillance, promotion and prevention activities for subjects who handle chemical substances, aiming to minimize risks to the health of workers and nearby residents, as well as to protect surrounding infrastructure and the environment.

7 Departamento de Risaralda (n.d). Control riesgo quimico https://www.risaralda.gov.co/salud/publicaciones/1236/control-riesgo-quimico/

What to do in case of emergency?

Many of the chemicals used in the home are hazardous materials for health and the environment if used and stored incorrectly.

The products that cause most emergencies in the home are pesticides. They are followed by medicines, cleaning products, alcoholic beverages and cosmetics.



Recommendations

1. Always read the product label as it provides information on handling, storage and precautions.
2. Do not accumulate large quantities. Buy only the necessary amount.
3. Store the products in a closed place and at a considerable height, out of the reach of children and pets.
4. Cover the products when you interrupt or stop using them.
5. Store all flammable liquids out of the habitable areas of your home and away from the oven, car or stove.
6. Never store hazardous products near food, food for animals or medicines.
7. Always store products in their original containers, which should include the corresponding label, instructions for use and first aid instructions.
8. Medicines and cosmetic products should also be stored in an isolated and closed place where they are out of reach of children and pets.

Keep in mind that in case of skin or eye contact or the ingestion of any of these chemicals, you should urgently go to the nearest doctor or hospital, taking the product with you and trying to remember the way the poisoning occurred.

If a chemical is inhaled, immediately seek fresh air and breathe deeply.

In case of skin contact, wash with plenty of water. Do not use soap.

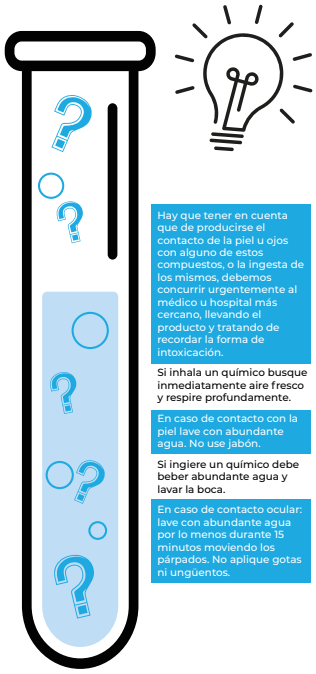
If a chemical is swallowed, drink plenty of water and wash out your mouth.

In case of eye contact: flush with plenty of water for at least 15 minutes while moving your eyelids. Do not apply eye drops or ointments.

¿Qué hacer en caso de emergencia?

Muchos de los productos químicos que se utilizan en el hogar son materiales peligrosos para la salud y el medio ambiente si son usados y almacenados incorrectamente.

Los productos que más ocasionan emergencias en el hogar son los plaguicidas. Le siguen los medicamentos, productos de aseo, bebidas alcohólicas y los cosméticos.



Recomendaciones

1. Leer siempre la etiqueta del producto ya que trae información sobre su manejo, almacenamiento y precauciones.
2. No acumular grandes cantidades. Comprar solamente la cantidad necesaria.
3. Almacenar los productos en un lugar cerrado y a una altura considerable fuera del alcance de los niños y los animales de compañía.
4. Tapar los productos cuando interrumpa o termine su uso.
5. Guardar todo líquido inflamable fuera de los ambientes habitables de su hogar y lejos del horno, el automóvil o la estufa.
6. Jamás almacenar productos peligrosos cerca de comida, alimentos para animales o medicamentos.
7. Siempre almacenar los productos en sus envases originales los cuales deben incluir la correspondiente etiqueta, instrucciones de uso e indicaciones de primeros auxilios.
8. Los medicamentos y productos cosméticos también se deben guardar en un lugar aislado y cerrado en donde no tenga alcance los niños y mascotas.

Hay que tener en cuenta que de producirse el contacto de la piel u ojos con alguno de estos compuestos, o la ingesta de los mismos, debemos concurrir urgentemente al médico u hospital más cercano, llevando el producto y tratando de recordar la forma de intoxicación.

Si inhala un químico busque inmediatamente aire fresco y respire profundamente.

En caso de contacto con la piel lave con abundante agua. No use jabón.

Si ingiere un químico debe beber abundante agua y lavar la boca.

En caso de contacto ocular: lave con abundante agua por lo menos durante 15 minutos moviendo los párpados. No aplique gotas ni ungüentos.

Crisis communication planning: challenges and good practices

CHALLENGES	GOOD PRACTICES
Lack of knowledge and techniques for **addressing disinformation and misinformation.**	▸ Create **protocols** to verify, clear, and disseminate accurate information in a timely manner. ▸ Train spokespersons and other stakeholders to use tools like the "truth sandwich" to effectively **debunk** misinformation and disinformation. ▸ Define processes to eventually **monitor** social media and other sources during a CBRN incident to understand the main false claims that need to be addressed.
Lack of **public awareness** regarding CBRN threats.	▸ Conduct **targeted awareness campaigns** tailored to local hazards, cultural norms, and languages. ▸ Develop **school programs** and integrate CBRN topics into curricula to foster long-term community preparedness.
Fragmented response communication, coming from multiple stakeholders during a CBRN incident due to lack of previous agreement.	▸ Establish **joint information centers** to unify messaging, manage media relations, and swiftly address false information. ▸ Create a comprehensive **CBRN communication plan** that includes designated responsibilities, verification procedures, and stakeholder engagement. ▸ Use **coordinated communication channels,** such as social media, press releases, and public hotlines, to disseminate clear and consistent messages. ▸ Conduct **simulations exercises to test** communication strategies, identify gaps, and improve public confidence in response systems.
Insufficient **educational materials** to increase awareness regarding CBRN threats.	▸ Develop brochures, videos, and interactive **content** in multiple languages with simple, actionable guidance on CBRN risks and responses. ▸ Ensure materials are **culturally sensitive** and consider the needs of vulnerable groups.
Limited engagement with local stakeholders.	▸ Involve trusted **community leaders** and organizations, such as the Red Cross, to enhance message credibility. ▸ Collaborate with trusted **influencers** or public figures who have a strong presence and credibility within social media platforms. ▸ Establish **feedback mechanisms** like surveys and hotlines to gather public input and refine communication strategies.

3.3 DEFINING EMERGENCY AUTHORITIES AND THE LEGAL FRAMEWORKS FOR DECLARING A STATE OF EMERGENCY

A state of emergency is a temporary grant of exceptional powers to governments, used as a last resort to manage crises that exceed normal response capabilities (e.g., natural disasters, CBRN incidents, etc.). These powers are typically outlined in constitutions or emergency laws, designed to allow for swift and decisive action. However, they must be subject to clear limitations and safeguards to protect human rights and civil liberties.

Declaring a state of emergency empowers authorities to:

- Mobilize additional resources from regional, national, or even international sources, enabling authorities to acquire critical supplies, deploy specialized personnel, and scale up response efforts effectively.
- Expedite decision-making by temporarily bypassing bureaucratic hurdles, thus allowing for quicker decisions and actions that are vital in a time-sensitive situation like a CBRN incident.
- Implement enhanced control measures like curfews, movement restrictions, evacuations, and increased law enforcement presence to maintain order, conduct search and rescue, enforce emergency regulations, and secure critical infrastructure.
- Facilitate intelligence gathering and collection and preservation of evidence from the scene.

KEY ACTIONS

1) Define the **legal basis** for declaring a state of emergency to ensure clarity, legitimacy, and alignment with national laws and international standards, enabling decisive action while safeguarding rights and preventing misuse of authority.

2) Define the **process** of declaring a state of emergency. This process typically includes activating pre-determined emergency response protocols, conducting assessments and receiving recommendations from subject-matter experts, consulting with relevant stakeholders, and issuing a formal announcement through appropriate legal channels.

3) Specify the **scope** of the state of emergency. Clearly delineate the powers granted during a state of emergency, including requisitioning resources, enforcing quarantines, implementing curfews or evacuations, and restricting travel or assembly.

4) Incorporate **safeguards,** such as judicial review, legislative oversight, and time-bound restrictions, to prevent misuse of emergency powers. It is essential to specify the **limitations** of the state of emergency to ensure that these powers are legally constrained to prevent abuse. Actions taken during the response and recovery phases

must adhere to existing laws and regulations, with safeguards for oversight and accountability.

5) Clearly specify **trigger conditions,** e.g. the conditions under which a state of emergency can be declared. Countries have pre-established criteria outlining the conditions that necessitate a state of emergency declaration, typically focusing on factors such as:

- overwhelmed response capabilities,
- severity and risk (e.g. large-scale release of hazardous CBRN agents and materials, significant threats to public health, safety, or critical infrastructure),
- potential for high number of casualties, and
- the need for extraordinary measures.

While these criteria are likely applicable in most countries, some potential variations may exist, such as the inclusion of more specific details regarding CBRN agent and material types, contamination thresholds, or casualty numbers to trigger a state of emergency. Examples of how criteria for declaring a state of emergency for a CBRN incident are applied in different countries.

6) Assign **authority to declare an emergency.** Specify who holds the authority to declare an emergency, including provisions for delegating authority in localized situations and scenarios that require national coordination. The authority can reside with the executive (president, prime minister), the legislative (parliament), a combination of both, or even lower-level officials for localized emergencies. This ensures a balance between necessary government action and the protection of individual freedoms. Notably, emergency rules do not always disrupt regular government operations. Countries like Spain and Portugal maintain normal functioning during emergencies. Judicial review often exists to ensure the declaration's legality and proportionality. Examples include the President of the United States of America declaring a state of emergency subject to congressional termination, or Canada where the federal government consults provinces before declaring. Some countries have time limits or specific triggers for emergencies, like France's 12-day limit on presidential declarations or Australia's Biosecurity Act outlining triggers for biosecurity emergencies.

7) Outline **the implications** of declaring a state of emergency. A declaration of a state of emergency enables swift resource mobilization, allowing authorities to access funding, personnel, and equipment critical for response efforts. It also authorizes temporary restrictions, such as movement controls, evacuations, or quarantines, to safeguard public safety and prevent further harm. Additionally, it activates enhanced coordination mechanisms across agencies, jurisdictions, and international partners to ensure a unified and efficient response.

8) Define **post-declaration procedures,** such as mechanisms for extending, modifying, or terminating the state of emergency based on evolving conditions should be defined and provisions for transparent communication with the public and international partners to maintain trust and cooperation.

UNITED STATES

The National Response Framework outlines a tiered approach to emergencies. A state of Emergency might be declared for a CBRN incident exceeding local response capability.
Specific agencies like the Environmental Protection Agency (EPA), the Department of Homeland Security (DHS), and the Centers for Disease Control and Prevention (CDC) all have their own criteria for CBRN events, focusing on contamination levels that need federal intervention.
These criteria might also inlcude factors like specific decontamination procedures and evacuation protocols.

EUROPEAN UNION

The EU Council Decision 2017/733EU on the Union Civil Protection Mechanism (UCPM) emphasizes solidarity and coordinated response among member states.
A state of Emergency might be declared if a CBRN incident requires assistance beyond the capacity of a single member state. The UPCM framework has specific protocols for CBRN incident notification and resource mobilization, ensuring a swift and unified response.

JAPAN

Japan's Basic Law on Disaster Management estabilishes a framework for Emergency response. A state of Emergency might be declared based on the severity of casualties, disruption to critical infrastructure, and the type and scale of CBRN agent release.

Emergency authorities and legal frameworks: challenges and good practices

CHALLENGES	GOOD PRACTICES
Overlapping authority and unclear command structures can lead to confusion, delays, and inefficient resource allocation.	▸ Clearly **define roles and responsibilities** of different agencies. ▸ Establish **effective communication channels** and coordination mechanisms. ▸ Develop and exercise **standardized operating procedures** for interagency cooperation.
Encountering **legal limitations** on emergency powers and potential human rights concerns when declaring a state of emergency.	▸ Consult with **legal experts** to ensure compliance with relevant laws and regulations. ▸ Establish **clear guidelines** for the exercise of emergency powers. ▸ **Implement safeguards** to protect civil liberties and human rights.
Inadequate **legal frameworks** may hinder timely response efforts or lead to legal disputes post-incident.	▸ Regularly **review and update legal frameworks** to adapt to evolving threats and ensure their effectiveness.

3.4 ESTABLISHING INTERNATIONAL COOPERATION AND ASSISTANCE FRAMEWORKS

CBRN incidents may require international assistance when they exceed national response capabilities or when specialized resources are needed. While many countries have developed robust CBRN response programs, others may still face limitations in accessing advanced equipment, technical expertise, decontamination capabilities, or specialized medical treatments. In addition, international cooperation enables critical information sharing and exchange of technical expertise. This collaboration helps inform response strategies, access specialized capabilities, and coordinate efforts, especially when incidents have potential cross-border implications.

Furthermore, capacity-building initiatives facilitated through international partnerships strengthen CBRN planning by enhancing national capabilities, bridging resource gaps, and fostering resilience.

KEY ACTIONS

1) Identify potential international partners and their capabilities and areas of expertise

As an initial step, the following activities should be undertaken:

- **Identify countries and agencies with specialized expertise** in specific areas such as medical countermeasures, decontamination technologies, and detection capabilities. This can include:
  - Establishing joint working groups, conducting collaborative research projects, and organizing exchange programs to leverage shared strengths and promote knowledge transfer.
  - Proactively engaging with neighbouring countries. A CBRN incident can have far-reaching consequences, even if the agent or material does not physically cross borders. Early notification allows neighbouring countries to take preventive measures to protect their populations and prepare for potential impacts such as refugees, environmental, and economic impact. Moreover, neighbouring countries might be the first to provide critical support due to geographical proximity and potential for cross-border impact of the CBRN agent. Their expertise and resources can be invaluable in the initial response phase.
- **Engage with regional and international organizations** to access technical assistance, participate in joint preparedness exercises, and benefit from their expertise in specific CBRN threat domains. International organizations such as the IAEA, OPCW, and WHO play essential roles in global CBRN preparedness and response. Both international and regional organizations are crucial for facilitating international coordination and providing assistance during a CBRN incident. Their specific contributions will vary depending on the nature of the CBRN incident.

International organizations often collaborate among themselves and with regional organizations to ensure a comprehensive and coordinated response.

Specifically, international and regional organizations:

- Serve as a central communication hub, facilitating the exchange of information between affected countries, international organizations, and other regional members, and allowing for a coordinated response and avoids duplication of efforts.
- Maintain stockpiles of essential supplies, equipment, and resources for disaster response. By pooling resources, these organizations can provide vital support to countries facing a CBRN incident, especially those with limited national stockpiles.
- Maintain a roster of experts in CBRN response, disaster management, and public health. International organizations can facilitate the deployment of these experts to the affected country to advise on response strategies, best practices, and technical aspects of the CBRN incident.
- Promote standardized protocols and best practices for CBRN response within their Member States. This ensures a more coordinated regional response and facilitates communication and collaboration between different countries.
- Offer financial assistance to member states facing a CBRN incident. This can help defray the costs of response efforts, medical treatment, and decontamination procedures.
- Provide other supporting documentation and information during a CBRN incident (e.g., satellite images).

- **Establish agreements and protocols.** To ensure readiness, countries should establish pre-incident agreements and protocols to enable swift international assistance. This may require to negotiate agreements to facilitate cooperation in several key areas, including:
  - Resource-sharing agreements, such as Memorandums of Understanding (MOUs) and mutual aid agreements, which establish prearranged frameworks for the efficient allocation and deployment of personnel, equipment, and expertise during CBRN incidents. These should outline procedures for requesting, providing, and coordinating assistance during a CBRN incident, including deployment of personnel, sharing of resources (e.g., medical supplies, decontamination equipment), and provision of technical expertise. It is critical to ensure compatibility between national and regional legal frameworks for CBRN response to facilitate smooth implementation of mutual assistance agreements. This ensures that all participating countries understand their roles and responsibilities, and that responders have the legal authority to take necessary actions within the framework of the regional or international response plan.
  - Joint research and development agreements that promote collaboration on critical areas - such as CBRN detection technologies, decontamination methods, and medical countermeasures - through coordinated research initiatives, technology transfer arrangements, and peer-to-peer exchanges.
  - Information sharing agreements that establish protocols for secure and timely exchange of sensitive information related to CBRN threats and incidents. This

may include information on suspected CBRN threats, detection methods, and best practices for response.

- These arrangements should include the designation of points of contact within partnering countries' customs agencies to facilitate communication and clearance for pre-designated CBRN response cargo, the use of standardized documentation templates (in both sending and receiving country languages) that clearly outline the contents and urgency of CBRN response shipments, and provisions for waiving import taxes and duties on specific aid requested under international assistance agreements.

- **Develop standardized communication channels, protocols and templates for requesting international aid.** These measures facilitate smoother communication, information exchange, and coordinated response during a CBRN incident. Examples include standardized decontamination techniques, medical treatment protocols, and data sharing formats. It is important to allow for some flexibility to accommodate cultural practices and resource limitations. For example, core decontamination principles can be standardized, but specific procedures might be adapted based on cultural practices related to clothing or personal hygiene.
- **Develop joint response strategies with international partners.** It is recommended to consider creating a unified response plan that defines roles and responsibilities for each participating team in the event of the request and provision of international assistance.
- **Ensure compatibility of equipment, training, and protocols with potential partners.** It is important to establish common specifications for detection equipment, protective gear, and decontamination tools used by different countries to enable seamless collaboration and minimize integration challenges during international CBRN emergencies.

2) Create tools for effective requests for assistance

Developing tools and systems in advance can significantly streamline the process of requesting international assistance both prior to and during a CBRN incident. The following activities should be undertaken:

- **Establish a database of international contacts and resources.** Create a comprehensive database of international and regional organizations, partner countries, existing agreements, and the resources they can offer in the event that assistance is needed. Include details about the mandates and expertise of each organization and partner country as well as contact details and points of contact (e.g., IAEA for nuclear and radiological issues, OPCW for chemical incidents, WHO and UNODA ISU for biological threats). In many cases, the simplest and most efficient way to contact a potential international partner is through the Embassy of the respective country or through pre-established mutual assistance agreements. Embassies can facilitate communication with relevant governmental agencies or organizations. Participation in initiative such as the EU CBRN CoE can also help establish contacts with other countries, regional and international organizations.
- **Designate points of contact (POCs).** Assign specific personnel or units as points of contact for coordination with international organizations and bi-lateral partners.

Ensure POCs are trained in international communication protocols and understand their roles in both the planning and response phases.

- **Define communication protocols.** Develop clear protocols for contacting international partners, including pre-agreed communication platforms (e.g., secure email, phone lines, or designated international systems). Standardize the formats for sharing incident-related data, such as incident summaries, resource requests, and updates on national response efforts.
- **Implement systems to align offers with needs.** In the event of a request for international assistance:
  - Design systems (e.g., databases or algorithms) that:
    - Allow for quick identification of relevant resources during the response phase.
    - Match offers of assistance with specific national needs.
    - Prioritize offers based on critical gaps, high-value resources, or complementary support.
  - When implementing these systems, it is essential to include human review of system outputs to ensure compatibility and to address unforeseen challenges, such as language barriers or technical differences in equipment.
- **Allocate resources for the deployment of trained translators and interpreters.** As an integral part of response, international teams should have a pre-prepared standardized visual aids, pictograms, and pre-translated reference materials (e.g., decontamination procedures, medical protocols) to overcome language barriers and ensure expediency.
- **Create standardized request templates.** To minimize confusion and ensure consistency in operations, it is important to develop standardized templates. These templates should promote clarity and comprehensiveness and include:
  - Specific resource needs categorized by priority (e.g., critical, high-value, complementary).
  - Precise location of the incident (e.g., geographic coordinates, regional identifiers).
  - Details of the CBRN agent involved and its potential impacts.
  - Current national response efforts to prevent duplication.

3) Promote regional and international cooperation for capacity building

Collaborating with international partners before a CBRN incident enhances overall preparedness. It fosters a shared understanding of response strategies, facilitates the exchange of critical information and technical expertise, strengthens coordination mechanisms for managing potential cross-border impacts, and supports the adoption of standardized protocols and best practices.

- **Joint training exercises.** Participating in cross-border simulated CBRN exercises with regional and international partners allow countries to share best practices, refine response techniques, and build familiarity and trust between first responders and CBRN specialists.

- **Online training modules and resources.** Developing and sharing resources focused on standardized decontamination procedures provide readily accessible knowledge on CBRN preparedness, detection, decontamination, and response for national and regional stakeholders.
- **Targeted capacity building programs.** Engaging with regional and international partner countries through training, workshops, and exercises aimed at addressing identified gaps helps apply evidence-based methodologies to national challenges.
- **Foster communication.** Through regular engagements and workshops, regional and international stakeholders build relationships with one another that can be utilized in responding to a CBRN incident.
- **Encourage collaboration.** Governments, the private sector, and research institutions should work together to leverage expertise and resources for CBRN preparedness advancements. Public-private partnerships can facilitate the development of innovative technologies, efficient production of CBRN equipment, and knowledge sharing between different sectors.

International cooperation and assistance: challenges and good practices

CHALLENGES	GOOD PRACTICES
Compliance with **domestic and international laws** and regulations.	▸ Consult with legal experts to ensure **compliance** with relevant laws and regulations. ▸ Develop **clear guidelines** for the legal framework governing international assistance.
Unclear **points of contact and procedures** to request international assistance.	▸ Contact **relevant stakeholders,** such as embassies, international organizations, NGOs, and others to seek information regarding the process to request international assistance, including points of contact and requirements.
The **administrative requirements** to request or approve international assistance can slow response times.	▸ **Pre-establish agreements** and simplify the approval process to expedite requests for international aid. ▸ Use **pre-prepared templates** for rapid and comprehensive documentation of needs during incidents.
Governments or organizations may be hesitant to accept international aid due to concerns over **sovereignty or dependency.**	▸ **Foster relationships** with international partners through regular meetings, joint exercises, and transparent communication. ▸ Promote **mutual benefits** by highlighting how international collaboration strengthens national and regional capabilities.

3.5 ESTABLISHING A CBRN TRAINING PROGRAMME

Effectively managing CBRN risks requires training, including strategic-level training that empowers leaders and policymakers to navigate the complexities of evolving threats. This training extends beyond operational readiness, addressing the broader strategic imperatives of policy alignment, inter-agency coordination, and sustainable resource allocation.

At the strategic-level, training emphasizes the integration of national security goals, international obligations, and cross-sectoral priorities, ensuring coherence across all levels of preparedness and response. By focusing on the broader context – such as linking training to national CBRN response plans, international commitments, and policies related to health and environmental protection – this approach enables stakeholders to strategically align their efforts with long-term organizational and national objectives.

KEY ACTIONS

1) Development of training curriculum

Effective training in the context of CBRN planning and response is essential to ensure that relevant stakeholders are equipped with the necessary skills and knowledge to manage complex crises. The following steps outline the process of developing and delivering tailored training that is both relevant and accessible, ensuring the engagement of key stakeholders and the continuous improvement of the training materials.

The first step in developing a CBRN training curriculum is to define **clear and relevant learning objectives** that focus on the critical skills and knowledge required for effective crisis management and response to CBRN incidents. These objectives should address key areas, such as:

- Crisis management and decision-making during CBRN incidents, ensuring that participants, particularly policymakers and CBRN managers, can assess situations and make informed decisions under pressure.
- Resource allocation to ensure the efficient deployment of materials, personnel, and equipment in response to a crisis.
- Strategic planning for long-term risk management and preparedness, enabling participants to anticipate potential CBRN threats and develop proactive solutions.
- Interagency coordination and collaboration to facilitate a unified and coordinated response across multiple sectors and jurisdictions, which is critical for effective CBRN management.

The next step is to design **tailored training content** that addresses the specific needs of the target audience, including policymakers and CBRN managers. It is important to consider the following:

- **Developing accessible and relevant training materials:** It is essential to deliver training content in diverse formats to accommodate participants with varying levels of technical expertise. This could include traditional materials such as manuals, as well as multimedia formats like videos and interactive online modules. Offering multiple formats ensures that the training can be adapted to different learning styles and environments. Additionally, it is important to tailor the content to be culturally sensitive and relevant to the diverse backgrounds of participants. Customizing materials for specific regions or countries, while maintaining global relevance, enhances engagement and the effectiveness of the training.
- **Collaboration with key stakeholders:** Involving key stakeholders throughout the development of the training curriculum ensures that the content addresses the real needs of the target audience. Collaboration should include government officials, policymakers, international organizations, and CBRN experts, as their insights help align the training with national priorities and expectations. Incorporating feedback from previous workshops, exercises, and training events is also crucial for refining the materials and improving their quality and impact.
- **Continuous improvement:** To maintain relevance and impact, the training curriculum should be viewed as a dynamic, evolving tool. It is important to regularly review and update the materials to reflect new developments in international policy, scientific advancements, and lessons learned from past CBRN incidents. Additionally, integrating participant feedback after each training session ensures that the curriculum remains responsive to their needs, enhancing its effectiveness over time.
- **Alignment with international framework:** Training should also align with national security policies and relevant international frameworks ensuring that participants gain a comprehensive understanding of both domestic and international obligations in CBRN response.

Examples of a training curriculum for policymakers and CBRN managers

1. Introduction to CBRN planning and response

🏆 **Target Audience:** Entry-level policymakers, junior CBRN managers, new government officials.

☑ **Topics Covered:**

- Overview of CBRN threats and their potential impact.
- Introduction to CBRN materials and associated risks.
- Key principles of CBRN response planning and coordination.
- Overview of international conventions (e.g., Chemical Weapons Convention, Biological Weapons Convention) and national frameworks.
- Roles and responsibilities of stakeholders in CBRN preparedness and response.

2. CBRN risk assessment and vulnerability analysis

🏆 **Target Audience:** Mid-level policymakers, emergency planners, regional coordinators.

☑ **Topics Covered:**

- Identifying and assessing CBRN hazards and vulnerabilities.
- Tools and methodologies for risk assessments.
- Assessing infrastructure, population risks, and resource gaps.
- Prioritization of resources and strategies for response based on risk analysis.

3. Developing national and regional CBRN response plans

🏆 **Target Audience:** Policymakers, planners, response coordinators.

☑ **Topics Covered:**

- Developing and structuring national and regional CBRN response strategies.
- Planning for multi-agency coordination in CBRN incidents.
- Resource allocation, contingency planning, and logistics.
- Assessing national capabilities to respond to CBRN incidents.
- Legal, regulatory, and policy frameworks for CBRN response.

4. Advanced CBRN incident command and coordination

🏆 **Target Audience:** Senior CBRN managers, emergency response leaders, high-level government officials.

☑ **Topics Covered:**

- Establishing and managing the Unified Command Structure.
- Coordinating operations across multiple agencies and jurisdictions.
- Managing crisis communication and information flow.
- Balancing operational response and strategic decision-making.

5. CBRN simulation and tabletop exercises

🏆 **Target Audience:** Policymakers, response coordinators, operational managers.

☑ **Topics Covered:**

- Design and conduct CBRN tabletop exercises and simulations.
- Scenario development for CBRN incidents (e.g., chemical attacks, biological outbreaks).
- Engaging stakeholders in simulation exercises (government, law enforcement, and industry).
- After-action reviews and identifying areas for improvement.

6. Inter-agency coordination and public-private partnerships

🏆 **Target Audience:** Policymakers, regulatory officials, private sector CBRN managers.

☑ **Topics Covered:**

- Developing inter-agency SOPs.
- Best practices for public-private sector coordination in CBRN preparedness and response.
- Developing joint action plans for CBRN security and mitigation.
- Ensuring secure supply chains of dual-use chemicals and materials.
- Strategies for enhancing collaboration between government, private companies, and academia.

7. CBRN crisis communication and information management

🏆 **Target Audience:** Policymakers, communication officers, public information managers.

☑ **Topics Covered:**

- Crisis communication strategies during CBRN incidents.

- Information management protocols for inter-agency coordination.
- Dealing with misinformation, disinformation and panic during a CBRN crisis.
- Developing public messaging strategies for CBRN-related emergencies.

8. Legal, regulatory, and ethical issues in CBRN response

🏆 **Target Audience:** Policymakers, legal advisors, national security officials.

☑ **Topics Covered:**

- Legal and ethical considerations in CBRN response, including international law and national legislation.
- Liability issues related to CBRN incidents.
- Human rights concerns during CBRN response and mitigation efforts.
- The role of international cooperation and law enforcement in CBRN security.

9. CBRN recovery and restoration

🏆 **Target Audience:** Policymakers, health officials, environmental planners.

☑ **Topics Covered:**

- Planning for long-term recovery after a CBRN incident.
- Public health and environmental considerations during recovery.
- Socio-economic impact assessments and rebuilding strategies.
- Metrics for measuring recovery success and monitoring post-incident remediation.

10. Regional and international collaboration on CBRN threats

🏆 **Target Audience:** Senior policymakers, diplomats, international relations officers.

☑ **Topics Covered:**

- Frameworks for international collaboration in CBRN risk management.
- Cross-border cooperation during CBRN events (e.g., sharing resources, information).
- Coordination with international organizations such as WHO, OPCW, and UNICRI.
- Requesting international assistance.
- Promoting transparency, trust-building, and mutual assistance in CBRN preparedness.

2) Implementing and evaluating training programs

Effective training is essential to ensuring that all stakeholders involved in CBRN planning and response are prepared to fulfill their roles during a crisis. The processes of implementation and evaluation are critical to achieving this goal. Implementation involves selecting appropriate content and methodologies that align with the unique responsibilities of the target audience, ensuring that the training is relevant and impactful. Evaluation, on the other hand, ensures that the training achieves its intended outcomes, identifying areas for improvement and enabling continuous refinement. Together, these processes form the foundation of robust capacity-building efforts in CBRN preparedness, equipping stakeholders with the skills and knowledge necessary to respond effectively to crises.

Key considerations for implementing and evaluating training programs include:

- **Relevance to roles and responsibilities:** Decision-makers may benefit from strategic planning workshops and tabletop exercises that simulate crisis scenarios requiring high-level judgment and coordination. On the other hand, first responders may need hands-on simulation drills to practice operational procedures under realistic conditions. Selecting the appropriate methodology ensures that stakeholders receive training tailored to their roles, allowing them to effectively contribute to a coordinated response.
- **Learning preferences and context:** The appropriate methodology should consider how stakeholders learn best and the specific context in which the training will be applied. For instance, interactive methods like simulation drills and joint exercises engage participants by recreating real-world challenges, while classroom sessions are more suited for delivering foundational knowledge. Incorporating diverse methodologies ensures inclusivity and addresses varying learning styles.
- **Practical feasibility:** The choice of methodology has also practical implications. While simulation drills provide unparalleled realism, they are resource-intensive and may not always be feasible. In such cases, a combination of classroom sessions and tabletop exercises can achieve training objectives with fewer resources. Striking a balance between impact and feasibility is key to designing effective training.

The table below explores different training methodologies, their advantages and disadvantages, and the evaluation approaches needed to assess the impact and effectiveness of training initiatives.

CLASSROOM SESSIONS:

Traditional training method focused on delivering foundational knowledge about CBRN planning and response strategies through lectures, presentations, and discussions.

Advantages

- **Foundational knowledge:** This method provides stakeholders with essential theories and principles needed to understand CBRN incident management.
- **Structured learning:** Offers a well-organized approach with clear explanations of complex topics and opportunities for engagement through discussions and questions.
- **Cost-effective:** Typically requires fewer resources compared to other hands-on methods, making them a more economical option for basic training.

Disadvantages

- **Limited practical application:** While effective for imparting theoretical knowledge, classroom sessions offer limited opportunities for stakeholders to practice skills in real-world scenarios.
- **Engagement challenges:** Depending on the format, classroom sessions can sometimes can be passive, reducing engagement, particularly for decision-makers who may prefer more hands-on activities.

TABLETOP EXERCISES (TTX):

Discussion-based exercises in which stakeholders collaboratively assess and respond to simulated CBRN scenarios. These exercises are conducted in a low-risk, controlled environment, making them ideal for planning and decision-making.

Advantages

- **Scenario-based learning:** Simulates real-world situations, allowing stakeholders to practice decision-making and problem-solving without operational risks.
- **Promotes critical thinking:** Encourages strategic analysis, collaboration, and problem-solving, which are essential for policymakers and managers.
- **Flexible and adaptable:** Easily customized to address specific cbrn scenarios and the needs of different stakeholders.

Disadvantages

- **Limited realism:** Lacks the hands-on, practical experience of responding to an actual incident, which can limit their ability to fully test operational responses.
- **Time-consuming:** Designing and conducting TTXs can require significant time and effort, as scenarios must be thoroughly researched and stakeholders must dedicate time to participate.

SIMULATION DRILLS:

Hands-on exercises that replicate real-world CBRN scenarios, requiring stakeholders to actively engage in managing a simulated crisis.

Advantages

- **Realistic experience:** These drills provide stakeholders with hands-on experience, allowing them to test and refine their response protocols in a dynamic, realistic environment.
- **Improved interagency coordination:** Simulation drills bring multiple agencies together to practice working as a cohesive unit, enhancing communication and coordination during actual incidents.
- **Immediate feedback:** Participants receive direct feedback on their actions, helping to identify both strengths and areas for improvement.

Disadvantages

- **Resource-intensive:** Simulation drills require significant resources, including equipment, personnel, and facilities, making them expensive and challenging to organize.
- **Stressful:** The high-pressure environment of realistic simulations may overwhelm some stakeholders, potentially hindering their learning process.

JOINT EXERCISES:

Large-scale, multi-agency simulations designed to practice coordinated responses to complex CBRN incidents. These exercises involve stakeholders from various sectors, including government agencies, law enforcement, and first responders.

Advantages

- **Multi-stakeholder collaboration:** Joint exercises bring together diverse stakeholders to improve collaboration and coordination across sectors during large-scale incidents.
- **Real-world crisis simulation:** They simulate large, complex CBRN incidents, providing stakeholders with experience in managing multifaceted crises.
- **Comprehensive training:** Joint exercises cover a broad range of skills, including crisis communication, resource allocation, and inter-agency leadership, offering a holistic approach to CBRN response.

Disadvantages

- **Complex coordination:** Organizing joint exercises is logistically complex and requires careful planning and coordination among numerous stakeholders.
- **High cost:** These exercises demand substantial investments in resources and personnel, making them more expensive compared to other training methods.

Evaluation is also a critical component of any training program, ensuring its effectiveness and providing actionable insights for future improvement. Without a robust evaluation framework, it is difficult to determine whether the training has met its objectives or contributed to building the desired capacity among stakeholders.

Key benefits include:

- **Measuring impact:** Evaluation helps assess whether stakeholders have gained the intended knowledge and skills. It ensures that training outcomes are aligned with organizational goals, such as improving crisis management or enhancing interagency coordination during CBRN incidents.
- **Identifying gaps:** Evaluations highlight areas where the training may be lacking. For example, participants may excel in theoretical knowledge but struggle to apply it during practical exercises. Identifying such gaps allows for targeted improvements in the curriculum.
- **Demonstrating accountability:** For organizations investing resources in CBRN training, evaluations provide evidence of impact and accountability. This is especially important for securing continued funding and support from stakeholders, such as government bodies or international partners.
- **Adapting to emerging needs:** CBRN threats are dynamic, and training programs must evolve to address new challenges. Evaluation results help organizations adapt their training to include emerging risks, updated policies, and advancements in response technologies.

The process of choosing the right methodology and evaluating its effectiveness is interconnected. Evaluations can inform the selection of methodologies by highlighting what works best for specific audiences and contexts. Conversely, the choice of methodology can influence the design of the evaluation framework.

The following table outlines how different CBRN training methodologies can be evaluated, with examples of **key performance metrics** used to assess their effectiveness.

TRAINING TYPE	EVALUATION APPROACH	PERFORMANCE METRICS
Classroom sessions	Pre- and post-training assessments	**Knowledge acquisition:** Measured through tests or quizzes assessing theoretical understanding.
		Participant feedback: Evaluates the clarity and relevance of content (e.g., surveys or ratings).
		Engagement level: Measured through participation in discussions or Q&A sessions.
Tabletop exercises (TTX)	Facilitated debriefings and scenario discussions	**Decision quality:** How well decisions align with established protocols or best practices.
		Collaboration: Assessed by communication clarity, timely resource sharing, and effective problem-solving.
		Strategic thinking: Measured through the ability to consider long-term consequences of decisions.
Simulation drills	Performance metrics and real-time observation	**Response time:** How quickly participants respond to simulated CBRN incidents.
		Interagency communication: Assessed through coordination, clarity, and accuracy of information shared.
		Adherence to protocols: Assesses how well participants follow operational procedures under stress.
		Stress management: Evaluates participants' ability to make decisions under pressure.
Joint exercises	Post-exercise analysis and feedback from all stakeholders	**Collaboration and coordination:** Evaluated by how well multiple agencies interact and cooperate.
		Resource allocation: Evaluates the effective distribution and use of resources (e.g., personnel, equipment).
		Leadership effectiveness: Measures how well leaders manage teams, resolve conflicts, and direct the response.

By integrating these considerations, training programs can ensure that methodologies are not only effective during delivery but also contribute to measurable and sustained improvements in CBRN preparedness and response.

Example of a training evaluation matrix for advanced CBRN incident command and coordination

EVALUATION CRITERIA	DESCRIPTION	MEASUREMENT METHOD	SCALE/RATING	PURPOSE OF EVALUATION
Relevance of training topics	The training topics align with the needs and challenges of the target audience.	Participant feedback surveys or pre/post-training assessments	1 (Not Relevant) to 5 (Highly Relevant)	Assess if the topics address the real needs and challenges faced by the target audience.
Clarity of objectives and expectations	Clarity in understanding the objectives of the training and expected outcomes.	Participant feedback surveys, facilitator observation	1 (Unclear) to 5 (Very Clear)	Evaluate if participants understand the purpose and goals of the training.
Effectiveness of scenario-based learning	Use of simulations or exercises that reflect real-world situations and challenges in CBRN response.	Participant surveys, facilitator observation, group discussions	1 (Ineffective) to 5 (Highly Effective)	Assess how well the training uses practical scenarios to reinforce learning and decision-making.
Quality of instruction	The expertise and delivery of trainers, and how well they engage participants.	Participant feedback surveys, instructor evaluations	1 (Poor) to 5 (Excellent)	Evaluate the competence and effectiveness of the trainers in delivering the content effectively.
Coordinating multi-agency operations	Effectiveness of teaching how to coordinate between agencies during a CBRN incident.	Pre/post-training assessments, practical scenario feedback	1 (Unclear) to 5 (Very Clear)	Assess how well participants understand cross-agency coordination and its application.
Crisis communication and information flow	Participants' understanding of crisis communication management in multi-agency settings.	Participant surveys, role-play feedback	1 (Poor Understanding) to 5 (Excellent Understanding)	Evaluate the clarity and usefulness of communication strategies taught during the training.
Balancing operational and strategic decisions	Ability of participants to balance tactical operations with strategic objectives.	Simulation/role-play observations, post-training assessments	1 (Unclear) to 5 (Very Clear)	Assess how well the training prepares participants to make effective decisions under pressure.

EVALUATION CRITERIA	DESCRIPTION	MEASUREMENT METHOD	SCALE/RATING	PURPOSE OF EVALUATION
Engagement and interaction	Level of participant interaction, engagement, and collaborative learning.	Participant surveys, group activity participation.	1 (Not Engaging) to 5 (Highly Engaging)	Measure the level of participant involvement and collaboration throughout the training.
Usefulness of training materials and resources	Appropriateness and quality of materials provided, such as handouts, guides, and visual aids.	Participant feedback surveys, material evaluation forms.	1 (Poor Quality) to 5 (Excellent Quality)	Assess the quality and usefulness of training materials provided.
Participant confidence in applying learning	Participant confidence in applying knowledge and skills learned in their own professional roles.	Post-training assessments, participant self-assessment.	1 (Not Confident) to 5 (Very Confident)	Evaluate how confident participants feel in applying the training content to real-world scenarios.
Overall training satisfaction	Overall satisfaction with the training content, delivery, and outcomes.	Participant feedback surveys, instructor evaluation.	1 (Very Dissatisfied) to 5 (Very Satisfied)	Assess the overall experience and satisfaction of the participants.

SCORING SYSTEM FOR EVALUATION

1. **Not effective/unclear:** The training or content did not meet expectations or was ineffective in addressing the participants' needs.
2. **Somewhat effective/needs improvement:** The training met some expectations but requires refinement to be more impactful.
3. **Satisfactory:** The training was adequate, but there is room for improvement in certain areas.
4. **Effective:** The training met most of the participants' needs and expectations effectively.
5. **Highly effective/excellent:** The training fully met the objectives, was well-delivered, and highly relevant to the participants' roles.

This matrix allows for a structured and comprehensive evaluation of the training program's effectiveness, focusing on knowledge acquisition, practical skills, and the ability to perform in real-world scenarios.

3) Certification and accreditation of training

Certification and accreditation play vital roles in ensuring the quality, credibility, and long-term effectiveness of training programs. Both processes are designed to validate the knowledge, skills, and competence of individuals participating in CBRN training, while also ensuring that the training meets high standards of quality and relevance.

Certification refers to the formal recognition that an individual has successfully completed a training program and has demonstrated the necessary competencies required to perform tasks effectively within the context of CBRN preparedness and response. The process of certification usually includes assessments (written exams, practical evaluations, etc.) to measure knowledge acquisition and the ability to apply learned skills in real-world scenarios.

There are different types of certification based on the level of expertise:

- **Basic certification** is awarded to entry-level responders and staff involved in CBRN incident management. It covers foundational topics such as basic response strategies and the fundamentals of CBRN incidents.
- **Advanced certification** targets decision-makers and managers, focusing on more complex areas like crisis management, resource coordination, and interagency collaboration. This certification is ideal for those in leadership roles who need to make critical decisions during CBRN events.
- **Specialized certification** is designed for professionals in specific sectors such as CBRN medical response, radiological safety, or forensic investigation. This type of certification provides in-depth expertise in specialized areas, which is critical for handling specific aspects of CBRN incidents effectively.

A significant component of making CBRN training sustainable is the **Train-the-Trainer (TTT) Certification.** This program certifies individuals to become trainers themselves, ensuring that knowledge is passed down within the organization or community, thereby creating a self-sustaining cycle of expertise.

The benefits of certification extend beyond formal recognition. It encourages deeper engagement from participants by motivating them to perform well, as it often leads to career advancement and increased recognition in the field. Additionally, many certification programs require ongoing professional development or recertification, fostering a culture of continuous learning and improvement.

On the other hand, **accreditation** focuses on ensuring that the training programs themselves meet established standards of quality and effectiveness. Accreditation is typically granted by recognized bodies—either national or international—that evaluate the training curriculum, delivery methods, and the qualifications of instructors.

Accredited programs adhere to strict **quality assurance** processes, ensuring that the content is accurate, up-to-date, and well-structured to provide meaningful learning experiences. Moreover, accreditation offers **global recognition,** adding credibility to the program and ensuring that participants and employers trust the quality of the training.

4) Making training sustainable

Sustainability is crucial for ensuring that CBRN training initiatives have a long-term, meaningful impact. A sustainable training program allows stakeholders to continuously build and update their knowledge, ensuring that the skills and capabilities gained remain relevant as CBRN threats evolve. To achieve this, it is essential to establish mechanisms that promote ongoing learning, build local capacity, and facilitate the sharing of best practices. Strategies for sustainability include implementing Train-the-Trainer (TTT) programs, collaborating with training institutions, and leveraging international networks for ongoing support.

There are some strategic elements for sustainable training to be considered:

- **Develop a cadre of trainers:** Identifying local experts and practitioners who can be trained to become trainers themselves ensures that knowledge is passed down within the community. These trainers can then deliver training programs to other stakeholders, expanding the reach and impact of the initiative. By training local personnel, training becomes more culturally relevant and adaptable to local contexts.
- **Partner with established training academies:** Collaborating with national or international training organizations or regional training hubs, can provide formal certification and accreditation for training participants. This partnership helps maintain the quality of training and aligns it with international standards, making the training program more credible and widely accepted.
- **Create ongoing learning opportunities:** Setting up a network of trained professionals ensures that learning does not stop after the completion of a training program. These professionals can share updates, lessons learned, and best practices, fostering continuous improvement and collaboration. Ongoing learning opportunities could include webinars, workshops, or regular conferences where stakeholders discuss emerging CBRN threats and evolving response strategies.
- **Establish a framework for continuous evaluation and improvement:** A sustainable training program should include regular feedback loops to assess its effectiveness and identify areas for improvement. Engaging with stakeholders to gather insights and evaluate the program's impact helps to refine the training, making it more responsive to changing needs. This evaluation process should be systematic and aligned with evolving CBRN challenges.
- **Collaboration with International Organizations:** Partnering with international organizations ensures that training stays aligned with global standards. For example, working with IAEA, ECDC, OPCW, UNICRI, WHO, or other relevant bodies ensures that the training content incorporates the latest research and best practices in CBRN planning and response.
- **Certification is a key component of making CBRN training sustainable:** It not only serves as a formal acknowledgment of the knowledge and skills acquired but also incentivizes participants to engage more deeply with the training program. Certification can take various forms, including formal certificates awarded by recognized national or international training academies or through Train-the-Trainer (TTT) programs that designate qualified individuals to train others.

Establishing a CBRN training program: challenges and good practices

CHALLENGES	GOOD PRACTICES
Stakeholder engagement is crucial to ensure the training program is aligned with organizational or national priorities. Lack of clear engagement can lead to misaligned goals or insufficient support for the program.	▸ **Early involvement of stakeholders** through workshops, meetings, and focus groups to ensure shared understanding of training goals. Regular engagement is key to aligning expectations and fostering commitment.
Trainers can leave their positions causing a **loss of institutional knowledge, expertise, and continuity,** which can significantly hinder the development and sustainment of robust CBRN planning and response capabilities.	▸ Develop **a pool of trainers ("Train-the-Trainers" programs)** and maintain a database of trained personnel to track available trainers and their qualifications. ▸ Establish clear procedures for **knowledge transfer** in case trainers leave, including detailed documentation of training materials, lesson plans, and methodologies. ▸ Use **mentorship programs** where outgoing trainers mentor their replacements during a transition period. ▸ Develop and maintain **online training modules, videos, and virtual reality simulations** to standardize and preserve training content. ▸ Create a **unified, standardized curriculum for CBRN training** that includes lesson plans, exercises, and assessment tools. ▸ **Retention strategies** for trainers including competitive salaries, benefits, and opportunities for career advancement. ▸ Establish a **national CBRN training framework** that outlines the long-term strategy for recruiting, training, and retaining CBRN trainers.
Incomplete or inaccurate data can result in misidentifying training needs or priorities. It is essential to ensure that data collection methods are diverse and validated for comprehensive insights.	▸ Use a **multi-method approach** (surveys, interviews, focus groups, job task analysis) and cross-check data from different sources to ensure its reliability. ▸ Include **feedback loops** to validate findings.
Resistance to change can occur if the need for training is not clearly articulated or understood. Involving key stakeholders early on ensures their support and helps mitigate resistance.	▸ Demonstrate the value of the training through **real-world case studies** and show how it aligns with broader organizational goals. ▸ Engage stakeholders in the **planning phase** to gain buy-in.

CHALLENGES	GOOD PRACTICES
Financial and logistical constraints are a common challenges in implementing large-scale training programs. Prioritizing resources helps focus on the most critical areas while exploring cost-effective solutions.	▸ Prioritize training based on **risk assessments and available resources.** ▸ Consider **phased implementation** and explore external funding sources or partnerships to support training.
The **fast-evolving nature of CBRN threats** means training needs can quickly become outdated. Regular updates and focus on emerging threats ensure that training remains relevant and timely.	▸ Conduct thorough **risk assessments** using tools like risk matrices to evaluate and prioritize CBRN threats. ▸ Regularly **update training needs** based on feedback from past incidents and exercises.
Training that does not align with international frameworks or national policies may lack credibility or fail to meet regulatory requirements. Aligning content ensures consistency and applicability.	▸ Ensure training content **aligns with international guidelines** (e.g., IAEA, OPCW, WHO) and national policies. ▸ Incorporate **lessons learned** from international case studies and best practices.
Engaging participants is crucial for **effective learning and knowledge retention.** Traditional lecture-based training may not be as engaging, so adopting more interactive and diverse training methods is key.	▸ Use **interactive training formats** (scenario-based exercises, case studies) and blended learning methods to appeal to different learning styles. ▸ Tailor content to **participants' roles** for maximum relevance.
Without proper **evaluation**, it is difficult **to measure the effectiveness of training.** Pre- and post-training assessments ensure that participants have gained the required knowledge, while performance-based evaluations gauge real-world effectiveness.	▸ Implement **pre- and post-training assessments**, as well as performance-based evaluations such as simulations. ▸ Use **KPIs** (e.g., response times, inter-agency coordination) to track improvements.
CBRN incidents often involve multiple agencies, and poor coordination can hinder response efforts. Training that **emphasizes inter-agency collaboration** prepares participants for coordinated efforts during real-world crises, fostering a better understanding of each agency's role and responsibility.	▸ Design training to include **multi-agency coordination exercises**, role-playing, and real-world collaboration scenarios. ▸ Focus on how **each agency's responsibilities align** and how they coordinate during a CBRN incident. ▸ Emphasize **joint decision-making** and **resource allocation** across agencies.

CHALLENGES	GOOD PRACTICES
Without proper **tracking and reporting,** it is difficult to assess whether the training is delivering the intended results. Using KPIs allows for measuring the real-world impact of training efforts and justifying resource allocation.	▸ Implement a robust **system for monitoring and evaluating training,** using KPIs and performance metrics (e.g., response time improvements). ▸ Regularly **report on the progress** of training outcomes.
CBRN threats require **specialized knowledge.** Without experts to guide the training, the program might lack depth or miss important details. Partnering with specialists helps ensure high-quality content.	▸ **Bring in CBRN experts** to design and deliver the training, and partner with international organizations to access specialized knowledge.
Cultural and organizational differences can affect the effectiveness of training. Ensuring content is relevant and culturally appropriate makes it more accessible and engaging for participants.	▸ Adapt training materials and scenarios to **local contexts and organizational structures.** ▸ Consider **cultural sensitivities** when designing content to ensure it resonates with participants.

Section 2

Response

The **response phase** is the critical period immediately following a CBRN incident, during which the plans developed in the planning phase are activated and implemented. This phase involves unified leadership, rapid mobilization of resources, implementation of emergency protocols, and coordinated interagency efforts to minimize the impact of the incident. Response activities focus on saving lives, preventing further damage, and containing the CBRN threat.

Emergency response to CBRN incidents requires a structured and systematic approach to decision-making. A well-prepared response framework enhances interoperability between agencies, ensuring that all stakeholders understand their roles and responsibilities in crisis situations.

Effective response efforts rely on pre-established communication channels and information-sharing mechanisms to facilitate swift coordination. Additionally, continuous training and simulation exercises strengthen preparedness by allowing responders to test and refine emergency procedures in realistic scenarios. The process incorporates essential elements of emergency management including **assessment, resource allocation, communication with the public, and investigation,** while providing clear pathways for escalation to national resources when local resources become overwhelmed. This operational framework ensures a coordinated and efficient response while maintaining flexibility to adapt to various types and scales of CBRN incidents

The following flowchart illustrates a structured approach to managing a CBRN incident. The process begins with the deployment of first responders to **assess the situation**. If the incident is successfully resolved at this stage, the response phase concludes.

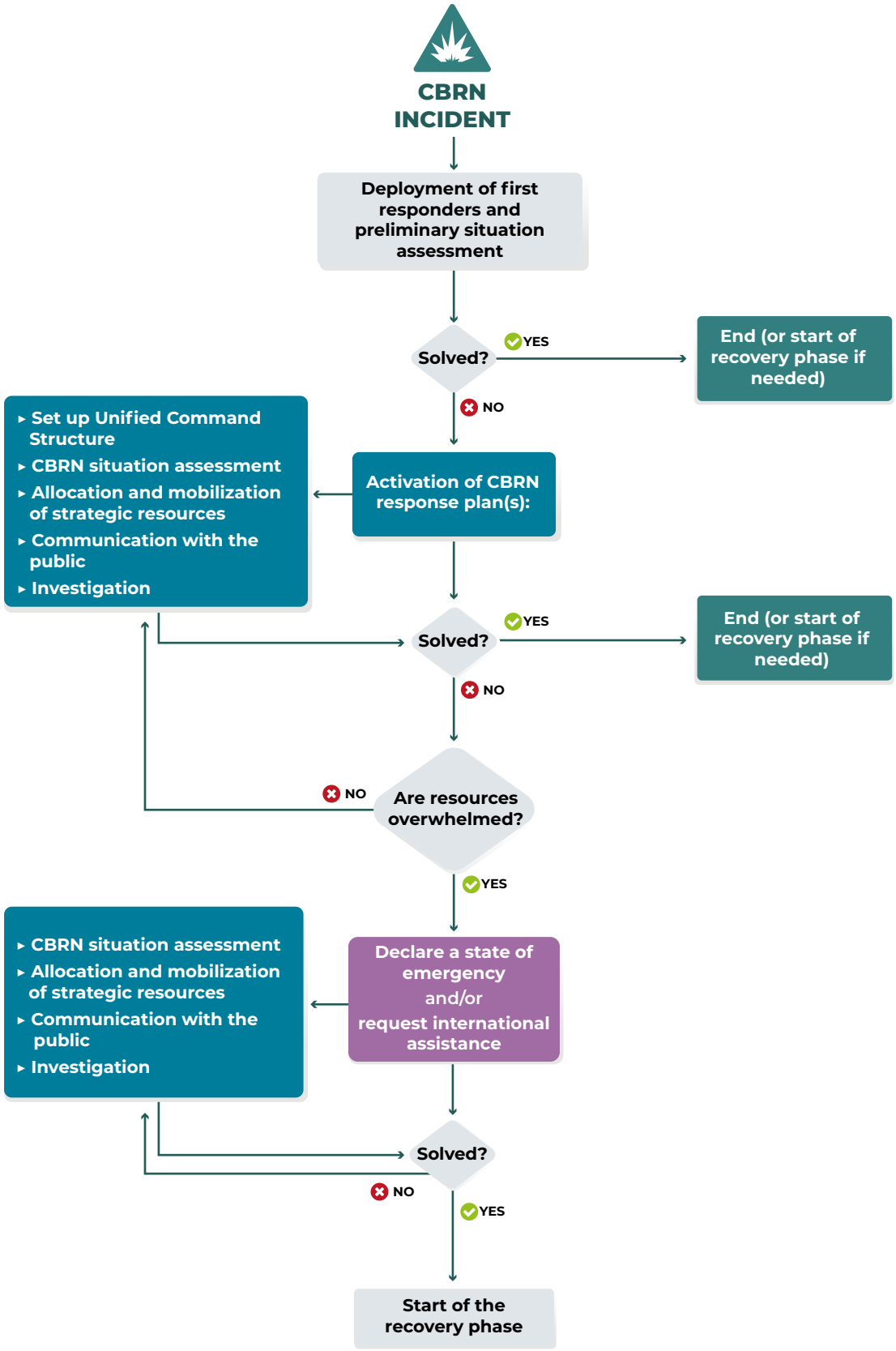
If the situation remains unresolved, a **Unified Command Structure** is established to coordinate the response. At this point, the CBRN **response plan(s)** is activated.

These plans rely on information gathered during the initial assessment to **allocate resources, implement public communication strategies,** and initiate **investigation and intelligence-gathering** activities as the situation evolves.

If available resources are insufficient to manage the incident, authorities may declare a **state of emergency and/or request international assistance.** The response phase may involve multiple cycles of assessment, resource allocation, communication, and investigation until the incident is brought under control. Once the immediate threat is mitigated, the response transitions into the recovery phase.

The flowchart serves as a practical guide for CBRN managers and responders, supporting informed decision-making throughout the crisis. It underscores the importance of continuous assessment and adaptability, highlighting the potential escalation from localized incident management to full-scale emergency response with international support.

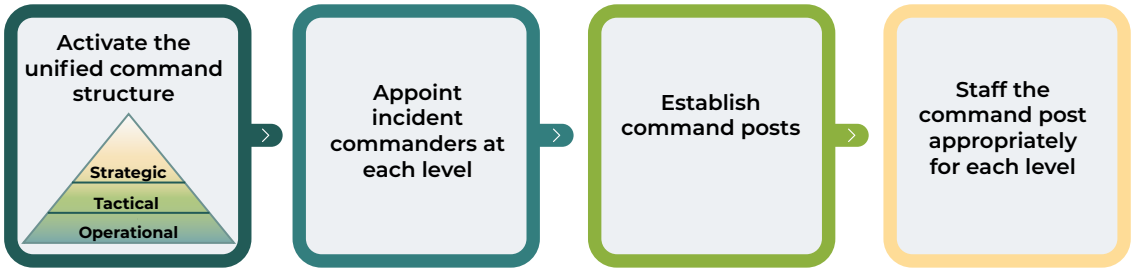
Response phase



1. UNIFIED COMMAND AND COORDINATION

The Unified Command Structure (UCS) plays a critical role in responding to CBRN incidents by facilitating coordinated efforts among multiple agencies and organizations, ensuring effective communication, streamlined decision-making, and efficient resource allocation during complex emergencies.

KEY ACTIONS



1) Activate the unified command structure

The Unified Command Structure is activated immediately upon the identification of a suspected or potential CBRN incident, based on pre-defined activation thresholds. This timely activation enables rapid mobilization of resources, alignment of inter-agency coordination, and seamless integration of operational efforts. Once activated, the UCS can operate at one or all of the three management levels – strategic, tactical, and operational – depending on the scale and complexity of the incident. Its flexible structure enables it to expand as the situation evolves, ensuring the response remains efficient, coordinated, and aligned with incident demands.

2) Appoint incident commanders at each level

Incident Commanders are designated from a pool of pre-identified candidates, based on the scale, complexity, and evolving operational needs of the incident. Initially, the role is typically assumed by the most senior responder on the scene, who is responsible for stabilizing the situation and coordinating immediate actions. As the incident progresses, the Incident Commander role may transfer to higher-ranking officials or specialized experts to address the increasing complexity of operations. This flexible approach ensures that leadership remains aligned with the scope and complexity of the response, maintaining effective oversight across strategic, tactical, and operational levels.

In large-scale CBRN incidents, Incident Commanders are typically appointed at each level of the response hierarchy (strategic, tactical and operational). Each level has a progressively broader scope and longer-term focus, with formal decisions and resource requests flowing through the established chain of command to ensure coherence and accountability throughout the response.

Their roles and responsibilities are as follows:

LEVEL	COMMANDER	KEY RESPONSIBILITIES
Strategic	Strategic commander	▸ Oversees the CBRN response effort at national/ regional level ▸ Sets overall policy and strategic direction ▸ Manages high-level resource allocation and coordinates with government officials ▸ Makes decisions on large-scale evacuations, public communications strategies, and international assistance requests ▸ Ensures alignment of the response with national security and public health objectives
Tactical	Tactical commander	▸ Implements the decisions made the strategic-level and reports to the Strategic Commander ▸ Coordinates the overall response effort across multiple agencies and jurisdictions ▸ Develops tactical plans and ensures their implementation ▸ Manages resource distribution among different operational areas ▸ Serves as the primary link between strategic decision-making and on-scene operations ▸ Oversees the establishment and operation of decontamination sites, medical triage areas, and safety perimeters
Operational	Operational commander	▸ Directs immediate response activities at the incident site and reports to the Tactical Commander ▸ Implements plans developed at the tactical-level, adapting to real-time conditions, as needed ▸ Coordinates the activities of various response teams (e.g., HAZMAT, medical, law enforcement) ▸ Ensures adherence to safety protocols for responders and the public in the immediate area ▸ Provides regular situation updates to the Tactical Commander ▸ Makes decisions regarding immediate life-safety issues

3) Establish command posts

Command posts serve as critical coordination and decision-making hubs during a CBRN response. These physical or virtual locations are aligned with the strategic, tactical, and operational levels of the UCS, enabling each level to focus on its respective responsibilities. The separation of command posts supports more effective decision-making, resource allocation, and operational oversight, while also ensuring safety and accessibility. The locations and configurations of command posts should remain flexible, adapting as needed to evolving circumstances to maintain operational effectiveness and responder safety.

The following table can be used as a reference to establish the command posts:

LEVEL	LOCATION	SAFETY	ACCESSIBILITY	COMMUNICATION
Strategic-level command post	Pre-established, secure government facility or emergency operations center, far from the incident site	Not directly impacted by CBRN threat	For high-level officials, strict security measures are typically put in place	Robust, redundant communication systems are implemented to maintain contact with all levels and external agencies
Tactical-level command post	Closer to the incident site than the strategic-level Command Post, but still at a safe distance. Often mobile or semi-permanent	Should consider potential expansion of the CBRN threat, but remains outside immediate danger	Needs good access for mid-level managers and logistics, with moderate security measures	Requires strong communication links with both strategic- and operational-level command posts
Operational-level command post	Nearest to the incident site, but outside the immediate danger zone	Immediate physical security from CBRN threat is a priority	Easily accessible for first responders and operational teams	Direct communication links to the tactical-level post and in-field teams

4) Staff each level of the command post

Each command level requires specific personnel to ensure effective management and coordination during a CBRN incident. Staffing remains flexible at all levels, adapting to the nature and evolving needs of the incident. This approach ensures that roles and resources are allocated appropriately—avoiding duplication or delay—based on real-time threat assessments and operational demands.

The following table can be used as a reference for staffing requirements at each command post level:

COMMAND POST LEVEL	STAFFING REQUIREMENTS
Strategic-level command post	▸ High-level decision-makers (e.g., senior government officials, agency heads) ▸ Representatives from key agencies (e.g., Emergency Management, Public Health, Defense) ▸ Policy advisor(s) and legal counsel(s) ▸ Senior communications and public relations staff ▸ Intelligence and security analysts ▸ Liaison officers for international coordination (if applicable) ▸ Logistics and resource management specialists ▸ Senior scientific and technical advisors with CBRN expertise
Tactical-level command post	▸ Incident commanders with CBRN response experience ▸ Scientific and technical experts in CBRN materials and their effects ▸ Representatives from various response agencies (e.g., Fire Department, Police, and Emergency Medical Services) ▸ Logistics and resource allocation specialists ▸ Communication and information management personnel ▸ Safety officers ▸ Planning managers for developing and updating incident action plans ▸ Operations managers for coordinating response activities ▸ Liaison officers for inter-agency coordination
Operational-level command post	▸ On-scene commander (typically a senior first responder with CBRN training) ▸ HAZMAT team leaders and members ▸ Medical response team leaders (e.g., paramedics and emergency physicians) ▸ Law enforcement officers for security and evacuation management

COMMAND POST LEVEL	STAFFING REQUIREMENTS
	▸ Fire department personnel for containment and rescue operations ▸ Decontamination team leaders and members ▸ Field communication specialists ▸ On-site safety officers ▸ Logistics coordinators for immediate resource needs ▸ Environmental monitoring specialists

Unified command and coordination: challenges and good practices

CHALLENGES	GOOD PRACTICES
Not **adapting the command structure** as the incident grows or changes and, when necessary, transferring leadership to a different agency, can delay response.	▸ Design a **flexible modular command structure,** that can be easily expanded or contracted to match the scale and complexity of the incident, ensuring clear communication and seamless coordination between agencies at all levels of response. ▸ Practice **scenario scaling,** conducting training exercises that simulate incidents of varying sizes and complexities. This allows teams to adapt the command structure and transition leadership roles as the situation evolves.
Lack of **effective leadership** in case of changes of the UCS or the Strategic Commander during a CBRN incident can lead to a loss of critical knowledge during transitions.	▸ **Early planning and having a succession strategy,** ensuring that pre-agreed plans detail the steps for transition of responsibilities, the timeline, and the preparation required. ▸ Ensure **transparent communication** on the transition of responsibilities to all affected parties. ▸ Ensure that the **incoming leader** is fully informed and up to date by the outgoing leader.
Lack of **specialized CBRN knowledge** among some command staff can put responders and public at risk.	▸ Integrate **CBRN experts** into the command structure. Provide ongoing **training and exercising.** Regularly deliver targeted training programs and simulation exercises to ensure command staff maintain up-to-date specialized CBRN knowledge, enhancing their ability to make informed decisions during incidents.

2. CBRN SITUATION ASSESSMENT

A CBRN situation assessment is a systematic, continuous, and comprehensive evaluation of conditions, hazards, and risks during a CBRN incident. The goal of the assessment is to provide responders and decision-makers with accurate, timely, relevant, and actionable information to manage the incident effectively, protect the population, and mitigate the impact across affected areas.

Conducted in real-time or near real-time, this ongoing assessment is incident-specific and provides immediate and constant information to guide response efforts, protect lives, contain the threat, and mitigate immediate consequences. The assessment is updated regularly based on the evolving situation, including the effectiveness of ongoing response actions.

The CBRN situation assessment differs from the risk assessment described in the Chapter 1 Risk assessment of the Planning Section, which is designed to inform national response plans and related SOPs.

Initial assessments of the CBRN incident are typically conducted by first responders at the incident scene, providing critical information for immediate action. However, CBRN incidents often involve hazards that are not immediately detectable, such as viruses, radioactive material, or chemical agents. Given the complexity of these threats, a multi-level assessment process is essential to determine severity, scale, and risk accurately.

As assessment data originates from various sources and experts, clearly defined internal communication protocols are vital. Without them, conflicting assessments could emerge, leading to uncoordinated or ineffective responses. Therefore, a comprehensive CBRN situation assessment must be initiated at the level of the Unified Command Structure, involving structured collaboration among first responders, CBRN specialists, government agencies, and other relevant stakeholders. This integrated approach ensures that both on-the-ground observations and expert analysis inform strategic response decisions.

The CBRN situation assessment is crucial for:

- **Identifying the type and source of the threat** including its origin and nature (e.g., accidental release or intentional attack).
- **Assessing the immediate and long-term impact of the incident** on public health, safety, infrastructure, the environment, and the economy.
- **Determining the resources required for response and recovery operations,** including personnel, survey equipment, specialized decontamination equipment, and medical supplies.
- **Providing actionable information** to support tactical and strategic decision-making to guide effective response and recovery actions.
- **Providing clear and timely updates to the public,** responders, and other stakeholders.
- **Providing comprehensive reports** to decision-makers and relevant authorities for further action and planning.

KEY ACTIONS

1) Activate an inter-agency group responsible to assess the CBRN incident

The activation of the inter-agency group is initiated by the Unified Command leadership following the initial assessment conducted by first responders. The activation takes place when a potential or confirmed CBRN incident poses significant risks and/or presents inherent complexities that demand extensive, multi-disciplinary expertise.

Functioning as an integral component of the Unified Command Structure, the inter-agency group provides expert advice, supports decision-making, and facilitates coordination across sectors.

The group is composed of representatives from relevant agencies and experts, including—but not limited to—government ministries, public health authorities, environmental agencies, specialized response teams, CBRN subject matter experts, military authorities, law enforcement agencies, and intelligence services (particularly in cases of suspected intentional incidents).

2) Ensure the timely and accurate collection of data

The group gathers information from multiple sources, such as:

SOURCE	TYPE OF DATA
Field assessment	On-site observations, immediate impact reports, risk assessments
Laboratory analysis	Agent/material identification, concentration levels
Environmental monitoring	Air quality, water contamination levels
Public health information	Hospital admissions, symptom reports
Open-Source Intelligence (OSINT)	Social media reports, news updates, satellite imagery, mapping and Geographic Information Systems (GIS)
Government reports	Official statements, inter-agency communications
Satellite imagery	Geographical spread, visible environmental impacts
Expert consultations	Specialized insights, risk projections
Actions taken	Chronological log of response activities, resource deployment, outcomes of implemented measures

3) Analyze data and prioritize the most critical information

The group should initially prioritize information that directly affects safety and response effectiveness—such as the identification of the agent or material, the rate of contamination spread or progression, the severity and scale of the incident, populations at risk, resource availability, and the status of containment efforts.

A range of analytical tools and methods can be employed, including direct observation and detection, laboratory analysis, risk and hazard modeling (which may incorporate scenario development, weather patterns, and population factors), field reports, and expert interpretation.

4) Produce regular situation assessment reports

The group should regularly produce CBRN situation assessments. These reports provide a structured approach to present assessment findings, ensuring that all critical information on the evolving situation is included and easily accessible to all involved agencies. It is recommended to establish a standardized reporting format for presenting the CBRN situation assessment information, ensuring consistency, completeness, and clarity across different reports and time periods.

Information typically included in a CBRN situation assessment includes:

CATEGORY OF INFORMATION	KEY INFORMATION ELEMENTS
Incident basics	▸ Time and location ▸ Type of CBRN agent/material (if known) ▸ Source/cause (if known) ▸ Location of the incident
Current status	▸ Affected area/perimeter ▸ Current and forecasted weather conditions ▸ Observed symptoms/effects ▸ Detection and survey equipment readings/measurement ▸ Current hazard levels (low, medium, high)
Population and environmental profile	▸ Population density and demographics of the affected area ▸ Identification of vulnerable groups (e.g. elderly or disable persons, and children) ▸ Health considerations and access to medical care ▸ Key environmental factors, including infrastructure and evacuation routes

CATEGORY OF INFORMATION	KEY INFORMATION ELEMENTS
Impact assessment	▸ Number of casualties: confirmed fatalities, critical condition (life-threatening), non-critical conditions, and uninjured (evacuated safely) ▸ Disruption to critical infrastructure (e.g. hospitals, power grids, and water supplies) ▸ Evacuated areas ▸ Environmental impact (contamination of air, water, and soil)
Hazard/risk modelling and projection	▸ Results of hazard and risk modelling ▸ Evaluate scenarios and expected outcomes. ▸ Potential routes of exposure (through which CBRN agent may affect humans, animals or the environment)
Response status	▸ Resources deployed ▸ Actions taken ▸ Protective measures in place ▸ Decontamination status (if needed) ▸ Response coordination ▸ Public communication
Ongoing needs and challenges	▸ Priority actions ▸ Required resources (human, equipment, medical supplies, infrastructure, etc.) ▸ Challenges that have hindered response efforts ▸ Possible gaps in data, analysis, or resource availability

5) Continuously reassess and update the situation assessment

A CBRN incident is constantly evolving. The group should regularly review the situation assessment to ensure informed decision-making at all levels. By analyzing the latest information, necessary adjustments can be made to the overall approach and plans for managing the CBRN incident.

Below is an example of a CBRN situation assessment report for a fictionalized CBRN terrorist attack involving chemical weapons at a hotel:

CBRN Situation Assessment Report

Date: 04 December 20xx

Time of Incident: 14:30

Time of this Report: 16:00

Incident overview:

- **Location:** Hotel Riverside, 114 Main Street, Circular City - 3rd floor conference center. Confined space with approximately 100 attendees
- **Time:** 14:30, during international business conference
- **Agent:** Chemical (unidentified); suspected nerve agent (symptoms align with sarin but have not been confirmed)
- **Origin of the Incident:** Believed to be intentional chemical attack based on casualty pattern and witness reports
- **Affected Area:** Hotel interior, possible outdoor contamination. Hotel ventilation system potentially spread the agent to adjacent rooms, floors, and buildings
- **Weather:** 26-28°C, 80-90% humidity, cloudy with light rain; similar forecast for 24h

Current situation:

1. **Impact assessment:**

- 30+ casualties in conference room
- 10+ secondary casualties (hotel staff/guests)
- Contamination contained mainly to 3rd floor
- Heating, ventilation, and air conditioning (HVAC) system possibly contaminated
- Multiple floors potentially affected through ventilation
- High-risk to first responders and surrounding population
- Potential for secondary devices or additional attacks being considered
- Risk of contamination spread through evacuees

2. Current response status:

- Hotel evacuation in progress
- First responders operating in Level A PPE
- Triage area established in parking lot adjacent to hotel on 100 block of Main Street
- Hotel ventilation system shut down
- Building access controlled
- Local hospitals notified and preparing
- Antidote cache deployed
- Specialized CBRN teams en-route
- Mobile decontamination units setting up

3. Critical concerns:

- Unknown number of exposed people who left scene
- Agent migration through building heating, ventilation, and air conditioning (HVAC) systems
- Multiple nationalities involved (diplomatic implications), including high-profile victims
- Potential for delayed symptoms
- Local emergency services overwhelmed
- Specialized medical care and transportation resources strained
- Insufficient PPE and antidotes for responders

4. Immediate priorities:

- Contain the spread of the chemical agent
- Evacuate exposed individuals
- Implement decontamination procedures
- Secure building access/egress
- Track conference attendee list
- Establish victim registry
- Secure and preserve crime scene integrity and potential exhibits
- Control information flow
- Apprehend or neutralize alleged perpetrators

CBRN situation assessment: challenges and good practices

CHALLENGES	GOOD PRACTICES
Incomplete or uncertain information can impact response decisions.	▸ Document the **degree of trust** or certainty in the accuracy, reliability, or completeness of the information being assessed. ▸ Identify **information gaps,** particularly, highlight specific areas where information is missing or incomplete, allowing targeted efforts to close these gaps. ▸ Regularly **revise situation assessments** as new data becomes available to improve decision-making accuracy. ▸ Use **multiple information sources** to cross-verify data from independent sources to enhance reliability.
Managing **multiple information sources** can create inconsistencies or conflicts that hinder decision-making.	▸ Establish robust processes for confirming the **validity of information** from different sources. ▸ Use **uniform formats** for collecting and presenting data to facilitate comparison and integration. ▸ Clearly **identify the primary sources** for each type of information to reduce duplication and conflict. ▸ **Cross-check discrepancies** and prioritize the most reliable sources to reconcile conflicting information.
Information overload from multiple sources can make it difficult to focus on actionable intelligence.	▸ Use technology or predefined processes to sift through large datasets and **identify relevant information** by filtering it. Focus on **actionable intelligence,** prioritizing information that directly impacts decisions and response actions. ▸ **Categorize data systematically** to ensure it can be accessed and understood quickly. ▸ Prioritize **critical information streams** by allocating attention and resources to the most urgent and impactful issues.
Time pressure since decisions during CBRN incidents must often be made quickly, increasing the risk of errors or omissions.	▸ Use **standardized assessment templates** for reporting and analyzing information to streamline assessments under pressure. ▸ Focus on **critical information needs** of the situation in assessments to guide immediate decisions. ▸ Establish **clear deadlines** for updates to ensure assessments are provided consistently and in a timely manner. ▸ Have **readily available assessment instruments** or checklists to reduce preparation time during a crisis.

CHALLENGES	GOOD PRACTICES
The specialized nature of CBRN incidents means that some **data can be difficult** to understand for non-technical experts to interpret.	▸ **Involve qualified technical experts** in assessment teams to ensure accurate analysis of complex information. ▸ Use **clear, non-technical language** for key findings to translate technical data into straightforward language that can be understood by all stakeholders. ▸ Accompany raw technical readings with **expert analysis and explanations** to support decision-making. ▸ Incorporate graphs, charts, or other **visual aids** to make data easier to comprehend.
Rapidly **evolving situation,** requiring constant updates to maintain situational awareness.	▸ Implement **regular update schedule** by establishing regular intervals for refreshing and sharing updated assessments with all stakeholders. ▸ Clearly indicate the **time and date** of all information to ensure its relevance is understood. ▸ Maintain a **record of changes** to assessments over time to understand trends and adjust strategies. ▸ **Keep an archive** of previous assessments to provide context for future evaluations and decisions.
Managing **multiple information sources** can create inconsistencies or conflicts that hinder decision-making.	▸ Establish robust processes for confirming the **validity of information** from different sources. ▸ Use **uniform formats** for collecting and presenting data to facilitate comparison and integration. ▸ Clearly **identify the primary sources** for each type of information to reduce duplication and conflict. ▸ **Cross-check discrepancies** and prioritize the most reliable sources to reconcile conflicting information.
Technical limitations since systems may have inherent constraints, such as accuracy limits or maintenance issues, that impact data quality.	▸ Deploy a variety of **detection technologies** to ensure comprehensive data collection. ▸ Consider the **known weaknesses** of equipment in assessments and decision-making. ▸ Perform **regular calibration, testing, and upkeep** of detection systems to ensure optimal functionality. ▸ Have **backup detection systems** to minimize the impact of failures or shortages during critical moments.

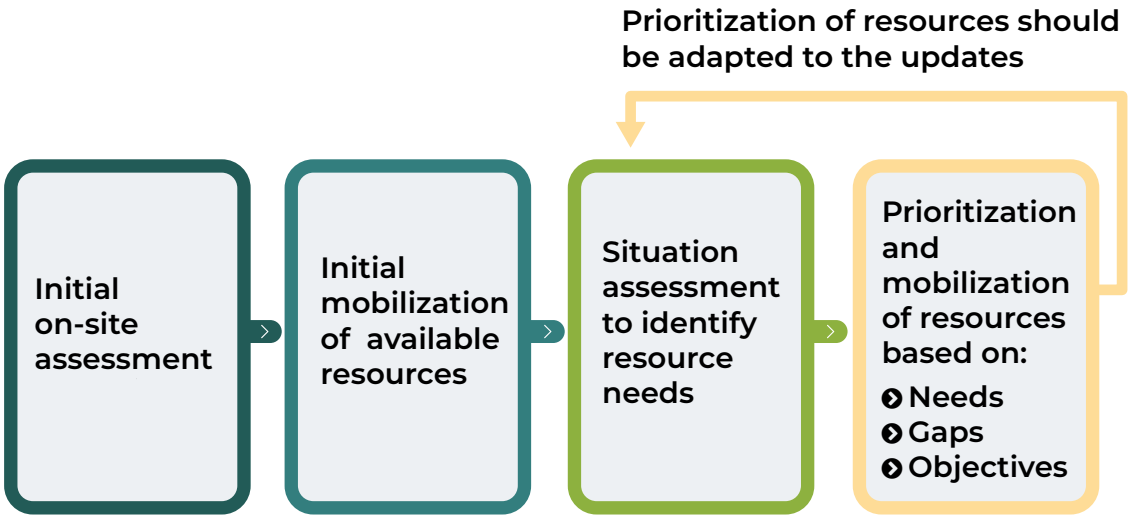
3. ALLOCATION AND MOBILIZATION OF STRATEGIC RESOURCES

A CBRN response must adapt to the specific nature of the incident. CBRN incidents are likely to overwhelm local capacities, necessitating the mobilization of resources at regional, national, or even international levels. Effective resource allocation, mobilization, and deployment are therefore critical to a successful response.

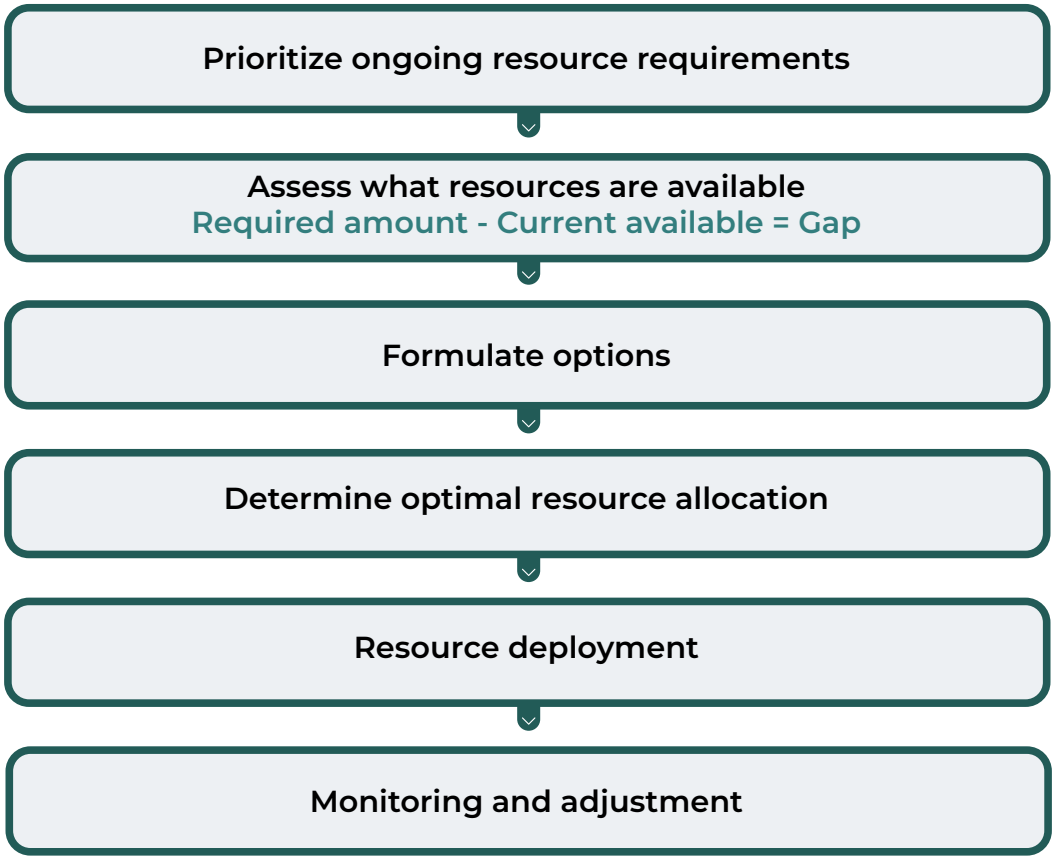
At the operational-level, the mobilization of resources is often pre-planned through established protocols and procedures (see box below). For example, when a CBRN incident occurs, local first responders such as fire departments, ambulance services, and hazardous materials teams are typically dispatched immediately. These initial response actions are usually guided by pre-existing emergency plans and standard operating procedures (see Chapter 3. CBRN response planning of the Planning Section).

However, at the strategic level, resource management and allocation involve high-level planning and decision-making that consider long-term implications, resource sustainability, and inter-agency coordination. This strategic approach ensures that resources are not only available but are also effectively utilized and distributed.

Strategic-level resource management becomes especially important during large-scale incidents that require coordination across multiple jurisdictions and extended timeframes, as it addresses broader impacts and informs decisions that shape the overall response effort.



KEY ACTIONS



1) Prioritize ongoing resource requirements

After the initial mobilization of resources, CBRN managers at the strategic level begin a more complex process of resource mobilization. This requires careful analysis of what is needed, what is available, where resources are located, and which resources should be mobilized first.

The first step is to assess ongoing resource requirements, as outlined in the CBRN situation assessment, detailed in the previous Chapter 2 CBRN situation assessment. The purpose of this assessment is to establish a **priority order** for resource mobilization.

There are several general criteria that should be considered when prioritizing resources, including, but not limited to:

- **Protecting human life,** including the CBRN responders
- **Neutralize the immediate hazard,** including the identification, isolation, and control of the CBRN hazard
- **Contain the hazard,** which includes the prevention of event escalation, stabilization of the scene, and control of the environment, and
- **Preserving infrastructure** necessary for public safety, emergency response, and community resilience (e.g., hospitals, water supplies, power stations, etc.)

Moreover, CBRN managers can use categories such as 'critical,' 'high-value,' and 'complementary' to prioritize projected needs. The following is an example of CBRN situation categorization:

CATEGORY	EXAMPLES
Critical needs (e.g., essential resources or capabilities that are urgently required and cannot be met by existing national resources)	▸ CBRN survey and identification equipment ▸ PPE ▸ Decontamination units ▸ Specialized medical treatment facilities ▸ CBRN expert teams ▸ Mass casualty management resources
High-value needs (e.g., important resources that significantly enhance the response capability but may not be critical for immediate life-saving operations)	▸ Advanced laboratory analysis capabilities ▸ Long-term environmental monitoring equipment ▸ Specialized waste management resources ▸ Public communication systems ▸ Evacuation transport and temporary shelter ▸ Psychological support teams
Complementary needs (e.g., resources that support and optimize the response effort but are not essential for core operations)	▸ Additional security personnel ▸ Logistics and supply chain management support ▸ International liaison officers ▸ Documentation and data management systems ▸ Long-term health monitoring resources ▸ Economic impact assessment teams ▸ Legal and regulatory compliance support ▸ Public education and awareness resources

To illustrate the concept of prioritizing resources, consider the example of a CBRN situation assessment report involving a terrorist group releasing a nerve agent in a conference room of a hotel (see previous Chapter 2 CBRN situation assessment). In this case, CBRN managers at the strategic-level would likely receive requests for the following types of resources:

- Additional medical personnel, including doctors, nurses, and paramedics, specialized in treating chemical exposure.
- Medical equipment, such as ventilators, oxygen tanks, and decontamination equipment.
- Mobile medical units to provide on-site treatment and triage.

- Blood banks to provide blood products for transfusion.
- Psychological support teams to address the emotional and psychological impact of the incident.
- CBRN experts to assess the extent of contamination and develop decontamination strategies.
- Forensic teams to collect and analyze evidence.
- Environmental experts to assess the environmental impact of the incident.
- Additional transportation resources, such as buses and ambulances, to evacuate and transport victims.
- Security personnel to control access to the affected area and maintain order.
- Temporary shelter for displaced individuals.
- Communication equipment to facilitate communication between responders and coordinate the response effort.
- Food and water supplies to provide sustenance for emergency responders and displaced individuals.
- Trained law enforcement personnel, special operation forces equipped to respond to terrorist incidents, and
- Intelligence agencies to gather information and track the perpetrators.

After conducting an assessment, CBRN managers can determine the priority order. The table below provides an example of how to categorize resource requests:

CRITICAL NEEDS	HIGH-VALUE NEEDS	COMPLEMENTARY NEEDS
▸ Additional medical personnel ▸ Specialized medical equipment ▸ Mobile medical units ▸ Blood banks ▸ Security personnel ▸ Forensic teams ▸ Additional transportation resources	▸ Law enforcement personnel and special operations forces ▸ CBRN experts ▸ Psychological support teams ▸ Intelligence agencies ▸ Communication equipment	▸ Environmental experts ▸ Food and water supplies ▸ Temporary shelter

2) Assess what resources are available

It is critical to understand what resources are available to address the needs. This requires a gap analysis in which strategic commanders compare available resources against prioritized needs. In other words, the assessment can be calculated as follows:

required amount - current available = gap

The result of this assessment should help CBRN managers to understand:

- what requested resources are available immediately
- what requested resources are not available immediately but can be procured at national level (e.g. national reserves, stockpiles etc.), and
- what requested resources are unavailable at the national level but can be requested through international channels (e.g., neighboring countries, international organizations, etc.).

Considering that decisions are often made rapidly, strategic commanders must frequently assess current inventory levels, personnel skill sets, and equipment readiness with little notice. It is recommended to develop a consolidated **interagency database of CBRN resources** during the planning phase. This should provide a comprehensive overview of all CBRN capabilities available across different agencies and jurisdictions, including personnel expertise, equipment, and specialized resources. Such a database would enable strategic decision-makers to quickly assess available resources and coordinate an effective response during incidents. Based on available resources and the current needs, existing gaps can then be identified.

The following table illustrates examples of how to visualize resource gaps:

SPECIALIZED TEAMS				
Team type	**Available**	**Status/notes**	**Current needs**	**Gap**
CBRN expert teams	(e.g. 8 teams available)	(e.g. 6 assessment teams active & 2 teams on standby; Response time: 15-30 min)	(e.g. 10 teams are needed)	(e.g. -2)
Environmental assessment				
Forensic units				
Special operations forces				
Intelligence teams				
Security teams				

MEDICAL RESOURCES				
Team type	**Available**	**Status/notes**	**Current needs**	**Gap**
Chemical exposure specialists	(e.g. 20 staff)	(e.g. 8 doctors & 12 nurses Response time: 15-30 min)	(e.g. 30 staff)	(e.g. -10)
Mobile medical units				
Blood bank resources				
Psychological support teams				
CRITICAL EQUIPMENT				
Team type	**Available**	**Status/notes**	**Current needs**	**Gap**
Medical equipment	(e.g. 50 units)	(e.g. 20 ventilators 30 oxygen tanks Deployment time: 15-30 min)	(e.g. 75)	(e.g. - 25 10 ventilators & 15 oxygen tanks)
Communication equipment				
Transportation resources				
SUPPORT INFRASTRUCTURE				
Infrastructure type	**Available**	**Status/notes**	**Current needs**	**Gap**
Emergency shelters				
Food/water supplies				
Command/control posts				

3) Formulate options

Once CBRN managers and decision-makers have information on: a) the priority order of the requested resources; and, b) the effective availability of the requested resources, they can begin to formulate optimal resource allocation strategy.

At the initial stage, CBRN managers and decision-makers should provide detailed information for each possible course of action, including:

- potential course of action: specific steps to be taken in response to the CBRN incident
- estimated resource allocation: a detailed breakdown of required resources
- expected outcomes: projected results of implementing the proposed option
- limitations: any potential constraints or challenges associated with the option

For example, based on the case above (involving a terrorist group using a nerve agent), CBRN managers and decision-makers should quickly identify the optimal way to treat individuals exposed to the chemical agent. Given time pressure and resource constraints (e.g. limited stocks of atropine and decontamination stations, high demand for medical personnel, etc.), they could consider, *inter alia*, the following options:

Option A: Centralized treatment at a single primary hospital

Course of action

- Designate a single hospital as the primary treatment center for high-priority cases.
- Deploy most medical resources at this location, including available atropine supplies, ventilators, and critical care staff.
- Evacuate and transfer patients with severe exposure symptoms directly to this facility.
- Prioritize life-saving treatments and quickly identify those in need of intensive care.

Estimated resource allocation

- **Medical supplies:** 80% of available atropine stock, ventilators, and neurotoxin countermeasures.
- **Personnel:** Majority of available CBRN-trained medical personnel and critical care staff concentrated at this facility.
- **Logistics:** Ambulances and transport support focused on rapid transfer to the hospital.

Expected outcomes

- **High survival rate:** Immediate access to concentrated resources improves survival rates for those with severe exposure.
- **Efficient treatment of critical cases:** Allows for specialized treatment in a well-equipped facility, reducing delays in life-saving interventions.
- **Faster identification of high-exposure cases:** Centralized triage and treatment support rapid identification and stabilization of the most critical cases.

Limitations

- **Hospital overload:** Potential overcrowding at a single facility, risking overextension of resources.
- **Delay for mild/moderate cases:** Patients with less severe symptoms may experience delays in receiving non-critical care.
- **Limited capacity for additional patients:** If the incident's scale expands or additional patients arrive, the hospital's capacity could quickly reach its limit, reducing treatment effectiveness.

Option B: Distributed treatment across multiple hospitals

Course of action

- Allocate medical resources, including atropine and trained staff, across multiple hospitals in the vicinity.
- Triage patients at the scene to assess severity and transport them to the nearest hospital(s) with capacity.
- Establish communication between hospital(s) for real-time updates on resource availability and patient distribution to manage treatment loads.

Estimated resource allocation

- **Medical supplies:** Spread atropine and antidote supplies across several hospitals, with approximately 30-40% allocated per hospital based on patient loads.
- **Personnel:** Divide CBRN-trained medical personnel among multiple sites to ensure broad coverage and emergency response capability.
- **Logistics:** Ambulance services and transportation teams distributed to each hospital(s).

Expected outcomes

- **Improved access for moderate cases:** Distributing resources allows more patients to receive timely, if less intensive, care.
- **Reduced hospital overload:** Distributing patients helps avoid overwhelming a single facility, allowing each hospital to manage a portion of the caseload.
- **Increased flexibility:** Multiple facilities provide backup options in case one hospital reaches capacity.

Limitations

- **Reduced focus on critical cases:** With resources spread across locations, response time for critical cases may not be as fast as in a centralized setting.
- **Potential delays in communication:** Coordinating across hospital(s) can result in logistical challenges and may delay the treatment of high-priority cases.
- **Logistical strain on transport teams:** Increased patient transportation requirements can slow down emergency responses and strain resources.

Option C: Mobile triage and treatment center near exclusion zone

Course of action

- Set up a mobile triage and decontamination station near the hotel, within the safe perimeter.
- Triage and stabilize patients at the mobile center, performing immediate interventions (such as atropine administration) before transferring only severe cases to hospital(s).
- Establish decontamination protocols at the mobile site to treat mildly exposed individuals on-site, reducing the need for hospital transport(s).

Estimated resource allocation

- **Medical supplies:** Approximately 50% of atropine supplies allocated to the mobile center; additional antidotes and equipment needed for on-site critical intervention.
- **Personnel:** Assign trained emergency responders, CBRN specialists, and medical staff to staff the mobile site.
- **Logistics:** Decontamination units, portable ventilators, and a temporary medical setup requiring tent and supply logistics.

Expected outcomes

- **Immediate stabilization for critical cases:** On-site intervention allows rapid stabilization of severely exposed individuals, potentially reducing fatalities before hospital(s) transfer.
- **Decreased hospital burden:** Reduces the number of patients needing full hospital(s) admission, freeing up hospital resources for severe cases.
- **Efficient patient management:** Allows moderate and mild cases to receive necessary treatment on-site, decreasing the likelihood of secondary contamination in hospital(s).

Limitations

- **Resource intensive:** Setting up a mobile center requires substantial initial resources, potentially straining personnel and medical supplies.
- **Risk of exposure to staff:** Staff working in proximity to the exclusion zone face a higher risk of secondary exposure if containment is not fully effective.
- **Requires specialized logistics:** Mobilizing and setting up a fully functional temporary site could delay initial treatment, especially if resources are already constrained.

4) Determine optimal resource mobilization

The next step is to analyze and determine what is the most suitable option for resource mobilization. To do so, CBRN managers and decision-makers at strategic-level should consider several factors, including, *inter alia*:

- **Consider impact on sustainability:** evaluate the durability of each option. Solutions that support prolonged, sustainable response efforts are often more effective, especially when facing prolonged incidents.
- **Analyze scalability and adaptability of actions:** options that can be scaled up or adapted as the situation evolves provide greater flexibility. This is important in CBRN incidents, where the scope and scale of contamination may shift unexpectedly. Commanders should avoid deploying all resources at once and instead retain reserves for flexibility.
- **Coordinate with interagency and partner support:** consult with other agencies and partners to ensure chosen actions complement overall response efforts. Options that allow for multi-agency collaboration may lead to more effective resource allocation.
- **Logistical feasibility:** evaluate the complexity and speed of mobilizing resources to each treatment site.
- **Public safety and risk of secondary exposure:** balance the need to control public exposure while providing life-saving treatment to the affected population.
- **Regulatory compliance:** e.g., legal requirements, international standards adherence, transportation restrictions; and,
- **Utilize scenario-specific contingency plans:** apply contingency planning, ensuring selected options align with established emergency protocols and response frameworks. This reduces ambiguity and ensures coherence in decision-making.

Another tool that can be used to select optimal resource mobilization is a **cost-benefit analysis** to evaluate each option using a comprehensive cost-benefit analysis.

The following factors can be considered:

FACTOR	DESCRIPTION
Cost	Financial costs, human resources required, time to implement
Benefits	Lives potentially saved, area secured, long-term positive impacts
Risks	Potential for failure, unintended consequences, scalability issues
Alignment	How well the option aligns with overall strategic objectives

In the example of nerve agent use, CBRN managers and decision-makers could produce a table to help optimize resources:

CRITERIA	OPTION A: CENTRALIZED HOSPITAL	OPTION B: DISTRIBUTED HOSPITALS	OPTION C: MOBILE CENTER
Primary focus	High survival rate for critical cases	Broad access to care for varied case severity	Immediate on-site intervention and containment
Resource utilization	Efficient use, high concentration	Moderate distribution, shared resources	High resource demand, includes decontamination
Setup complexity	Low, utilizes existing hospital infrastructure	Moderate, requires inter-hospital coordination	High, requires mobile setup and specialized staff
Capacity for critical cases	High for critical cases	Moderate, balanced between all cases	Moderate, prioritizes immediate stabilization
Capacity for mild cases	Low, risk of delays for mild cases	High, dispersed demand across hospitals	Moderate, on-site triage alleviates hospital demand
Risk of staff exposure	Low, hospital protocols in place	Low, spread across multiple hospitals	High, near incident site with high contamination
Flexibility and scalability	Low, single-site constraint	High, adaptable across facilities	Moderate, scalable but resource-intensive
Transport needs	Moderate, focused on one facility	High, spread over multiple sites	High, for moving critical cases from mobile center
Best For	High-severity, limited spread, moderate patients	Mixed-severity, high patient load, logistical support	Immediate containment, localized contamination risk

Based on this analysis, CBRN managers and decision-makers could determine that:

- **Option A** is optimal if the focus as it stabilizes the great amount of critical cases with the highest possible survival rates, despite limited hospital(s) resources.
- **Option B** is best for managing moderate case-loads across the incident area, minimizing the risk of overwhelming a single facility and ensuring broad access to care.
- **Option C** is ideal if immediate on-site intervention is critical and there's a need to reduce hospital load by managing mild and moderate cases closer to the incident site.

5) Resource deployment

Once the optimal option is determined, CBRN managers can deploy resources. It is advisable to consider the following steps:

- Implement the chosen option without delay
- Assign specific responsibilities for resource management tasks to team members
- Activate pre-planned logistics and supply chain management protocols
- Begin mobilizing the required resources in line with the selected option
- Establish a timeline for deployment and set up checkpoints for progress evaluation

6) Monitoring and adjustment

It is critical for CBRN managers and decision-makers to continuously assess both resource availability and needs as the situation evolves. The complexity of resource allocation and mobilization in a CBRN incident stems from the need to balance urgent actions with careful attention to safety, coordination, and adaptability.

CBRN managers and decision-makers are advised to regularly reasses the selected options, considering:

- changes in CBRN agent concentration or spread
- detection of new CBRN agents
- unexpected weather pattern changes affecting dispersion
- shifts in population movement or exposure levels, and
- effectiveness of current countermeasures falling below predetermined thresholds.

CBRN managers and decision-makers must ensure that the monitoring system is integrated with the CBRN situation assessment, allowing for real-time adjustments to resource allocation and deployment strategies.

Allocation and mobilization of strategic resources: challenges and good practices

CHALLENGES	GOOD PRACTICES
Incomplete CBRN situation assessments can lead to incorrect decisions, including inaccurate resource allocation.	▸ **Prioritize safety** and implement protective measures based on worst-case scenarios (e.g., implementing protective measures that are designed to mitigate the potential risks associated with the most severe possible scenario). ▸ **Communicate uncertainty** and clearly state information limitations to all agencies involved. ▸ **Act on available data,** make initial decisions using current information. ▸ **Gather more information,** deploy CBRN detection teams and consult experts. ▸ Use **predictive modelling** in CBRN situation assessments and prepare for multiple scenarios. This will enhance response actions by simulating potential incidents, thereby enabling effective resource allocation, dynamic risk assessment, and improved inter-agency coordination. ▸ **Implement scalable response,** design flexible actions that can be adjusted as needed. ▸ **Reassess continuously,** establish ongoing evaluation and rapid information sharing and adapt resource assessments and allocations as the situation evolves. ▸ **Engage internationally,** consult international partners for insights. ▸ **Inform public,** provide transparent updates, acknowledging uncertainties. ▸ **Document decisions,** keep records of choices made with incomplete information. ▸ **Apply judgment and intuition.** Strategic commanders should rely on their experience and intuition, especially when faced with incomplete or ambiguous information. This involves: › Drawing on past experiences with similar incidents. › Considering factors that may not be easily quantifiable. › Anticipating potential cascading effects or unforeseen complications. › Assessing the political and social implications of each option. › Considering gut feelings about potential success or failure of each option.

CHALLENGES	GOOD PRACTICES
Stress can cause incorrect decision and suboptimal choices.	▸ Provide **pre-established protocols** to guide actions, reducing the mental load during stressful situations. ▸ Conduct **realistic simulations** of CBRN scenarios to train decision-makers under high-stress conditions. ▸ **Draw on past experiences.** Familiarity with similar situations provides a mental framework for analyzing the current incident, enabling faster and more accurate decisions. Past experiences help identify past mistakes and adapt to unforeseen challenges. ▸ **Focus on selective use of key information.** CBRN incidents often generate large amounts of data, and an attempt to process all available information can overwhelm decision-makers, leading to indecision or errors. Focusing only on high-priority, actionable information ensures that mental resources are directed where they are most needed. ▸ **Employ simplified decision strategies.** Simplified strategies help filter and prioritize essential information, enabling decision-makers to focus on actionable data. Instead of analyzing every variable, decision-makers may rely on pre-established thresholds (e.g., radiation levels requiring evacuation) to make critical decisions.
Overconfidence can cause rushed actions without thorough consideration.	▸ Avoid taking **immediate action** without a proper situation assessment to prevent ineffective response efforts and potential exacerbation of the situation.
Unexpected developments (e.g., a change in weather or a secondary explosion) can disrupt initial response.	▸ Prepare **contingency plans** to address unexpected situations or changes in a CBRN incident. Contingency plans should be developed for a range of potential challenges, such as: › Escalation of the threat: if the CBRN agent spreads further or becomes more dangerous. › Failure of primary containment measures: if efforts to contain the CBRN agent are unsuccessful. › Discovery of secondary sources of contamination: if additional sources of the CBRN agent are identified. › Changes in available resources: if resources become scarce or are diverted to other priorities. › Unexpected weather conditions: if weather conditions change in a way that affects the spread of the CBRN agent or the effectiveness of response efforts. ▸ Maintain **flexibility** and adjust based on evolving situation and changing needs.

CHALLENGES	GOOD PRACTICES
Competing demands for **limited resources** can significantly hinder the effectiveness of the response.	▸ Use **standardized protocols and pre-established guidelines** for allocating different resources based on threat level and population size to expedite decision-making. ▸ **Enhance coordination,** create a centralized resource management system to manage resource allocation across agencies and regions. ▸ **Monitor resource availability,** including personnel (number and expertise of responders, including specialized CBRN teams), equipment (protective gear, detection tools, and decontamination equipment), medical resources (treatments, antidotes, and medical facility capacities), logistics (transportation, communication systems, and supply chain capabilities), mutual aid (activate agreements with neighboring jurisdictions or agencies) and specialized support (identify and engage experts or specialized units as needed). ▸ Establish **clear criteria** to prioritize resource needs as well as to analyze and determine what is the most suitable option for resource mobilization. ▸ **Consider trade-offs,** including: › Evaluate the trade-offs between competing needs, such as immediate safety vs. long-term recovery. › Consider how each option affects different stakeholders (e.g., civilians, first responders, local economy). ▸ **Optimize** resource allocation by allocating resources based on the evolving threat level, contamination zone, and real-time casualty reports. Leverage technology (e.g., GIS mapping, real-time data analytics) for resource tracking. ▸ Maintain **strategic reserve stockpiles** of critical supplies to address unforeseen needs.
Lack of **interagency coordination** can impede the ability to scale up the response in a timely manner.	▸ Ensure coordination among relevant agencies and apply a structured timeline-approach, for example: › Step 1: Local level (e.g., first 0-2 hours) Access immediate local resources first, including first responder equipment, local hospitals, and stockpiles. Activate local emergency operations center. Assess immediate needs and available resources. Deploy immediately available resources based on prioritization criteria. › Step 2: Intermediate level (e.g., 2-6 hours) If local resources insufficient, activate mutual aid agreements with neighbouring areas. Contact neighbouring CBRN response teams and specialized facilities. Access neighbouring stockpiles and equipment caches. Coordinate through neighbouring emergency management structures.

CHALLENGES	GOOD PRACTICES
	› Step 3: National level (e.g., 6-12 hours) When resources from neighbouring areas are exceeded, request national assistance. Activate national response frameworks and specialized CBRN teams. Access national strategic stockpiles and specialized equipment. Coordinate through national emergency management structures. › Step 4: International level (e.g.,12-24+ hours) If national resources are insufficient, initiate international assistance requests.
Misjudgement when determining the appropriate response strategy and deciding between **evacuation and sheltering** in place can lead to unnecessary evacuations, exposing individuals to greater danger, or inadequate sheltering, which may leave populations vulnerable to harmful agents.	▸ Conduct thorough **CBRN situation assessments** to evaluate the nature of the threat, the potential for exposure, and the effectiveness of both evacuation and sheltering strategies. ▸ Develop **flexible emergency response plans** that outline criteria for when to evacuate or shelter based on real-time assessments of the situation. ▸ **Evaluate feasibility** of both plans: assess the availability of resources, transportation, and safe routes for evacuation; determine the capacity and readiness of the community to shelter-in-place effectively. ▸ Include **contingency plans** for both options to ensure a seamless transition between evacuation and sheltering if conditions change. ▸ Provide **clear, timely, and accurate information to the public** about the nature of the threat, recommended actions (evacuate or shelter), and safety measures to minimize panic and confusion.

4. COMMUNICATION WITH THE PUBLIC

Effective communication during a CBRN incident is critical to ensuring public safety, public confidence, and maintaining public trust. Transparent, timely, and accurate information helps to reduce panic, prevent misinformation and disinformation, and guide the public on appropriate actions to protect their health and safety. Additionally, clear, concise, and consistent information aims to prevent the public from overwhelming medical and emergency services unnecessarily.

Clear communication fosters community resilience and enhances the overall effectiveness of the emergency response. Messages shared by the government during a CBRN incident provide essential information to enhance public safety by advising on protective actions and directing individuals to sources for treatment or further information.

Public communication should be structured as a multi-phased process, adaptable to evolving circumstances. Each phase needs individual assessment to ascertain the timing and methods for disseminating updates to the public.

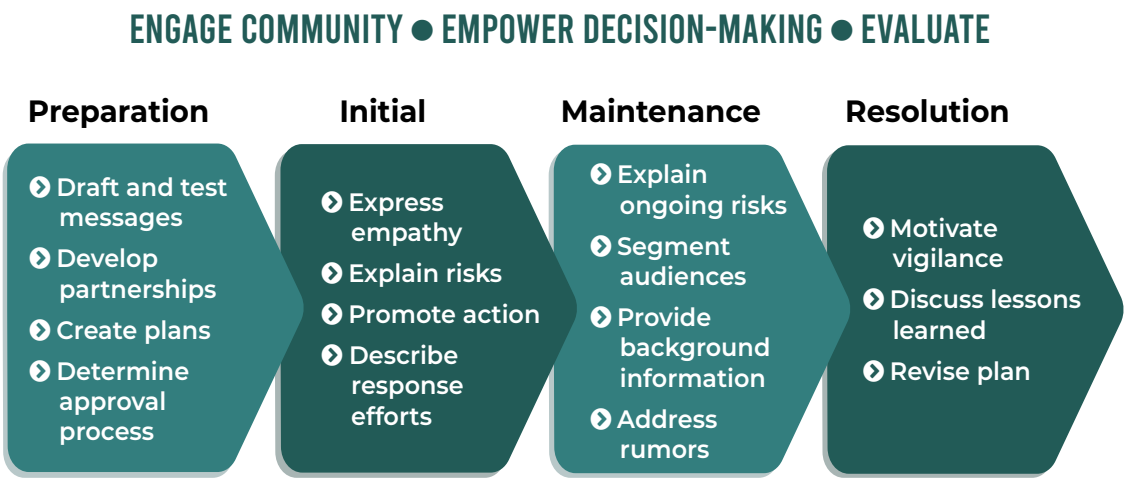
KEY ACTIONS

Frequently, there is insufficient time immediately following a CBRN incident to engage in detailed consultations with emergency service partners, health agencies, or scientists to draft specific messages tailored to the actual substance released. It can take several hours before such detailed information becomes available. Considering these challenges, there are actions that can be taken to ensure effective communication during a CBRN incident.

1) Activate existing communication plans

At the onset of incident response, it is essential to begin implementing of previously defined comprehensive communication strategies and key contacts plan (see Chapter 3.2 Crisis communication planning of the Planning Section). Communication with the public is a multi-phased process that starts at the preparedness stage and continues to the recovery stage. For example, the CDC's Crisis and Emergency Risk Communication (CERC)[8] proposes four communication stages:

8 Centers for Disease Control and Prevention (2018). Crisis & Emergency Risk Communication (CERC).



2) Initiate a joint information center

A **joint information center** should be established to coordinate communication efforts across all involved agencies and stakeholders, ensuring a unified public messaging campaign. Public information professionals from all agencies and organizations participating in incident response activities coordinate and disseminate official, timely, accurate, comprehensible, and consistent information to the public through a joint information center, which can be either physically or virtually located. Establishing a joint information center requires considering multiple factors, such as ensuring essential resources like internet access and multiple electrical outlets, defining operational tasks and staff, and preferably predesigning it during the preparedness stage.[9]

3) Use pre-prepared message templates

Using pre-prepared and exercised messaging campaigns ensures that all communications staff are ready to respond effectively during an incident. The information in these messages is necessarily generic, aiming to provide as much guidance as possible despite the initial lack of detail regarding the nature of the incident, number of casualties, contaminant involved, health effects, or the extent of any atmospheric plume or environmental impact. Such specifics typically become clear only at later stages of the incident and will then guide the type of message to be disseminated. Pre-prepared messages are designed for immediate distribution to media outlets—including television and local radio networks—as well as through other channels such as online platforms and social media. One of the most relevant examples of a pre-prepared message is a **holding statement.** In crisis communication, a holding statement is a pre-written, concise, and adaptable message that an organization uses to provide an initial response during the early stages of a crisis, before all details are available. Its primary purpose is to acknowledge the situation, demonstrate concern, and reassure stakeholders that the organization is actively assessing and managing the crisis. An initial holding statement template, along with general templates for CBRN incidents, can serve as the first form of communication with the public.

9 U.S Department of Homeland Security, Crisis Communications Planning: Establishing Joint Information Centers, https://www.hsdl.org/c/view?docid=765584

In a holding statement, as well as in following statements, it is crucial to clearly outline key actions for the public to ensure the message is both clear and concise. These actions should align with the information available at the time and can be updated or expanded as more details become available. For example:

Holding statement for initial notification

Subject: Urgent Public Safety Announcement [title can be adapted to specific CBRN incident]

Message:

> *"We are responding to an ongoing situation involving [describe the event, e.g., a chemical spill, radiological release, or biological threat] in [specific location]. Government agencies and emergency response teams are actively managing the incident. At this moment, details are still being confirmed, and we will provide more information as it becomes available.*
> *For your safety, please take the following actions immediately:*
> *Avoid the area of [affected location] entirely.*
> *Stay indoors, and ensure all windows and doors are securely closed until further instructions are provided [specific security measures should be adapted to CBRN incident].*
> *Follow updates from [government agency] through [specific communication channels: TV, radio, social media, etc.].*
> *Use [emergency hotline number] only for urgent assistance to keep lines available for critical needs.*
> *We are working to confirm further details and will provide updates as soon as they become available. Your safety remains our top priority. Thank you for your cooperation and vigilance."*

Key actions highlighted in the example:

- Avoid the area of [affected location].
- Stay indoors and keep windows and doors closed until further instructions are given.
- Follow all updates from [government agency] through [communication channels: TV, radio, social media, etc.].
- Dial [emergency hotline number] only for urgent assistance.
- Other specific actions depending on the CBRN event.

4) Create clear messages

Disseminating clear messages to the public is essential to support the response efforts. Although it is relevant to assess the context before deciding to share information, there are some general elements that can be considered when drafting a message.

Before drafting the message during a CBRN incident, it is critical to:

- **Choose and understand the audience:** Identifying a target audience is essential for defining how the message is crafted and shared. Considering this upfront can enhance both the impact and dissemination of the message. Different audiences, depending on their relation to the situation, have varying priorities in terms of information needs. While the facts remain consistent, it may be necessary to adjust the context and delivery of the message to meet the audience's demands for accessibility and cultural sensitivity.
- **Means of communication and accessibility:** After selecting the target audiences, it's important to select the most appropriate means of communication. The availability and utilization of specific communication channels, —such as TV, radio, text messages, social media, and print media—can vary based on infrastructure, individual preferences, societal norms, and income levels, all of which influence physical access to information. Accessibility to these channels is also determined by factors such as language, literacy, education, vocabulary, and vision or hearing capabilities. During a CBRN incident, other non-traditional means can be employed. These include emergency alert systems to send public notifications, public information hotlines staffed with trained personnel to answer questions, mobile apps offering real-time updates and safety instructions, and websites or online portals that serve as central hubs for all public information related to the incident.

The example below shows how communication was adapted to target the Japanese population by using an anime character after the Fukushima Daiichi Nuclear Disaster in 2011. The aim of this communication campaign by the Fukushima Health Management Survey (FHMS) was to offer information about thyroid screening to

inhabitants of Fukishima aged 11 and older. To support this, the FHMS created and distributed a poster and clear file folder featuring characters from the manga "Hataraku Saibo" (Cells at Work!, ©Shimizu Akane/Kodansha LTD) in Fukushima Prefecture. This manga explains physiological processes through anthropomorphized cells, such as red and white blood cells and platelets. The materials also provided QR codes linking to websites with the latest details on thyroid screenings and participating medical organizations.[10]

When drafting a message, it is critical to consider that its length, format, and level of detail will depend on the communication channel and target audience. For example, a social media post will require a short message presented in a visual or graphic manner to generate more impact. Some of the aspects to consider include:

- A comprehensive but simple description of the situation, including the mode of agent spread, and an outline of governmental response efforts.
- Instructions on safety measures and risk guidance.
- Areas to avoid, movement restrictions, evacuation procedures, and transportation modifications.
- Information on the availability of medical and non-medical countermeasures, specifying what is available, for whom, when, and where.
- Locations of supportive care and treatment facilities, detailing availability, intended recipients, timing, and locations.
- Information on decontamination, evacuation, and shelter-in-place procedures.
- Details on the frequency of updates and the communication channels used (TV, radio, social media, etc.).
- Clear instructions on how to contact emergency services and government hotlines for additional information or assistance.
- Forward-looking information about the forthcoming response.
- Basic explanation of the rationale behind the government's actions and instructions, especially those that might contradict the public's intuitive behavior.

In addition, it is important to:

- Ensure that information is provided in **multiple languages and accessible formats** (e.g., for individuals with disabilities).
- Acknowledge **ambiguity and uncertainty,** as well as the possibility that action may be required before all the facts are known. For instance, communication officers might include statements such as, "The situation is currently evolving, and we anticipate that updates will be provided shortly." Be prepared to discuss how conditions are changing and the steps being taken to close knowledge gaps.

10 Amir, I., Eguchi, Y., Saotome, K. et al, 2023. The "GU-GU-RU" project to eliminate discrimination related to the health effects of the Fukushima nuclear accident. BMC Public Health 23, 2050, https://bmcpublichealth.biomedcentral.com/articles/10.1186/s12889-023-16883-2

- Provide **frequent updates** to keep the public informed as the situation evolves and to counter misinformation. Regular communication such as updates on emergency response activities is especially crucial during times of uncertainty when the public may need to wait, and response efforts may not be immediately visible. Clear and consistent messaging helps address rumors, misinformation, and disinformation, reducing uncertainty and building trust by delivering timely, honest, and forward-looking information.
- Ensure **collaboration with CBRN experts** to effectively convey data that help people make informed decisions. These experts can clarify the reasoning behind the decisions made and can support the overall process of understanding how the assessment was used to decide which actions should be taken. This information should be communicated in a straightforward manner, avoiding overly technical language whenever possible.
- If the message is delivered by a person, it is important to select an appropriate **spokesperson**—preferably a person with previous experience or training in the role and a trustworthy or well-known figure.
- Decision-makers should **validate** the content of the messages before communicating crucial information to the public.

Example for a biological event

Subject: Public Health Warning – Potential Biological Hazard in [location]

Message:

> *"We are responding to reports of a potential biological hazard in [location]. Early information indicates that [name or type of biological agent, if known] may be involved. While investigations are ongoing, we ask the public to prioritize their safety by taking the following steps:*
>
> - *Avoid close contact with others, especially in public spaces, to reduce the risk of spreading infection.*
> - *Practice strict hygiene by washing hands frequently with soap and water for at least 20 seconds or using a hand sanitizer with at least 60% alcohol.*
> - *If you experience symptoms such as [list symptoms, e.g., fever, cough, respiratory issues], contact [health authority or hospital] immediately and self-isolate to prevent transmission.*
> - *Follow guidance from health authorities, which may include vaccination, medication, or other specific actions depending on the nature of the incident.*

> *Health authorities are working closely with experts to contain the situation and provide appropriate care. Stay informed through updates on [specific channels, e.g., TV, radio, official social media platforms], as we will share new information promptly as it becomes available.*
> *Your cooperation is vital in managing this situation. Thank you for your prompt actions and understanding."*

Key actions highlighted in the example:

- Avoid the specific actions or follow certain instructions [depending on the agent involved].
- Follow all updates from [government agency] through [communication channelshTV, radio, social media, etc.].
- Dial [emergency hotline number] only for urgent assistance.
- Other specific actions depending on the CBRN event.

5) Consider other reliable sources of information

Given the uncertainties surrounding many types of CBRN incidents and the need for prompt action to save lives and mitigate adverse impacts, it is crucial to leverage all available sources of information and expertise. Numerous resources—such as academia, private companies, and other governmental agencies—can assist in assessing the situation, predicting agent behavior and transmission, estimating potential consequences, and providing recommendations for protective actions.

6) Engage with the community

Hold press conferences, town hall meetings, and Q&A sessions to address public concerns and questions. Provide clear and transparent updates on the situation, including any known risks and safety measures in place to protect the public. Ensure that communication is accessible to all segments of the population by using multiple channels such as social media, radio, and local news outlets.

Example – Considering cultural sensitivities

As part of EU CBRN Centres of Excellence (CoE) Project 48, titled "Improved Regional Management of Outbreaks in the CBRN Centres of Excellence Partner Countries of the African Atlantic Facade," a training module on "safe and dignified burial techniques" was developed, proving especially crucial during the Ebola crisis and the COVID-19 pandemic.

Between June and October 2020, 18 practical, hands-on training sessions were held to instruct participants in safe and dignified burial practices for COVID-19 victims and effective crisis communication. These sessions, led by experts trained through EU CBRN CoE Project 48, engaged 400 practitioners, including representatives from health ministries, civil protection agencies, mosque burial teams, local and regional authorities, religious leaders, funeral directors, cemetery workers, doctors, and nurses. The training took place across seven partner countries (Cameroon, Côte d'Ivoire, Gabon, Liberia, Morocco, Senegal, and Sierra Leone) and reached multiple regions within each country. Additionally, a three-day door-to-door COVID-19 awareness campaign was conducted in Monrovia, Liberia, reaching five local communities.

A training session on "safe and dignified burial" in Sierra Leone.

7) Monitor and address misinformation (non-intentional) and disinformation (intentional)

Misinformation refers to false or factually inaccurate information that is not created with malicious intent. Disinformation, on the other hand, is false information deliberately crafted to harm a person, social group, organization, or country. Actively monitor media and social platforms for both misinformation and disinformation, and promptly provide accurate corrections. These forms of false information can influence decision-making processes, trigger unnecessary panic, or hinder effective crisis management. Therefore, it is essential to establish continuous monitoring of media and social platforms to detect these false claims. Quick and accurate corrections should be issued through official channels—ideally pre-emptively—to prevent false information from gaining traction and causing widespread confusion or harm.[11]

11 For more information on disinformation, see UNICRI *Handbook to combat CBRN disinformation*, produced in January 2023 and available on UNICRI website.

Communication with the public: challenges and good practices

CHALLENGES	GOOD PRACTICES
Providing **inaccurate or misleading information** can erode public trust and exacerbate the crisis.	▸ Establish a strict **fact-checking protocol** that verifies information from multiple reliable sources before release. ▸ Cultivate **partnerships** with trusted agencies and commit to prompt, transparent corrections if inaccurate information is released.
Delayed or inconsistent messaging can create confusion and ensure public safety.	▸ Prepare **pre-approved messages** and maintain consistency by designating informed spokespersons, who can ensure that messages are timely and accurate. ▸ Use **dedicated crisis channels** for rapid updates, helping to keep the public well-informed without delay.
Withholding relevant information or being opaque about decision-making processes can breed suspicion and hinder cooperation.	▸ Implement a controlled **disclosure policy** to balance public safety with security needs, sharing essential details only. ▸ Regularly **update the public** on decision-making processes to enhance transparency, fostering. understanding and trust without compromising sensitive information.
When interacting with the media or the public, be mindful that certain statements or questions may be **framed** in a way that suggests mistakes or errors are being made. This can create unnecessary tension or distrust, especially in a crisis.	▸ In such cases, it is more effective to **reframe the questions** to focus on facts and solutions. For example, if the question is: "Wouldn't you agree that the government's slow response to this incident has directly contributed to the widespread devastation it has caused?", the answer can reframe it as: "While it's essential to thoroughly assess the response and its impact on any incident, I would like to clarify that the situation was incredibly complex, and we have been working diligently to address it. Our response has been guided by the latest scientific knowledge and interagency coordination. It's not a straightforward issue, and I'd be happy to provide more details on the specific challenges and steps we've taken to mitigate the incident's impact".
Not engaging with stakeholders, such as community leaders or local organizations, can result in ineffective communication strategies.	▸ Identify and **involve community leaders** and organizations early in the communication strategy to create a unified front. ▸ Structured **feedback mechanisms** enable stakeholders to contribute insights, helping to avoid conflicting messages and enhance overall communication effectiveness.

CHALLENGES	GOOD PRACTICES
Neglecting feedback and evaluation from the public can prevent improvements and adjustments for future crises.	▸ Use direct feedback channels to **monitor public understanding** and communication gaps. ▸ Conduct **post-incident evaluations** to refine communication strategies, using lessons learned to improve future responses and maintain adaptability.
Disregarding cultural, and other types of sensitivities can lead to misunderstanding and alienation of certain segments of the population.	▸ Provide **cultural sensitivity training** to communicators and develop messaging materials that respect diverse cultural and linguistic needs. Inclusive, culturally aware communication ensures that information reaches and resonates with all community segments, reducing misunderstandings and enhancing cooperation.
Overpromising or underdelivering can lead to disappointment and distrust among the public.	▸ Gather **information from experts** and other relevant stakeholders regarding the response capacity and the expected results. ▸ Set **realistic expectations** and avoid making assurances that may be difficult to keep, as these can lead to the erosion of public trust. ▸ Clearly communicate achievable goals and **emphasize the uncertainty** of certain outcomes to maintain credibility.
Failing to **address public concerns or questions** can heighten anxiety and undermine confidence in government response efforts. This may include not countering rumors and myths in a timely manner.	▸ Survey media, social media, and public gatherings to **gauge emerging concerns** and address them directly. ▸ Provide **timely responses to rumors** and myths to dispel misinformation, reduce public anxiety, and show responsiveness to community issues, using different techniques, including debunking.
Considering that **nothing is off the record,** especially if you are wearing a microphone.	▸ Approach every interaction, especially when using microphones, as though it is on the record. This mindset helps ensure that all **communications are thoughtful, accurate, and aligned with official messaging,** reducing the risk of unintended statements.
Sharing evidence details during investigations can compromise the integrity of ongoing investigations, hinder legal proceedings, or reveal operational vulnerabilities.	▸ **Avoid sharing details about ongoing investigations,** such as leads, testimonies, or forensic methods, to protect the integrity of the investigation and prevent compromising any legal proceedings.
Disclosing sensitive resources, such as the locations, capabilities, or movements of specialized response teams, could expose them to sabotage or misuse and compromise operational security.	▸ **Withhold details** about the location, capabilities, and movements of specialized CBRN response teams or investigation sites. This precaution minimizes security risks and safeguards critical response resources from potential threats.

5. INVESTIGATION, INTELLIGENCE GATHERING, AND FORENSICS

Following a CBRN incident, the incident location becomes a critical zone for both response and investigation. This applies regardless of whether the incident is accidental, natural, or potentially criminal in nature.

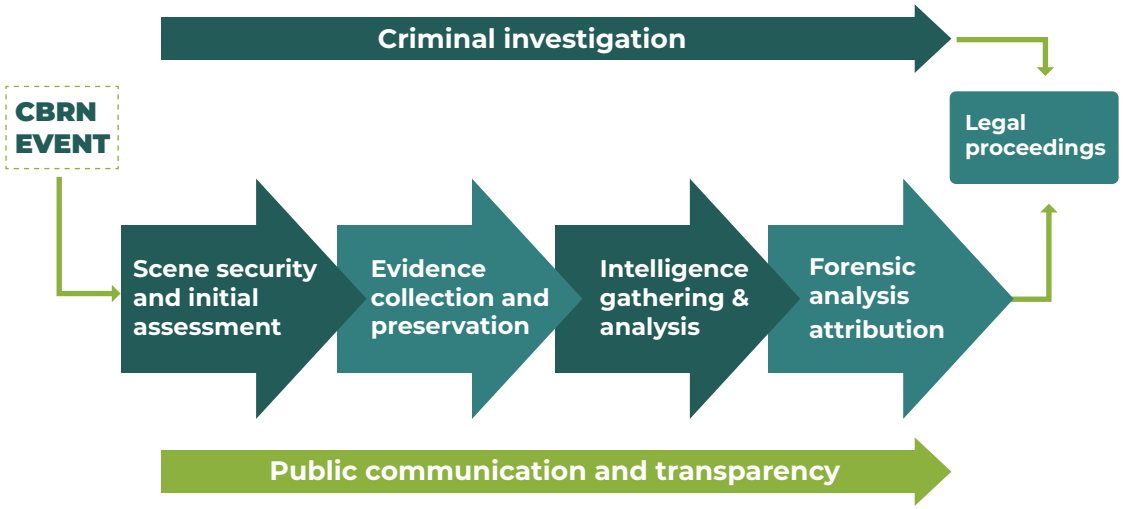
To ensure public safety and an effective response, it is crucial to initiate an investigation as early as possible. This investigation will determine the cause, assess the impact, and gather evidence for potential legal proceedings. Ultimately, it will support the prevention of future incidents and reinforce public safety. All actions—from evidence collection at the scene to any subsequent legal proceedings—must be conducted in a way that preserves the integrity of the investigation while prioritizing both public safety and an effective response.

Investigation, intelligence gathering, and forensics are all critical aspects of a strategic response following a CBRN incident regardless of its cause (accidental, natural, or intentional). This is essential for several reasons:

- **Establish the cause of the incident:** This helps guide response efforts and prevent future occurrences. Investigation techniques, such as forensics and intelligence gathering, play a key role in this process.
- **Accountability and deterrence:** Identifying the perpetrators and gathering evidence allows for holding them accountable. This discourages future attacks by demonstrating the consequences of CBRN use.
- **Public trust:** A thorough investigation fosters public trust by demonstrating a commitment to bringing those responsible to justice and preventing similar incidents.
- **Preventing future attacks:** Understanding the cause, intent, and capabilities behind the incident (if applicable) allows for the development of preventive measures to address vulnerabilities and thwart future attacks.
- **Mitigating long-term risks:** Investigative findings can reveal the source of the CBRN agent and potential environmental contamination. This knowledge helps address long-term health risks and guide environmental remediation efforts.

KEY ACTIONS

Following a CBRN incident, a successful investigation requires a coordinated effort among various stakeholders, including investigative and intelligence agencies, national laboratories, medical professionals, environmental agencies, first responders, veterinarians, animal control and agricultural agencies, as well as subject matter experts in fields such as epidemiology, analytical chemistry, nuclear science, toxicology, forensics, and environmental science. These stakeholders rely on critical information from various sources to make informed decisions throughout the investigation process.



1) Containment, scene security, and initial assessment

These initial actions lay the foundation for a successful CBRN investigation. They ensure the safety of investigators, preserve evidence, and provide the necessary information to effectively trace the source and identify the perpetrators of the attack. These initial actions include, *inter alia*:

- Establishing a **comprehensive strategy to secure the affected area,** prioritizing the safety of civilians and first responders. Allocating resources to establish a secure perimeter and implementing access control measures to preserve the scene.
- Strategically allocating **CBRN survey and identification equipment** to determine the nature and extent of the CBRN hazard, guiding evidence collection efforts.
- Authorizing the **analysis of available intelligence and witness reports** to gain situational awareness, identify initial leads, and help establish a timeline of events.
- Initiating **coordination with national and international CBRN response agencies** to gain access to specialized expertise and resources for investigation and forensics.
- Initiating **communication channels with the public** to provide clear and timely information.

Several sources of information can assist with decision-making on containment, scene safety and security, and initial assessment following a CBRN incident. These include witness reports describing the incident itself; aerial imagery; real-time data from survey meters and monitors; physical evidence from the scene, such as fragments of containers, dispersal devices, environmental samples, documents, and digital equipment; maps of the area, including buildings, infrastructure, and ventilation systems, to help predict potential contamination spread; and available intelligence reports.

2) Evidence collection and preservation

Meticulous evidence collection and preservation are the cornerstone of successful CBRN investigations as they shed light on the nature and scope of the CBRN incident and ensure build a compelling case. This includes the following:

- Direct the development of a **comprehensive plan** for collecting environmental samples, potential agent remnants, and other forensic evidence prioritizing high-yield locations, and ensuring proper sample handling and chain of custody for collected evidence. It is recommended that:
  - Necessary collection and preservation of evidence must be balanced with health and safety concerns and the need for immediate site remediation or treatment of the injured.
  - The collection of evidence, whether physical, trace, or electronic, must be executed by designated and trained teams, in a way that protects its integrity, relevance, and reliability.
  - Oversight falls under the designated legal authority (e.g., special prosecutor or law enforcement).
- Mandate the use of **approved protocols** for containment and transportation of collected samples to specialized laboratories. Integrity and preservation of evidence can be especially challenging as there could be many agencies and investigative bodies involved within the incident scene (first responders, military, CBRN teams, police, and environmental agencies).
- Mobilize the **necessary expertise** (within law enforcement or from academia and the private sector) and strategically deploy resources (personnel, equipment, funding) based on the CBRN agent and investigation scope.
- Decide on the level of **international cooperation** needed for sample analysis considering specialized laboratories or technical assistance from partner nations.

3) Intelligence gathering and analysis

In CBRN investigations—regardless of whether the cause is accidental, natural, or intentional—intelligence gathering and analysis provide investigators with vital leads, context, and potential suspects early in the process. This helps them focus their efforts and may also contribute to preventing future attacks.

- Determine the most critical intelligence needs for the investigation, including the identification of the potential origin of the CBRN agent, potential perpetrators and their capabilities if a deliberate attack is suspected, and potential secondary risks and cascading effects, such as disruptions to critical services (e.g., water, electricity, etc.).

- Authorize and oversee the execution of investigative measures, such as searches and surveillance, in accordance with legal guidelines.
- Authorize the analysis of OSINT such as communication intercepts, social media feeds, news reports, and other publicly available information to understand the incident, identify potential future attacks and develop relevant leads.
- Set timelines for intelligence gathering to prioritize the most urgent intelligence needs.
- Allocate resources (personnel, equipment, and funding) for specific intelligence gathering methods like human intelligence or technical surveillance to increase the likelihood of gathering valuable information.
- Coordinate with domestic and international intelligence agencies balancing national security concerns with the need for collaborative analysis.
- Direct the dissemination of intelligence findings to relevant parties including investigators, medical personnel, and first responders for informed decision making.

The following example from the UNICRI's Prosecutor's Guide to Chemical and Biological Crimes[12] highlights the process, main challenges and outcomes from a chemical and biological investigation in Czech Republic.

Case Title:
Operation Cury "Dimethylmercury and Abrin"

Year of Investigation:
2018

Country of origin:
Czech Republic

Region/State:
Uherské Hradiště

Case category:
Chemical and Biological

Incident Summary:

- In 2017, the perpetrator M.H. unsuccessfully attempted to acquire dimethylmercury via the darknet.
- Between February and March 2018, he attempted to acquire C4 plastic explosive via the darknet. Again, unsuccessful, he turned his attention to the biological toxin abrin.
- Finally, he negotiated with a darknet seller to buy 100 grams of dimethylmercury and 200 milligrams of abrin. These ampules were hidden inside small toys and a clock for distribution to the buyer.
- The investigation involved the security forces of the Czech Republic in cooperation with the U.S. Federal Bureau of Investigation (FBI).
- The perpetrator was detained and several ampoules with the inscription dimethylmercury and abrin were seized. However, laboratory testing confirmed the substances sent to the preparatory by the seller were counterfeit.
- The investigation for prosecution focused on the illegal acquisition of the chemical and biological agents.
- A clear motive for these acts was not established.
- M.H. was convicted under § 21 par. 1 - § 284 of the Criminal Code for the attempted crime of possession of narcotics, psychotropic substances, and poison. (Refer to legislation below)

12 UNICRI (2022). A Prosecutor's Guide to Chemical and Biological Crimes https://unicri.it/Publication/Prosecutor-Guide-Chemical-Biological-Crimes

Investigative Intelligence:

- The investigation initiated due to established intelligence links between the US FBI and the Czech Police. The FBI intercepted communication between the buyer and seller and shared this intelligence which initiated collaborative investigations.
- Two main departments of the Czech police National Centre for the Combating of Organised Crime were involved, namely, the Cyber Department and the Counterterrorism and Extremism department (Firearms and Hazardous Material Unit).
- Interagency information was shared in the framework of international cooperation between U.S. FBI and Czech police.

Keys Points of Evidence:

- This proactive investigation was only possible due to ongoing surveillance of darknet sites and the identification of suspicious behaviour on darknet coming from a Czech IP address.
- The chemical and biological materials in question are restricted or prohibited items.
- Communications between the perpetrator and seller included knowledge of the toxicity of the substance, referring to the appropriate concentration of the biological toxin, per kg of body weight. Communication implied intent to cause harm rather than exploit profitability.

Challenges:

- Conducting cybercrime through the darknet, a platform that enables perpetrators to remain anonymous and untraceable and is always advancing with new and emerging information and technologies (ICT) that challenge the investigative process.
- Use of dark web platforms, cryptocurrency, fake names, and encrypted messaging apps.
- Collection and management of digital evidence and appropriate chain of custody.

- Linking acquisition to motive and intent. The perpetrator was never found in possession of illegal substances; however, the substances were counterfeit.
- Logistics and time to prepare all necessary detection devices (ability to confirm identify and safe handling of materials upon intercept) prior the package arriving in the Czech Republic.
- The coordination of parallel investigations undertaken by CZ Police and FBI.

Outcomes:

- The court did not agree with the prosecution's conviction (intent to profit from sale of dangerous substance). The prosecutor based the hypothesis on the allegations of a witness claiming the perpetrator had gambling habit and financial debts. It was also claimed the perpetrator intended to kidnap an acquaintance and subsequently blackmail his parents and demand a ransom.
- While claims were unsubstantiated with credible evidence, the court considered a possible motive of intent to cause harm.
- M.H. was convicted under § 21 par. 1 - § 284 of the Criminal Code for the attempted crime of possession of narcotics, psychotropic substances, and poisons, and according to § 21 par. 1 - § 272 par. 1 for the attempted crime of public menace. As no intention or motive could be proven, the perpetrator could not be convicted of other crimes, such as attempted murder or even terrorism.

4) Forensic analysis and attribution

Forensic analysis plays a vital role in investigating CBRN incidents, although the specific techniques used may vary depending on the cause. In the case of an intentional CBRN incident, forensic analysis provides crucial information for attributing the attack. While less prominent, forensics can also be valuable in accidental CBRN incidents, for example to identify the specific cause of an accidental release, determine the extent of contamination, and differentiate between accidental and intentional incident. Forensic techniques support investigations and legal actions, and may include:

- **Source tracking** to pinpoint the agent's origin (e.g., facility, stockpile) and route.
- **Microbial forensics** analyses microorganisms or toxins, identifying their source, characteristics, and potential manipulation.
- **Chemical fingerprinting** exploits the unique signatures in chemical agents to trace them back to a specific producer.
- **Nuclear forensics** examines the properties of nuclear and radioactive materials to pinpoint their origin, history, and potential trafficking routes.

To effectively utilize the forensic techniques, several key actions are crucial, including, but not limited to:

- Authorizing the prioritized analysis of collected samples to identify the specific CBRN agent and potentially link it back to a source. Clear objectives for the forensic analysis should be set.
- Deciding which specialized which specialized laboratories (domestic or international) possess the necessary expertise and equipment for analyzing the samples.
- Determining the approach of the approach to attributing the attack. This could involve analyzing forensic evidence, sharing findings with international partners, or utilizing intelligence sources to identify suspects.
- While a successful attribution can lead to prosecution, sanctions, and global cooperation, the process can be lengthy and complex, with conclusive evidence sometimes elusive. Considerations include:
  - Biological agents may be endemic or naturally occurring, making it difficult to identify potential criminal intent.
  - There are myriad types of existing and newly created chemicals and their precursors.
  - Raw materials or laboratory equipment needed to make CBRN weapons often have dual uses (legitimate and illicit ones).
  - Individuals who initially have authorization or permission to access certain materials can misuse their positions for criminal ends.

Investigation, intelligence gathering, and forensics: challenges and good practices

CHALLENGES	GOOD PRACTICES
Preserving evidence and maintaining a chain of custody for contaminated evidence.	▸ Implement **strict chain-of-custody protocols** to maintain the integrity of evidence. ▸ Provide specialized **training** to first responders and forensic personnel on **proper evidence collection and handling** technique. ▸ Implement **digital documentation** with real-time secure uploading before physical handling. ▸ Use **specialized contamination-resistant** evidence containers.
Contamination concerns leading to **evidence potentially degraded** by the agent and limiting evidence collection.	▸ If available, deploy **robotic collection** systems. ▸ Establish **"hot-cold" zone transition protocols** with dedicated decontamination stations for both evidence and personnel. ▸ Ensure adequate and **appropriate PPE** for all personnel involved in the evidence collection.

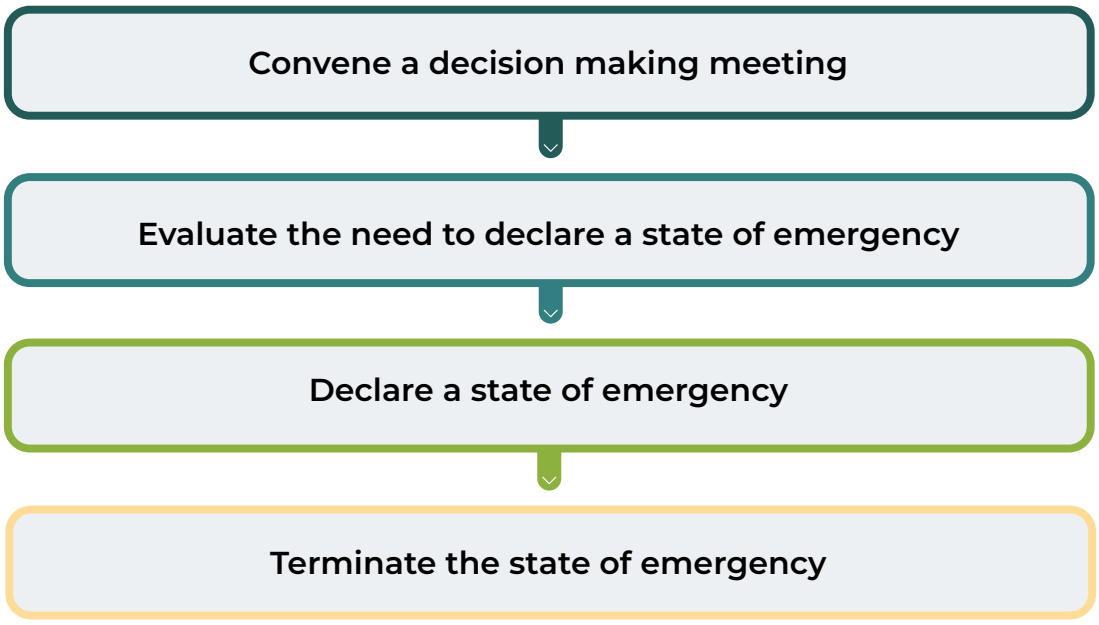
CHALLENGES	GOOD PRACTICES
Misinterpretations of data such as data related to the CBRN agents and environment.	▸ Create **multi-disciplinary analysis teams** with mandatory peer review processes. ▸ Use **standardized interpretation frameworks** and decision support software. ▸ **Foster collaboration** between scientists, engineers, and public health experts to interpret complex data.
Limited medical data due to evolving symptoms and the focus on immediate patient care.	▸ Develop **standardized protocols** for medical data collection and reporting. ▸ Implement **automated data aggregation.** ▸ Establish **rapid medical data sharing** to facilitate information exchange between healthcare providers and public health authorities.
Unreliable witness accounts, biased by media or discussions, impacting their accuracy.	▸ Implement immediate **witness isolation protocols** and rapid interview procedures. ▸ Use **trained interviewers** to conduct interviews in a neutral and supportive environment.
Security footage gaps due to malfunctions, limited coverage, or deletion policies or poor-quality recordings.	▸ Ensure that **surveillance systems are well-maintained,** have adequate coverage, and are equipped with high-quality cameras. ▸ Establish clear policies for the **retention and preservation of surveillance footage,** especially in the context of potential incidents. ▸ Share information and **collaborate with law enforcement** and intelligence agencies to obtain relevant footage from other sources.
Pinpointing the source of a CBRN agent especially for readily synthesized or widely obtainable agents.	▸ Create and maintain a **detailed agent signature database** with regular updates from partner agencies, coupled with automated pattern recognition tools. ▸ Utilize **advanced forensic techniques,** such as DNA analysis and chemical fingerprinting, to trace the source of the agent. ▸ Collaborate with **international partners** to share information and expertise.
Lack of specialized expertise, such as microbial forensics and chemical fingerprinting.	▸ Establish **virtual expert networks** with 24/7 availability. ▸ Develop **partnerships** with specialized laboratories and research institutions. ▸ Invest in **training and capacity building** to develop a skilled workforce.
Intelligence reports with various degrees of **accuracy or delayed** due to analysis.	▸ Implement a **multi-source intelligence system** with automated cross-referencing and real-time updating capabilities between agencies. ▸ Implement robust **cybersecurity** measures to protect sensitive information and critical infrastructure.

6. DECLARING A STATE OF EMERGENCY

In the context of responding to CBRN incidents, declaring a state of emergency is a crucial step that empowers authorities to take immediate and decisive action to protect public safety and health. This declaration facilitates the activation of emergency response protocols, enabling rapid resource mobilization and the implementation of essential measures such as quarantines and travel restrictions.

KEY ACTIONS

Defined within the national legal frameworks, the process of declaring a state of emergency following a CBRN incident varies by country but typically includes the following general steps:



1) Convene a meeting to consider the possibility of declaring a state of emergency

A group of key decision-makers will assemble to assess the situation and deliberate on whether declaring a state of emergency is necessary. The composition and level of this group will vary depending on the scope and severity of the CBRN incident, as well as the governmental level(s) affected (local, regional, or national). Each jurisdiction or country may have its own established protocols for such gatherings. This decision-making body typically includes:

LEVEL OF GOVERNMENT	DECISION-MAKING GROUP
Local	▸ Local emergency management director or similar ▸ Mayoral or city manager staff ▸ Representatives from emergency response agencies (police, fire, emergency medical services) ▸ Public health officials ▸ Environmental protection agency representatives ▸ School district officials, community leaders ▸ Shelter managers ▸ Local media representatives
Regional	▸ Governor or similar official (or their designee) ▸ Regional-level officials from relevant departments (public safety, health, transportation, environment) ▸ Law enforcement ▸ Public health official ▸ Regional environmental protection agency representatives ▸ Representatives from regional utilities and infrastructure providers
National	▸ President or designee ▸ Cabinet-level officials from relevant departments/ministries (Health, Defence, Interior, Environment, etc.)

To inform their decisions, the group consults with specialists from various agencies and disciplines, including:

Scientific and technical experts relevant to the specific CBRN agent involved

- National agencies with specific CBRN expertise
- Public information officers to manage communication with the public
- Legal counsel and,
- Representatives from non-governmental organizations (NGOs) involved in relief efforts.

2) Evaluate the need to declare a state of emergency

To decide whether to declare a state of emergency, the decision-making group should consider the following steps:

- **Review situation assessment.** The group of key decision-makers will receive and review the comprehensive CBRN situation assessment provided by the dedicated assessment group (see Chapter 2 CBRN situation assessment of the Response Section). If necessary, the group can request additional real-time information or clarifications from relevant agencies to supplement the assessment.

- **Utilize the pre-established criteria for declaring a state of emergency.** These criteria define the conditions that necessitate such a declaration and guide decision-making during crises (see Chapter 3.3 Defining emergency authorities and the legal frameworks for declaring a state of emergency of the Planning Section).
- **Evaluate against criteria and assess impact.** Based on the CBRN Situation Assessment and the pre-established criteria, the decision-making group should:
  - Evaluate the potential impact of the incident.
  - Consider the benefits of declaring a state of emergency.
  - Assess any potential drawbacks or consequences.
- **Make a recommendation.** Following the evaluation, the group formulates a recommendation. This recommendation to declare a state of emergency may be made by:
  - Consensus, or
  - Through a formal voting procedure.

Key questions to guide the evaluation

When considering whether to declare an emergency, a positive response to one or more of the following questions may indicate that the situation, whether actual or anticipated, warrants the declaration of a state of emergency:

- Is the situation an extraordinary incident requiring **extraordinary measures?**
- Is the situation **a large-scale or complex** CBRN incident?
- Does the situation pose a **danger of major proportions** to life, environment, or property?
- Does the situation **threaten essential services** (e.g., energy, potable water, sewage treatment/containment, supply of goods or medical care)?
- Does the situation require a response that exceeds, or threatens to **exceed the capabilities of local authorities** (state, province, municipality, township, etc.) in terms of either resources or deployment of personnel?
- Is it a consideration that the local response may be of such **duration** that additional personnel and resources may be required to maintain the continuity of operations?
- Does the situation require, or have the potential to require the **evacuation and/or shelter** of people or animals?
- Does the situation pose a **large-scale disruption** to routine patterns of transportation, or re-routing of large numbers of people and vehicles?
- Is an incident likely to have a **long term negative impact** on a community's economic viability/sustainability, including resulting unemployment, lack of available banking services and restorative measures necessary to re-establish commercial activity?
- Is it possible that a **specific person, corporation, or other party** has caused the situation?

3) Declare the state of emergency

Following the process defined in the legal framework, the designated person or institution with the authority to declare a state of emergency does so by issuing an official announcement that outlines the reasons for the declaration and the specific powers being activated to address the crisis.

The authority declaring the emergency must **document the justification** for the decision, citing the specific threats and the need for extraordinary measures. This documentation might be required for legislative oversight or potential legal challenges. In some countries, the legislative branch (parliament or congress) might have a role in reviewing or approving the state of emergency declaration, potentially setting time limits or requiring periodic updates.

Once the state of emergency is declared, a **clear public announcement** will be made through established channels, explaining the situation and providing instructions to the public. This declaration triggers the activation of **pre-determined response protocols,** which may include evacuations for at risk populations, mass decontamination (if needed), enhanced control measures to contain the CBRN agent, resource allocation for response and relief, and potential activation of military support.

Key considerations for declaring a state of emergency

Declaring a state of emergency carries significant implications and consequences that must be carefully weighed:

Impact on civil liberties: Restrictions on movement, assembly, and communication may be necessary for public safety. However, it is vital to ensure these limitations are proportionate and time bound as unchecked and unrestricted use of power could easily lead to a potential breach of civil rights protected by the Constitution.

- **Potential for abuse:** Granting broad emergency powers can create a risk of misuse or abuse by authorities. Strong legal and oversight mechanisms are essential to prevent this.
- **Psychological impact:** States of emergency can heighten anxiety, fear, and social unrest among the population. Effective communication and clear explanations can help mitigate these concerns.
- **Economic disruption:** Emergency measures can disrupt business operations, trade, and people's livelihoods. Careful consideration should be given to minimize such disruptions.
- **Erosion of public trust:** Prolonged restrictions or a lack of transparency during a state of emergency can damage public trust in the government. Upholding transparency and public engagement are critical.

4) Terminate the state of emergency

The state of emergency will be lifted through a legal process, following established criteria, once the threat subsides and the situation stabilizes.

Declaring a state of emergency: challenges and good practices

CHALLENGES	GOOD PRACTICES
Timing and criteria for the declaration, since declaring emergency too early or too late can have negative consequences, such as unnecessary resource allocation or compromised response effectiveness.	▸ Develop clear and objective **criteria** for declaring a state of emergency. ▸ Establish a **rapid assessment** and decision-making process. ▸ Conduct **regular drills and exercises** to practice decision-making under pressure.
Resource implications, declaring a state of emergency can place a significant financial burden on public resources and may lead to resource shortages.	▸ Conduct regular **resource assessments** and gap analysis. ▸ Develop **contingency plans** for resource allocation and procurement. ▸ Establish **financial management** and accountability systems.
Communication problems such as inaccurate or untimely information can lead to public panic, misinformation and disinformation.	▸ Develop a comprehensive **communication plan,** including key messages and target audiences. ▸ Designate a **single spokesperson** to provide consistent and accurate information. ▸ Utilize **multiple channels** for communication, including traditional and social media. ▸ See Chapter 4 Communication with the public in the Response Section.

7. REQUEST FOR INTERNATIONAL ASSISTANCE

When the CBRN situation assessment and resource gap analysis identify the need for international assistance, countries can request support through various multi- and bi-lateral mechanisms, either with or without declaring a state of emergency. While a declaration of emergency may facilitate certain aspects of international aid, it is not a prerequisite for requesting assistance. Countries can seek support through bilateral agreements, regional frameworks, or international organizations, depending on specific needs and circumstances.

KEY ACTIONS

1 Evaluate need for assistance	Assess national capacity and identify critical gaps.
2 Determine potential assistance sources	Find international organizations suited for the incident.
3 Activate notification systems	Use pre-established communication channels.
4 Submit formal request	Clearly state incident details, needs, and priorities.
5 Evaluate incoming offers	Match assistance offers with identified gaps.
6 Coordinate deployment	Ensure smooth arrival and integration of resources.
7 Continuous reassessment	Adjust requests as the situation evolves.
8 Maintain communication	Regularly update partners and share lessons learned.

1) Evaluate the need for international assistance

CBRN managers and decision-makers at the strategic level should be able to address the needs for an effective emergency response in a timely manner. One of their tasks is to assess the available resources, their locations, and how to best utilize them. As part of this assessment, CBRN managers must determine whether there are critical shortfalls in national capabilities and resources. In other words, they need to verify if the national response system is overwhelmed, at risk of being overwhelmed, or simply lacks the necessary resources, such as expertise, equipment, medical supplies, etc. When the required resources are not available at the national level, CBRN managers and decision-makers may need to consider requesting international assistance. If international assistance is required, CBRN managers should prioritize requests to address the most critical factors first.

Examples of gaps that could require international assistance:

- Limited medical teams: If a country lacks medical teams trained to treat a specific CBRN agent, or the number of casualties exceeds the existing medical capacity, requesting international deployment of specialized medical teams is essential.
- Lack of decontamination capacity: If the incident involves widespread environmental contamination and the decontamination units are insufficient, requesting additional units from international partners would expedite the clean-up process.
- Complexities of nuclear incident: In the case of a nuclear incident, the expertise and resources required for containment, decontamination, and radiation management might necessitate international assistance, especially from organizations like the IAEA.

2) Identify the international organizations, regional or international partners which can provide assistance for the particular CBRN incident and the identified gaps

CBRN managers and decision-makers should utilize existing databases of international organizations, regional and international partners, and the capabilities they can offer for specific CBRN incidents.

3) Activate international notification systems

Once the decision is made to request international assistance and the international organization(s) and partner(s) are identified, CBRN managers should use pre-established channels and existing communication protocols to liaise with them. This may involve using specific communication platforms or formats that have been agreed upon in advance.

4) Formal request for international assistance

When crafting the request, CBRN managers and decision-makers should integrate the following information, using clear and concise language:

- **Precise location of the incident.** Provide the most specific location information possible for assistance delivery, such as **geographic coordinates.** (e.g. latitude and longitude for precise location identification), **zone or region,** and **street address or unique landmarks.**
- **Information on the type of CBRN agent** involved. Knowing the specific agent allows international partners to:
  - **Offer targeted assistance:** Provide resources specifically suited to the type of CBRN agent, such as antidotes for chemical agents or vaccines for biological agents.
  - **Develop appropriate response protocols:** International organizations and partner countries can recommend specific decontamination procedures, medical treatment protocols, and public health advisories based on the agent's characteristics.

- **Assess potential threat level:** Understanding the agent's toxicity, dispersal patterns, and potential long-term health effects is crucial for threat assessment and response planning.
- **Provide information on the likely dispersal route** of the CBRN agent and areas potentially at risk, based on weather conditions and topography. Such information can allow international partners to:
  - **Initiate preventive measures:** Neighboring countries can take steps to protect their populations, such as issuing evacuation orders for at-risk areas or preparing decontamination procedures for incoming refugees.
  - **Monitor environmental impact:** International organizations and bi-lateral partners can coordinate air and water monitoring efforts to track the spread of the CBRN agent and assess the extent of contamination.
  - **Coordinate regional response:** Facilitate a more comprehensive regional response by informing neighboring countries and international partners about potential cross-border impacts.

- **Specific resource need** to be categorized by priority such as:
  - **Critical needs:** there may be a lack of medical teams trained to treat a specific biological agent. CBRN managers might request deployment of specialized medical teams from international partners.
  - **High-value needs:** while there may be decontamination units available, requesting additional units from international partners could expedite decontamination efforts and minimize the affected area.
  - **Complementary:** additional PPE may be requested from international partners to ensure sufficient PPE for all responders.
- **Current national response efforts** to avoid duplication, including:
  - **Existing resource deployments:** Quantify the resources you have already deployed, including medical teams, decontamination units, other resources (e.g., emergency response teams, search and rescue teams.
  - **Areas where national capabilities are sufficient.** Briefly explain areas where national capabilities are sufficient or insufficient.
- **Emphasize urgency:** Depending on the type of situation, highlight the associated need for assistance.
- **Designate a point of contact:** Provide contact information for a designated point of contact within your organization who can provide further details and coordinate the response.
- **Follow up:** After sending the request, follow up through appropriate channels to ensure that the request has been received and is being processed.

This is an example of information to be included in the request of assistance for international assistance:

REQUEST FOR INTERNATIONAL ASSISTANCE
CBRN INCIDENT

LEVEL OF EMERGENCY: ☐ URGENT (Under a delay of 1 week)
☐ EMI URGENT (From 1 week to 1 month)
☐ NON-URGENT (More than 1 month)

1. Requesting State: _____ Number of pages: ____
2. Subject of request: _____
3. Is this an official request made under an international assistance convention?
   ☐ No
   ☐ Yes → Convention reference:
4. Competent authority: Name:
   Function:
   Tel:
   E-mail:
5. Requesting state coordinator: Name:
   Function:
   Tel:
   E-mail:
6. Type of event:
   ☐ Chemical (C) ☐ Biological (B) ☐ Radiological (R) ☐ Nuclear (N)
7. Event description:
8. Actions taken:
9. Actions planned:
10. Challenges:
11. Type of assistance:
    ☐ Expertise ☐ Technical ☐ Expertise and technical
    ☐ On-site assistance (OSA) ☐ External based assistance (EBA)
12. Expected duration of the mission:
    ☐ Short term (Less than a week)
    ☐ Medium term (Between one week and one month)
    ☐ Long term (More than a month)
    ☐ Unknown
13. Details concerning the nature and extent of the assistance requested:
14. ☐ Further information in attachment, see:
15. Next steps to be followed by you (assisting State):
    ☐ Acknowledge receipt of this message
    ☐ Contact competent authority/Requesting state coordinator to get more information within 24 hours after the receipt of this message
    ☐ Send back your response/proposal to the request within 48 hours
16. If you respond positively, an Assistance Action Plan (AAP) will be developed in collaboration with your competent authority and your Assisting state coordinator to work out the details, including all financial, diplomatic, organizational and logistical aspects.

5) Evaluate incoming offers of assistance

The next step is to ensure that the offer of assistance is aligned with the request. CBRN managers should consider the following aspects:

- **Assess the compatibility** of offered equipment and protocols with national standards. Different countries may have variations in equipment design, operational procedures, and safety protocols for CBRN response. Incompatible equipment may require additional training for personnel or pose operational challenges.

  Example: A partnering nation might offer a mobile decontamination unit that utilizes a different decontamination agent than the one the country's teams are trained for. This might require additional training or limit the unit's immediate effectiveness.

- **Implement the pre-defined system** to efficiently **match received offers with national needs.** Make use of existing databases, pre-defined matching algorithms and human review to assess compatibility beyond technical specifications and identifying unforeseen needs.

  - **Databases:** A well-organized database of offered resources with clear categorization (type, quantity, capabilities) allows for quick identification of relevant resources. For example, the database could categorize offers by equipment type (e.g., decontamination units, medical supplies, communication equipment), quantity available, and specific capabilities (e.g., mobile vs. stationary decontamination units, type of medical treatment offered).

- **Matching algorithm** can prioritize offers based on critical gaps, high-value resources, or complementary capabilities. For example, the system could prioritize offers that address critical needs identified earlier (e.g., lack of medical supplies for treating a specific CBRN agent), followed by offers with high-value resources (e.g., specialized CBRN survey equipment) and then those that offer complementary capabilities (e.g., additional decontamination units).
- **Human review** is essential to verify compatibility and address unforeseen needs, such as language barriers, technical differences in equipment, and the nuances of local contexts. For example, human reviewers might identify logistical challenges in integrating offered equipment with existing national infrastructure.

- **Assess the alignment of offered assistance with identified needs.** Evaluate if the resources offered directly address critical needs or provide complementary support. For example, a partner might offer a highly specialized medical team trained in treating a specific biological agent, while another might offer a large stockpile PPE for first responders. Both offers are valuable but address different needs.

6) Coordinate deployment and integration

Effective coordination of deployment and integration of the international assistance received is crucial for ensuring a seamless response. This involves:

- Using pre-defined **communication channels** and points of contact for international partners and agreed **joint response strategies.**
- Coordinating **logistics** (transportation, accommodation):
  - Facilitate the arrival and deployment of international personnel and equipment.
  - Arrange accommodation and logistical support for international responders.
  - Expedite **customs clearance** by authorizing the use of pre-clearance arrangements and standardized documentation templates.
- Prioritizing **deployment:** Based on the needs assessment and offer evaluation, prioritize the deployment of international resources to address critical gaps first, then high-value needs, and lastly complementary needs.

7) Continuous reassessment

Regularly reassess the situation as the CBRN incident evolves. Be prepared to escalate or de-escalate international assistance requests based on changing circumstances.

8) Maintain communication and information sharing throughout the process

CBRN managers can consider the following aspects:

- Regularly **update** partners on the situation:
  - Provide ongoing briefings on the evolving situation and response efforts.
  - Share data on casualty numbers, containment progress, and environmental monitoring.

- Share **lessons learned** for future preparedness:
  - After the incident, conduct a joint after-action review with international partners.
  - Identify areas for improvement in communication, coordination, and resource sharing.

Request for international assistance: challenges and good practices

CHALLENGES	GOOD PRACTICES
Accurately **assessing the scale and nature of the incident** to determine specific assistance requirements.	▸ Conduct a rapid **needs assessment** to identify critical gaps. ▸ **Prioritize requests** based on urgency and impact. ▸ Use **pre-defined** CBRN assistance request packages.
Navigating **complex bureaucratic procedures** and obtaining necessary approvals.	▸ Establish **streamlined procedures** for requesting and receiving international assistance. ▸ Designate a **dedicated point of contact** to facilitate communication and coordination. ▸ Pre-establish bilateral/multilateral CBRN **assistance agreements.**
Limited resources for coordinating and managing international assistance.	▸ Create a **digital platform** where all international aid offers are registered, tracked, and matched with needs automatically. ▸ Maintain small, **versatile teams** trained to handle multiple coordination tasks rather than specialized units. ▸ Use **pre-approved procedures** and digital forms to speed up aid acceptance and customs clearance. ▸ Set up a **virtual coordination center** allowing remote management and reducing physical staff needs. ▸ Implement **automated scheduling and tracking tools** to maximize limited logistics resources.
Miscommunication and misunderstandings due to language and cultural differences.	▸ Use clear and **concise language** in all communications. ▸ Employ qualified **interpreters and translators**.
Coordinating the **arrival, deployment, and departure** of international assistance teams.	▸ Develop a comprehensive **logistics plan**, including transportation, accommodation, and security. ▸ Establish clear **communication channels** and coordination mechanisms. ▸ Appoint a **dedicated liaison officer** to facilitate communication and coordination with international partners. ▸ Establish **procedures to pre-clear the import** of essential CBRN equipment received following a request for assistance.

CHALLENGES	GOOD PRACTICES
Technical **compatibility** of the equipment that is sent for assistance.	▸ Establish equipment **standardization** protocols that define the specifications, performance criteria, and operational requirements for CBRN equipment. ▸ Maintain **compatibility guidelines** for CBRN equipment to ensure that all involved can effectively communicate, operate, and support one another during response efforts. ▸ Create, in the planning phase, technical **integration procedures** that outline compatibility requirements, interoperability testing protocols, and operational guidelines to ensure that equipment that may be received through international assistance can be seamlessly integrated with existing equipment and procedures.

ANNEX I. BIBLIOGRAPHY

SECTION I. PLANNING

Risk assessment

- **European Union.** (n.d.). *Integrated Directory on the CBRN Risk Spectrum*. Examines the types of CBRN risks and CBRN risk trajectories, analyzing risks in terms of perceptions, sources, and factors relevant to the EU CBRN policy context.
- **FEMA.** (n.d.). *The National Risk Index*. A dataset and online tool illustrating U.S. communities most at risk for 18 natural hazards, leveraging source data for natural hazard and community risk factors.
- **Homeland Security.** (2018). *Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide Comprehensive Preparedness Guide (CPG) 201*. 3rd Edition. Provides guidance for conducting a Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR), formerly State Preparedness Report.
- **International Atomic Energy Agency (IAEA).** (n.d.). *Nuclear Security*. Provides international consensus guidance on all aspects of nuclear security to support States as they work to fulfil their responsibility for nuclear security.

CBRN emergency planning

- **International Atomic Energy Agency (IAEA).** (1997). *Methods for the development of emergency response preparedness for nuclear or radiological events*. Provides practical advice and tools for emergency planning.
- **World Health Organization (WHO).** (2021). *WHO Guidance on Preparing for National Response to Health Emergencies and Disasters*. The purpose of this guidance is to assist countries in developing or updating their National Health Emergency Response Operations Plan for all hazards, taking a multi sectoral, whole-of-society approach.
- **World Health Organization (WHO).** (n.d.). *Chemical and Biological Deliberate Events Course Series*. Hosts online training to provide basic knowledge for managing the consequences of a CBDE.
- **World Health Organization (WHO).** (n.d.). *Academy: Chemical Training*. Learning center for the global health and care workforce and health sector decision-makers.
- **World Health Organization (WHO).** (n.d.). *Deliberate Event Webpage: Factsheets, Q&As, and Useful Material*.

Resource management

- **Federal Emergency Management Agency (FEMA).** (n.d.). *Logistics Technical Assistance Program*. A program within FEMA's Logistics Management Directorate, responsible for policy, guidance, standards, execution, and governance of logistics support, services, and operations.
- **Federal Emergency Management Agency (FEMA).** (n.d.). *National Event Management System (NIMS)*. Guides government, nongovernmental organizations, and the private sector in working together to prevent, protect, mitigate, respond to, and recover from events. Includes a toolkit with resources and tools for implementing NIMS concepts and principles.
- **Federal Emergency Management Agency (FEMA).** (2021). *National Event Management System (NIMS) Resource Management Guidance*. Provides a standardized framework for state, local, tribal, and federal agencies to effectively manage resources during emergencies, including CBRN threats.
- **Federal Emergency Management Agency (FEMA).** (n.d.). *Resource Inventory System (RIS)*. A centralized, secure, cloud-hosted solution enabling organizations to inventory resources in alignment with NIMS resource typing definitions and National Qualification System (NQS) positions.
- **Government of South Australia, Department of the Premier and Cabinet.** (n.d.). *State Emergency Management Plan*. Presents principles defining the responsibilities of government agencies and participating organizations in emergency management activities.

Infrastructure resilience

- **United Nations Office for Disaster Risk Reduction (UNDRR).** (2020). *Addressing the Infrastructure Failure Data Gap: A Governance Challenge*. Highlights the importance of integrating risk reduction and resilience considerations into public investment and structural reforms to ensure the effective allocation of recovery resources.
- **United Nations Office for Disaster Risk Reduction (UNDRR).** (2020). *Making Critical Infrastructure Resilient: Ensuring Continuity of Service - Policy and Regulations in Europe and Central Asia*. Assesses the inclusion of risk reduction and resilience measures in national policies and regulations for protecting critical infrastructure in Europe, Central Asia, and the South Caucasus.
- **United Nations Office for Disaster Risk Reduction (UNDRR).** (2024). *Principles for Resilient Infrastructure*. Describes principles, key actions, and guidelines to enhance national-scale resilience and ensure the continuity of critical services such as energy, transport, water, and digital communications.
- **United Nations Office for Disaster Risk Reduction (UNDRR).** (2020). *Working Paper: Options for Addressing Infrastructure Resilience*. Provides recommendations, lessons learned, and opportunities for building resilient infrastructure.

Public awareness and communication during CBRN incidents

- **Alabama Public Health.** (n.d.). *Needs Assessment for Crisis and Emergency Risk Communication*. Provides multiple checklists to assess the current state of crisis and emergency communication assets.
- **American Association for the Advancement of Science (AAAS).** (n.d.). *Communication Toolkit*. Provides relevant information related to communication to the public based on technical or scientific terminology.
- **Centers for Disease Control and Prevention (CDC).** (2014). *CERC: Crisis Communication Plans*. Provides information about multiple stages in preparing communication plans, including crisis phases, the table for communication, developing the plan, applying the plan during the first 24–48 hours, and applying the crisis plan throughout the response.
- **European Centre for Disease Prevention and Control (ECDC).** (2022). *Risk Communication and Community Engagement Approaches During the Monkeypox Outbreak in Europe*. Provides a recent case study of communication with the public during a biological event.
- **Federal Emergency Management Agency (FEMA).** (n.d.). R eady Campaign: CBRN-Related Sections. Provides examples in multiple languages of communication with the public in order to raise awareness on topics related to CBRN issues.
- **International Atomic Energy Agency (IAEA).** (2012). *Communication with the Public in a Nuclear or Radiological Emergency* Provides practical guidance for public information officers on the preparation for and response to a nuclear or radiological emergency, and to fulfil in part functions assigned to the IAEA in the Convention on Assistance.
- **International Federation of Red Cross and Red Crescent Societies (IFRCS).** (2021). CBRN Public Awareness and Public Education for Disaster Risk Reduction. Provides examples of communication with the public in order to raise awareness on CBRN issues.
- **Interpol.** (2017). *Public Messages to Use in the Immediate Response to a CBRN Attack*. Provides guidance on how to prepare messages before the CBRN event to increase efficiency of communication with the public if an event occurs.
- **RAND.** (2003). Individual Preparedness and Response to Terrorism: Chemical, Radiological, Nuclear, and Biological Attacks. As an example of communication with the public and raising awareness, it presents an individual's strategy for preparing for, and responding to, terrorist attacks involving chemical, radiological, nuclear, and biological weapons.
- **World Health Organization (WHO).** (n.d.). *Risk Communication and Community Engagement (RCCE) Action Plan Guidance COVID-19 Preparedness and Response*. This tool is designed to support risk communication, community engagement staff and responders working with national health authorities to develop, implement and monitor an effective action plan for communicating effectively with the public.

Key international and regional treaties and conventions relevant to CBRN threats

Chemical Weapons

- *Chemical Weapons Convention (CWC)*. (1997). Prohibits the development, production, stockpiling, and use of chemical weapons and requires the destruction of existing stockpiles.

Biological Weapons

- *Biological Weapons Convention (BWC)*. (1975). Prohibits the development, production, and acquisition of biological agents or toxins, except for peaceful research and medical purposes.

Nuclear Weapons

- *Treaty on the Non-Proliferation of Nuclear Weapons (NPT)*. (1970). Aims to prevent the spread of nuclear weapons and promote cooperation in the peaceful use of nuclear energy.
- *Comprehensive Nuclear-Test-Ban Treaty (CTBT)*. (Not yet in force). Prohibits all nuclear weapon test explosions or any other nuclear explosions but has widespread international support.

Radiological Materials

- *Convention on the Physical Protection of Nuclear Material (CPPNM)*. (1987). Requires states to establish measures for the physical protection of nuclear material to prevent unauthorized removal.
- *Amendment to the CPPNM*. (2004). Expands the scope of the original CPPNM to include nuclear materials during international transport and in peaceful use.
- *Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management*. (2001). Promotes public health and environmental protection in radioactive waste management.

Additional Instruments - United Nations Security Council Resolutions

- *Resolution 1540*. (2004). Affirms that the proliferation of CBRN materials constitutes a threat to international peace and requires UN member states to prevent non-state actors from acquiring these materials.
- *Resolution 1673*. (2006). Urges states to strengthen measures to prevent CBRN proliferation and establishes the 1540 Committee for monitoring implementation.
- *Resolution 1810*. (2008). Addresses nuclear proliferation threats and emphasizes compliance with Resolutions 1540 and 1673.
- *Resolution 1975*. (2011). Stresses the need to prevent terrorists from acquiring CBRN materials and calls for enhanced international cooperation.
- *Resolution 2325*. (2016). Reaffirms Resolution 1540 and calls for stronger national measures to prevent CBRN proliferation.

Regional Agreements

- Treaty of Tlatelolco. (1967). Establishes a nuclear-weapon-free zone in Latin America and the Caribbean.
- South Pacific Nuclear Free Zone Treaty (Rarotonga Treaty). (1986). Prohibits nuclear weapons in the South Pacific region.
- Treaty on the Southeast Asia Nuclear Weapon-Free Zone (Treaty of Bangkok). (1997). Establishes a nuclear-weapon-free zone in Southeast Asia.
- African Nuclear Weapon Free Zone Treaty (Treaty of Pelindaba). (2009). Prohibits nuclear weapons in Africa.
- Treaty on a Nuclear-Weapon-Free Zone in Central Asia (Semipalatinsk). (2009). Establishes a nuclear-weapon-free zone in Central Asia.

Examples of agreements for CBRN assistance

- Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency. (2005).
- EU Action Plan to Enhance Preparedness Against Chemical, Biological, Radiological, and Nuclear Security Risks. (2017).
- The Association of Southeast Asian Nations (ASEAN) Agreement on Disaster Management and Emergency Response (AADMER). (2005).

Comprehensive CBRN Training Program

- **World Health Organization (WHO).** (n.d.). *Simulation Exercise Manual*. Tool for planning, conducting and evaluating simulation exercises for outbreaks and public health emergency preparedness and response.
- **European Centre for Disease Prevention and Control (ECDC).** (2021). Simulation exercises in public health settings: Step-by-step exercise design.
- **Service for Foreign Policy Instruments (FPI) & Joint Research Centre (JRC).** (2024). Organization and Implementation of a CBRN Counter-Terrorism Field Exercise: Guiding Document. EU CBRN Centres of Excellence Initiative.
- **North Atlantic Treaty Organization (NATO).** (2011). *CBRN defence standards for education, training, and evaluation* (ATP-3.8.1 Vol. III). NATO Standardization Office.

SECTION II. RESPONSE

Unified command and coordination

- **U.S Federal Emergency Management Agency (FEMA).** (2022). *Emergency Operations Center How-to Quick Reference Guide*. This document can serve as an example of guidelines related to setting up, operating, maintaining and deactivating an Emergency Operations Center that successfully meets the jurisdiction's needs.

Communication with the public

- **Centers for Disease Control and Prevention (CDC).** (n.d.). *Crisis and Emergency Risk Communication (CERC) Manuals*. Includes manuals on: Psychology of a Crisis, Messages and Audiences, Community Engagement, Crisis Communication Plans (Including Checklist 4–1: First 48 Hours, Checklist 4–2: Notification Schedule, Checklist 4–3: Public Information Emergency Response Call Tracking), Spokesperson, and Working with the Media.
- **Caron Chess, PhD, & Lee Clarke, PhD.** (2007). *Facilitation of Risk Communication During the Anthrax Attacks of 2001: The Organizational Backstory*. Provides a case study.
- **EUvsDesinfo.** (n.d.). *Website* with disinformation cases, databases, and resources.
- **Government of South Australia, Department of the Premier and Cabinet.** (n.d.). *State Emergency Management Plan - Part 3C: Security and Emergency Management Arrangements*. Provides guidance on public information and warnings.
- **International Atomic Energy Agency (IAEA).** (2012). *Communication with the Public in a Nuclear or Radiological Emergency*. Provides guidance for public information officers on the preparation for and response to a nuclear or radiological emergency, and to fulfil in part functions assigned to the IAEA in the Convention on Assistance.
- **International Atomic Energy Agency (IAEA).** (2021). *Emergency Communication: What Have We Learned Since Fukushima?*. Provides insights on the communication efforts during the Fukushima nuclear plant incident.
- **INTERPOL and World Animal Health Organization (WHOA).** (2024). *Countering Disinformation and Misinformation in Animal Health Emergencies*. The guidelines introduce some key strategies for organizations working in animal health emergencies on how to manage disinformation and misinformation.
- **Pan American Health Organization (PAHO).** (2009). *Information Management and Communication in Emergencies and Disasters: Manual for Disaster Response Teams*. Provides guidelines on producing reports and distributing information for different audiences, how to manage communication media, and planning the work of communication during emergency response.

- **Rogers, M. B., Krieger, K., Jones, E., & Amlot, R.** (2014). *Responding to Emergencies Involving Chemical, Biological, Radiological, and Nuclear (CBRN) Hazards*. Provides information for emergency responders about public responses to CBRN incidents.
- **United Nations Interregional Crime and Justice Research Institute (UNICRI).** (2020). *Stop the Virus of Disinformation: The Malicious Use of Social Media by Terrorist, Violent Extremist, and Criminal Groups During the COVID-19 Pandemic*. Describes how groups took advantage of the COVID-19 pandemic to expand their activities and jeopardize the efficacy and credibility of response measures by governments.
- **United Nations Interregional Crime and Justice Research Institute (UNICRI).** (2023). *Handbook to Combat CBRN Disinformation*. Aims at enhancing understanding of CBRN disinformation on social media while developing competencies to prevent and respond to disinformation.
- **U.S. Department of Homeland Security.** (n.d.). *Crisis Communications Planning: Establishing Joint Information Centers* Provides guidance to state and local government departments on establishing and operating a joint information center during an emergency.
- **World Health Organization (WHO).** (2024). *Managing False Information in Health Emergencies: An Operational Toolkit*. Provides procedures for the detection and handling of false information, following a five-step process involving signal detection, verification, risk assessment, response design and outreach.
- **World Health Organization (WHO).** (n.d.). *Infodemic Management Course Series*. Provides an overview of the strategies, good practices, methods and tools that can be used in the field to prevent, prepare for and respond to the infodemic.

Investigation, intelligence gathering, and forensics

- **United Nations Interregional Crime and Justice Research Institute (UNICRI).** (2022). *A Prosecutor's Guide to Chemical and Biological Crimes*. Provides police and civil prosecutors, and relevant investigative agencies, with guidance to support the successful prosecution of incidents involving the deliberate use of a chemical or biological agents, in addition to awareness and insight into the current and emerging challenges related to the investigation and prosecution of such crimes.
- **United Nations Interregional Crime and Justice Research Institute (UNICRI).** (2024). *A Prosecutor's Guide to Radiological and Nuclear Crimes*. Includes practical tips, lessons learned, and best practices derived from real criminal case examples, serving as useful precedents. Step-by-step recommendations for the successful investigation and prosecution of RN crimes are integral parts of the Guide.

Recovery

- **Federal Emergency Management Agency (FEMA).** (2016). *National Disaster Recovery Framework*. Information on how the whole community builds, sustains, and coordinates delivery of recovery capabilities.
- **International Federation of Red Cross and Red Crescent Societies (IFRC).** (2012). *IFRC Recovery programming guidance*. IFRC Recovery programming guidance. Describe the main elements of a recovery programming approach required to deliver high-quality, timely and accountable humanitarian assistance.
- **United Nations Office for Disaster Risk Reduction (UNDRR).** (2015). *Sendai Framework for Disaster Risk Reduction 2015–2030*. Includes the section "Priority 4: Enhancing disaster preparedness for effective response and to "Build Back Better" in recovery, rehabilitation and reconstruction".
- **World Health Organization (WHO).** (2024). *Planning for health system recovery Guidance for application in countries*. Supports countries to prioritize and mainstream health system recovery through effective planning as part of efforts to build health system resilience.
- **World Bank.** (2018). *Building back better: achieving resilience through stronger, faster, and more inclusive post-disaster reconstruction*. Shows the benefits of building back better could be greatest among the communities and countries that are hit by disasters most intensely and frequently.

ANNEX II. ADDITIONAL RESOURCES

Checklist to verify the communication with the public strategy

Note: This form is provided solely for illustrative purposes. It is a generic example and must be thoroughly reviewed and adapted to align with the specific needs, context, and structure of your CBRN preparedness program. Adjustments should be made to reflect your country's unique legal framework, organizational setup, resource availability, and operational requirements. This document is not intended to serve as a finalized or one-size-fits-all solution.

1. Activation of communication plans

- Was the pre-existing communication plan activated promptly?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____

2. Establishment of a joint information center

- Was a joint information center or a similar structure established to coordinate communication?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____
- Does the center involve communication professionals from all relevant agencies and organizations?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____
- Are key resources (e.g., internet, electricity) in place to support the center's operation?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____

3. Clarity and accuracy of messages

- Is the public provided with a clear and concise description of the situation?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____

- Do the messages include safety measures, evacuation instructions, or shelter-in-place guidance?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____
- Are the messages fact-based, evidence-supported, and balanced?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____
- Is ambiguity or uncertainty acknowledged, with explanations about evolving circumstances?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____
- Are government response efforts outlined clearly (e.g., medical support, countermeasures)?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____
- Is information provided on available services (e.g., medical facilities, decontamination)?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____
- Are frequent updates issued to keep the public informed of new developments?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____
- Are updates shared quickly enough to address rumors or misinformation?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____

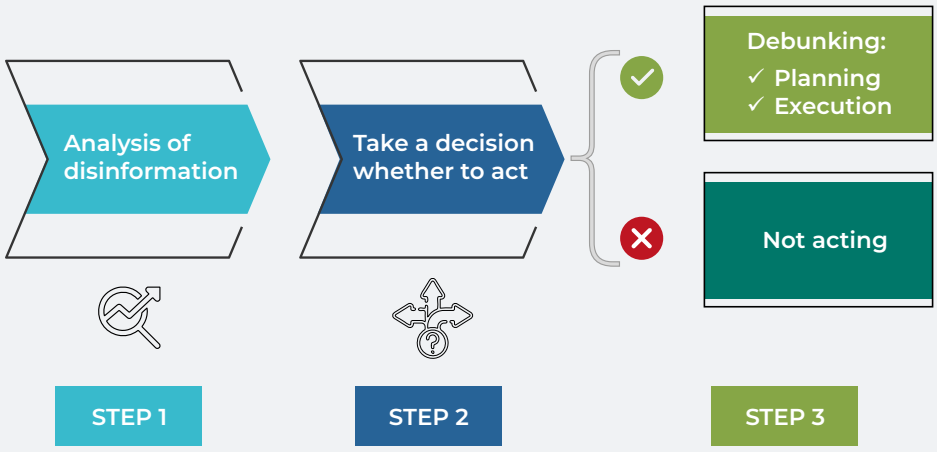
4. Audience-specific communication

- Is the communication tailored to different audience needs (e.g., local population, vulnerable groups)?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____

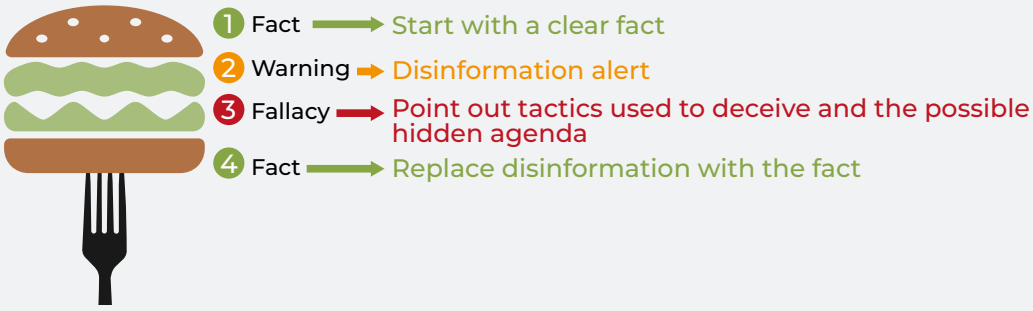
- Are messages provided in multiple languages and accessible formats (e.g., for people with disabilities)?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____
- Are cultural sensitivities considered in the messaging?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____
- Is misinformation or disinformation actively monitored and addressed promptly?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____
- Are accurate corrections or clarifications provided in response to false claims?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____
- Are efforts made to engage with the public through Q&A sessions, town halls, or press conferences?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____
- Are public concerns addressed in a timely and transparent manner?
  - ☐ Yes
  - ☐ No
  - ☐ Comments: _____

Communication with the public: debunking disinformation

Debunking: There are several actions that can be taken when dealing with disinformation and misinformation, particularly, debunking the false claims. Debunking can be defined as the process of showing that something, such as a belief or theory, is not true, or to show the falseness of a story, idea, statement, etc. For more details see Handbook to combat CBRN disinformation.



As it is the case when drafting a message, it is essential to define the target audience, the means and the accessibility before debunking. After this planning phase, the debunking can be done through different strategies. One of those strategies to draft a message is known as the "truth sandwich".



- **Start with the facts that support the verified information:** Debunking should begin with a sentence that contains verified factual information. The sentence should not be complex and should have explanatory relevance. The fact should not be written in a negative form (e.g. "this claim is not true").
- **Warning and addressing the false claim:** The second element in the truth sandwich consists of:

  a. An explicit warning that the information, visual, or audio content that is about to be presented is false;

b. A short description of the disinformation. It is important to repeat the false information **only once,** directly before the correction. Unnecessary repetitions should be avoided to minimize promulgating or reinforcing the false claim ("backfire effect").

- **Explain the fallacy:** An explanation of the false claim and why it is wrong is the third element in the truth sandwich. Please include:

  a. Explanation of why the source of disinformation is not credible (e.g. a video has been manipulated or a picture has been associated to a wrong context) and what the real intent (e.g. undermining trust in a government or making profit) of the disinformation is;

  b. Corrections should be presented in contrast to the false information to ensure a clear rebuttal. Use simple and concise language, as well as graphic elements to help highlight the facts, such as a larger font or different colors. Add some details, but not too many.

  c. The credibility and background of the person or organization performing the debunking is an important element. Referencing credible sources will help generate confidence in the correct information.

- **Restate the fact:** Replace the disinformation with the facts at the end of the process. By replacing the false information with the facts, the true version of events is made clear and understandable.

Request for international assistance

Non-comprehensive list of international and regional organizations and agencies

ORGANIZATION	GENERAL DESCRIPTION	CAPABILITIES
African Union (AU)	The African Union (AU) is a continental organization representing all 55 countries of Africa. Established in 2002, it promotes unity, peace, and development across Africa.	The African Union strives to achieve unity, solidarity, and socio-economic integration among African countries, while promoting peace, security, democratic governance, and human rights across the continent. It also aims to advance sustainable development, strengthen international cooperation, and position Africa as an influential player in global affairs through collaboration in science, technology, and public health initiatives.
Association of Southeast Asian Nations (ASEAN)	ASEAN is a regional organization in Southeast Asia with 10 member countries. Their main goals are to promote economic growth and trade among members; maintain peace and stability in the region; and foster cultural exchange and cooperation.	The ASEAN CBR Network, established during the 12th ASEAN Defence Ministers' Meeting in 2018, aims to strengthen regional counter-terrorism preparedness and cooperation against CBR threats by providing integrated incident response, fostering multilateral collaboration, sharing expertise, deepening professional ties, and enhancing regional safety in alignment with international standards.
European Union (EU)	The European Commission is composed of the College of Commissioners from 27 EU countries providing political leadership across a number of core areas including but not limited to, Climate action, Environment, Security policy, Justice and fundamental rights and public health. The EU CBRN Centres of Excellence Initiative deals with CBRN topics. The aim of the Initiative is to support Partner Countries and regions in strengthening CBRN risk mitigation and an all-hazards security governance in Partner Countries, following a voluntary and demand-driven approach.	The European Union (EU) Chemical, Biological, Radiological and Nuclear (CBRN) Risk Mitigation Centres of Excellence (CoE) is a global initiative funded and implemented by the European Union as part of its goal to promote peace, stability and conflict prevention. The EU support is provided to implement a wide range of CBRN risk mitigation activities including needs and risk assessments, national and regional action plans, capacity building activities, legal framework reviews, tabletop and real time (including cross-border) field exercises, inter-regional exchange of best practices and lessons learnt.

ORGANIZATION	GENERAL DESCRIPTION	CAPABILITIES
European Union Agency for Criminal Justice Cooperation (EUROJUST)	The European Union Agency for Criminal Justice Cooperation is responsible for the coordination of national authorities to assist in cross-border criminal investigations including terrorism and environmental crime. EUROJUST provides specific assistance in a number of areas including but not limited to, judicial cooperation including the life cycle of the case, transmission of information, joint investigative teams, extraditions and consultative forums.	EUROJUST can assist in setting up and coordinating Joint Investigation Teams comprising investigators and prosecutors from multiple EU member states; facilitate meetings between national authorities from different EU countries to share information, coordinate investigative strategies, and ensure a smooth exchange of evidence. EUROJUST can help member states navigate the complex legal framework surrounding mutual legal assistance requests, offers training programs for prosecutors and investigators on topics related to CBRN incidents. provide expert advice on relevant EU legislation related to CBRN incidents. EUROJUST published a CBRN-E Handbook to provide EU practitioners, in particular prosecutors and police authorities, with an overview of EU and international legislation applicable to CBRN.
European Union Agency for Law Enforcement Cooperation (EUROPOL)	The European Union's Law Enforcement agency, based in The Hague. Supporting 27 EU Member States, EUROPOL provides assistance and advice to law enforcement operations with a focus on organised crime, terrorism and cybercrime. They provide access to specialists and forums to support the training of chemical, biological, radiological and nuclear experts and investigators, in conjunction with the European Police College (CEPOL).	Provides access to CBRN expertise to Member States, supports Joint Investigative Teams (JITs) and provides forensics support to law enforcement agencies. CBRN training is provided to Member States through CEPOL.

ORGANIZATION	GENERAL DESCRIPTION	CAPABILITIES
International Atomic Energy Agency (IAEA)	The IAEA is mandated to accelerate and expand the contribution of atomic energy in promoting peace, health and prosperity globally. Its staff strives to ensure that assistance provided, either directly, or under its supervision or control, is not used in such a way as to further any offensive military operations. The agency aims to encourage and assist research, development and practical application of atomic energy for peaceful uses. Additionally, it fosters the exchange of scientific and technical information related to the peaceful use of atomic energy.	The IAEA supports Member States in capacity building regarding radiological crime scene management and nuclear forensics at national, regional and international levels. This support includes providing guidance, conducting training courses, workshops and expert missions, offering advisory services and coordinating research projects in these areas. The agency also plays a role in organizing international events such as conferences and technical meetings, serving as forums to exchange good practices, discuss scientific developments and foster international cooperation.
International Criminal Police Organization (INTERPOL)	An intergovernmental organization providing advanced international police cooperation to its 196 member countries. INTERPOL is uniquely placed to collect intelligence in its data repository system and share intelligence to support national criminal analysis and investigation. Specialized Chemical, Biological, Radiological and Nuclear analytical products, trainings and resources are provided by INTERPOL's CBRNE and Vulnerable Targets Sub-Directorate.	INTERPOL's support is coordinated through its headquarters in Lyon, France, and its network of National Central Bureaus (NCBs). INTERPOL'S CBRNE and Vulnerable Targets Sub-Directorate offers support to Member Countries through three main pillars: › Police Data Management and Analysis: INTERPOL is uniquely placed to collect intelligence on CBRNE threats from its 196 member countries, manage and analyze such police data and share it via analytical products and the publications of notices. Sharing of intelligence allows member countries to inform national law enforcement efforts on CBRNE criminality and terrorism and supports national investigation. › International Engagement: Interpol connects member countries law enforcement agencies, with international organizations, academia, and the private sector to address CBRNE threats, recognizing that law enforcement cannot counter these threats alone. INTERPOL represents law enforcement interests in international CBRNE forums and advocating for their needs in global security initiatives.

ORGANIZATION	GENERAL DESCRIPTION	CAPABILITIES
		› Specialized Expertise: INTERPOL offers access to law enforcement CBRNE specialists to provide capacity building and training activities to member countries. Each Unit identify high-threat countries and develop tailored action plans with national authorities to deliver hands-on training packages. Depending on the specific request for assistance from member Country and the needs on the ground, support may include operational response and investigative support, or victim identification related to CBRNE incidents.
International Security and Emergency Management Institute (ISEMI)	Professional platform of former and active police, military, internal security officers, prosecutors and emergency management experts, working mainly in the field of Counter-CBRN-E Terrorism and Crime.	Provides support and assistance in detection and investigation of CBRN-E crime, CBRN-E crime scene analysis, crime scene investigation, CBRN-E threat and hazard detection, sampling and identification, CBRN-E crime and criminal profiling, profiling in protective security and covert operation, vulnerability profiling of public places, and risk and threat assessment including the use of new technologies. Conduct training, tabletop and field exercises with simulants and live CBRN agents.
North Atlantic Treaty Organization (NATO)	NATO is a political and military alliance of countries from Europe and North America. Its members are committed to protecting each other from any threat.	NATO's CBRN Defence Policy outlines strategies to counter CBRN threats, emphasizing resilience, deterrence, and defense. It integrates military and non-military tools, promotes international cooperation, and aligns with broader strategies on hybrid warfare, cybersecurity, and climate change impacts. The policy addresses emerging challenges like WMD proliferation, terrorism, and geopolitical tensions, and incorporates gender perspectives and climate adaptation measures to enhance preparedness and operational effectiveness.

ORGANIZATION	GENERAL DESCRIPTION	CAPABILITIES
Nuclear Forensics International Technical Working Group (ITWG)	The objective of the ITWG is to advance the scientific discipline of nuclear forensics and to provide a common approach and effective technical solutions to competent national or international authorities that request assistance. The ITWG fights nuclear smuggling by improving ways to trace illegal materials and sharing best practices with countries.	The Nuclear Forensics International Technical Working Group (ITWG) helps countries investigate the source of illegal nuclear materials. They share knowledge and best practices to stop nuclear smuggling and unauthorized possession. ITWG conducts exercises and publishes guidelines to strengthen global nuclear security.
Nuclear Threat Initiative (NTI)	The NTI is a nonprofit, nonpartisan global security organization focused on reducing nuclear and biological threats imperiling humanity. NTI establishes practical solutions to strengthen nuclear security by convening leaders, developing actionable recommendations, and tracking progress on commitments.	The NTI works to strengthen global nuclear security and verifiably prevent the proliferation of nuclear materials that could be used to create nuclear weapons. The program collaborates closely with governments, international organizations, industry, and non-governmental organizations to fortify security for nuclear materials or eliminate materials where possible. The NTI Nuclear Security Index evaluates nuclear security conditions in 175 countries and Taiwan. NTI's website provides information on treaties, organizations, and regimes relating to nuclear security, including the amended Convention on Physical Protection of Nuclear Materials and Facilities and the International Convention for the Suppression of Acts of Nuclear Terrorism.
Organization of American States (OAS)	The OAS is a continental organization founded in 1948 to promote democracy, human rights, security, and development across the Americas. It consists of 35 member states.	OAS focuses on promoting regional cooperation, providing technical assistance, and enhancing member states' capabilities to prevent, detect, and respond to CBRN threats. Through its Inter-American Committee Against Terrorism (CICTE), the OAS works on capacity-building initiatives, legislative harmonization, and fostering partnerships to strengthen national and regional preparedness and resilience against CBRN incidents.

ORGANIZATION	GENERAL DESCRIPTION	CAPABILITIES
Organisation for the Prohibition of Chemical Weapons (OPCW)	OPCW is an intergovernmental organization and implementing body of the Chemical Weapons Convention. Based in the Hague, Netherlands, oversees implantation of the Convention.	The OPCW provides training and assistance to member states in several key areas: Chemical Event Response: Training for first responders on safe identification, decontamination, and casualty management during chemical incidents. National Implementation Programs: Supporting countries in developing and implementing national plans to counter chemical threats. Capacity Building: Offering technical assistance to enhance national capabilities for preventing, detecting, and responding to chemical incidents. Additionally, the OPCW can deploy investigative teams and provide expertise in sample collection, transportation, and analysis of high-risk chemicals and chemical weapons.
United Nations Interregional Crime and Justice Research Institute (UNICRI)	UNICRI is mandated to assist intergovernmental, governmental and nongovernmental organizations in their efforts to formulate and implement improved policies in the fields of crime prevention and justice; act with its partners in the international community to facilitate international law enforcement cooperation and judicial assistance; support the respect of international instruments and other standards; advance understanding of crime-related problems and foster just and efficient criminal justice systems.	UNICRI's Threat Response and Risk Mitigation Unit focuses on enhancing security governance by addressing emerging threats and mitigating risks related to organized crime, terrorism, and CBRN hazards. It provides tailored capacity-building programs, policy guidance, and innovative tools to strengthen national and regional security frameworks. The unit also fosters international cooperation to improve preparedness and response to complex global security challenges.

ORGANIZATION	GENERAL DESCRIPTION	CAPABILITIES
United Nations Office for Disarmament Affairs (UNODA) - BWC Implementation Support Unit	BWC Implementation Support Unit sits within the Geneva Branch of the UNODA with a mandate to provide administrative support and assistance to States Parties including national implementation and confidence building measures as well provide Secretariat to meetings of the BWC.	Article VII of the Biological Weapons Convention disposes that each State Party undertakes to provide or support assistance to any Party to the Convention which so requests, if the UN Security Council decides that such Party has been exposed to danger as a result of violation of the Convention. However, it provides no procedure for States to request such assistance nor for the international community to deliver it. The BWC is a treaty governed by its States Parties. The BWC ISU was established in 2006 and it has no mandate, legal personality or capacity to undertake coordination of response and assistance operations in case of use of biological weapons.
United Nations Office on Drugs and Crime (UNODC)	Through its CBRN Terrorism Prevention Programme, the UNODC assists countries in adopting international legal frameworks to combat nuclear and radiological terrorism. The program provides technical and legal support, training criminal justice officials to investigate, prosecute, and adjudicate CBRN-related offenses effectively.	The UNODC's CBRN Terrorism Prevention Programme helps Member States combat the risks of CBRN terrorism by promoting adherence to and implementation of international legal instruments. It supports countries in developing national legislation, provides training for criminal justice officials, and enhances international cooperation in investigating, prosecuting, and adjudicating CBRN-related crimes. Additionally, the program offers tools such as eLearning modules, webinars, and model legislative provisions to strengthen national capacities and foster compliance with global security frameworks.

ORGANIZATION	GENERAL DESCRIPTION	CAPABILITIES
World Customs Organization (WCO)	WCO is an independent intergovernmental body whose mission is to enhance the effectiveness and efficiency of Customs administrations. WCO represents 186 Customs administrations across the globe that collectively process approximately 98% of world trade.	WCO's Compliance and Enforcement Package (CEP) has been developed in order to assist Members to address the high-risk areas for Customs enforcement. As part of the CEP Concept there are 4 key components that are highlighted: Partnerships, Technology and Infrastructure, Tools, and Operational activities, all revolving around 5 key risk areas for Customs Compliance and Enforcement. WCO Policy Commission endorsed five key risk areas for Customs enforcement, namely, revenue assurance; drugs enforcement; health and safety/IPR; security; and environment.
The World Organization for Animal Health (WHOA)	WHOA provides technical support with regards to animal disease control, eradication and response to disease outbreaks including those that are transmissible from animal to human. The Biological Threat Reduction initiative provides a detailed strategy and a number of guidelines in relation to high-risk pathogens, investigation and analysis.	WOAH works to improve animal health and welfare globally by setting international standards, sharing expertise, and supporting veterinary services. It monitors and responds to animal diseases, including zoonoses, to safeguard public health and food security. Through its initiatives, WOAH enhances the capacity of nations to detect, prevent, and control health risks at the animal-human-environment interface.
World Health Organization (WHO)	WHO is the leading international organization for health matters. It is a specialized agency of the United Nations with a focus on global public health. It promotes health and well-being around the world, especially for vulnerable populations.	The WHO develops and disseminates guidelines for health professionals on medical management of CBRN exposures and public health measures to mitigate risks. They also conduct training programs for health workers to strengthen their capacity to respond effectively. The WHO plays a role in global health surveillance systems and facilitates communication and collaboration between countries and health organizations during a CBRN event. The WHO provides technical assistance to member countries in developing national CBRN preparedness plans and risk assessments and works with partners to ensure countries have access to essential medicines and equipment needed to manage casualties of such incidents.

Requesting assistance from international organizations

Requesting assistance from the International Atomic Energy Agency (IAEA)

General aspects

The IAEA maintains the international Emergency Preparedness and Response (EPR) framework, which is based on international legal instruments, IAEA Safety Standards and operational arrangements. IAEA assists Member States in building the capacity for emergency preparedness and response through dedicated trainings, workshops and exercises; supports MSs in evaluating and improving their national EPR arrangements through Emergency Preparedness Review mission (EPREV); and manages a network for MSs able and willing to provide assistance in case of Radiological or nuclear emergency (RANET). The IAEA maintains its Incident and Emergency System to efficiently implement its role in response to nuclear or radiological incidents and emergencies, regardless of their origin, through the Incident Emergency Centre-IEC, the IAEA's focal point. The IEC plays an essential role during radiological or nuclear emergency in notification and information exchange, providing assistance, and coordinating among international relevant organizations. Additionally, the IEC-IAEA role has been expanded to include the assessment of potential emergency consequences and prognosis of possible emergency progression.

1. **Eligibility Criteria:** The International Atomic Energy Agency (IAEA) provides assistance to member states under specific circumstances. Here are the general eligibility criteria for a country to request assistance from the IAEA:

   - **Membership:** Member States are countries that have ratified the IAEA Statute and participate in its programs. These countries can formally request assistance from the IAEA. Non-member states can receive assistance from the IAEA in certain circumstances, particularly if the assistance is related to global safety, security, and safeguards issues. Such assistance is typically provided on a case-by-case basis and often requires special arrangements or agreements with the IAEA.
   - **Compliance with IAEA's mandate:** Any assistance or collaboration must align with the IAEA's mandates, which emphasize the peaceful use of nuclear technology, radiation safety, nuclear security, and implementing safeguards agreements.

2. **Prerequisites:** To facilitate a structured and efficient response, certain prerequisites must be met before requesting assistance from the IAEA. Understanding and fulfilling these prerequisites ensures that the assistance process is seamless, timely, and effective.

   - Member States should designate, through official channels, a Competent Authority (CA) and inform the IAEA accordingly. Governments may designate more than one CA. This CA should be authorized to notify and receive notifications, request assistance, respond to requests from other Member States, request information, and provide additional information in cases of radiological or nuclear emergencies.
   - The Competent Authority (CA) should register at least one staff member on the Unified System for Information Exchange in Incidents and Emergencies (USIE) as

the "USIE Administrator." This staff member is responsible for registering other staff members as "Publishers." Their role includes publishing/receiving notifications, requesting/offering assistance, and requesting/providing information.

- The MS should define, and make it known to the IAEA the communication channels (E-mail, Fax, SMS), by which the CA and point of contacts will receive alert when a message or notification is published on USIE
- In case of radiological or nuclear emergency, communication with IEC should be through USI, fax and phone call.

3. **Type of Assistance:** States Party of the Assistance Convention and Member States of the IAEA can request assistance from and/or through the IAEA during radiological or nuclear emergency incidents. This assistance or support, coordinated through the IEC, encompasses various technical and operational activities to manage and mitigate the emergency effectively. The types of assistance provided by the IAEA are divided into groups: Field assistance and external-based support. These include source search and recovery, radiation survey, sampling and analysis, decontamination, medical support, dose assessment, nuclear installation assessment and advice.

4. **Request of assistance process:**

- Complete the form "Request for Assistance" available on USIE and submit it through USIE or to the IEC by fax, indicating the following: the nature and type of event; location; name and address of organization in charge of response; name and contact details of person assigned to liaise with the IEC-IAEA; type of assistance requested (preference of MS providing assistance could be included as well any objection for some MSs)
- Inform the Permanent Mission in Vienna about the request
- Once the request message is received through official channels, the IEC verifies the request, and an alert is sent to the MSs for providing assistance
- Member States registered on RANET provide an offer of assistance to the IAEA through USIE and the requesting state is alerted.
- The IEC prepares an assistance action plan in coordination with the national point of contact, send to the requesting MS for signature and approval. The Action Plan includes details about the assisting MSs and assistance team composition if field assistance is required.
- Once the assistance mission accomplished, the IEC provides the requesting MS a detailed assistance mission report.

References:

- Operational Manual for Incident and Emergency Communication. EPR-IECComm 2019. International Atomic Energy Agency, Vienna, 2020
- Operations Manual for Incident and Emergency Communications, Contact Details, Checklists and Forms, EPR-IECComm, Attachment 1 (2012), International Atomic Energy Agency, Vienna, Austria, 2012

Requesting international assistance from the Organisation for the Prohibition of Chemical Weapons (OPCW)

General aspects

1. Eligibility Criteria

The Organisation for the Prohibition of Chemical Weapons (OPCW) provides assistance to member states under specific circumstances. Here are the general eligibility criteria for a country to request assistance from the OPCW:

- **Membership:** The country must be a State Party to the Chemical Weapons Convention (CWC). This means it has ratified or acceded to the CWC and is thereby bound by its provisions.
- **Compliance with CWC Obligations:** The requesting State Party should be in compliance with its obligations under the CWC. This includes not developing, producing, acquiring, stockpiling, or using chemical weapons, and destroying any existing chemical weapons and production facilities.

2. Type of Assistance

Assistance can be requested in various forms, including:

- **Building protective capacity against chemical weapons:** States Parties are permitted to develop national protection programs against chemical weapons and the Convention ensures that they can receive assistance, if they require it, to build their national capacity to respond to the use of chemical weapons. The OPCW provides specific programs in this area, including detection and alarm systems, protective and decontamination equipment, training on medical assistance and treatment, and advice on protective measures. States Parties are permitted to develop national protection programs against chemical weapons and the Convention ensures that they can receive assistance, if they require it, to build their national capacity to respond to the use of chemical weapons. The OPCW provides specific programs in this area, including detection and alarm systems, protective and decontamination equipment, training on medical assistance and treatment, and advice on protective measures.
- **Investigation of alleged use:** If a State Party suspects the use of chemical weapons on its territory or against its nationals, it can request an investigation. There are two ways in which an investigation of alleged use (IAU) of chemical weapons can be triggered. The first is by submission of a request by a State Party for a challenge inspection under Article IX where the alleged use occurred in another State Party. The second is by submission of a request for assistance in accordance with Article X in a situation in which chemical weapons are alleged to have been used against the requesting State Party, or riot control agents are alleged to have been used against it as a method of warfare. In addition, the Technical Secretariat provides advice and assistance, upon request, to States Parties that do not seek an investigation or a rapid response but do wish to benefit from the Secretariat's technical expertise. For example, such expertise may be needed for identifying chemical agents used in an attack. If a State Party suspects the use of chemical weapons on its territory or against its nationals, it can request an investigation. There are two ways in which an investigation of alleged use (IAU) of chemical weapons can be triggered. The

first is by submission of a request by a State Party for a challenge inspection under Article IX where the alleged use occurred in another State Party. The second is by submission of a request for assistance in accordance with Article X in a situation in which chemical weapons are alleged to have been used against the requesting State Party, or riot control agents are alleged to have been used against it as a method of warfare. In addition, the Technical Secretariat provides advice and assistance, upon request, to States Parties that do not seek an investigation or a rapid response but do wish to benefit from the Secretariat's technical expertise. For example, such expertise may be needed for identifying chemical agents used in an attack.

- **Supporting the implementation:** For enhancing national capacities related to the implementation of the CWC. OPCW supports National Authorities through providing courses, workshops, and guidance on a number of mandated tasks for National Authorities such as filing declarations for the industrial verification regime. The National Authority Mentorship and Partnership Program promotes country-to-country support, networking, and cooperation. For enhancing national capacities related to the implementation of the CWC. OPCW supports National Authorities through providing courses, workshops, and guidance on a number of mandated tasks for National Authorities such as filing declarations for the industrial verification regime. The National Authority Mentorship and Partnership Program promotes country-to-country support, networking, and cooperation.
- **Building readiness to respond by providing protection advice:** Provide advice to States Parties concerning means of protection and the implementation of national protection programs. It does this through a data-bank of information and through courses and workshops on protection and civil defense. The Secretariat organizes trainings for first responders, government experts and emergency response units designed to build and develop national and regional capabilities and emergency response systems against the use, or threat of use, of chemical weapons. Provide advice to States Parties concerning means of protection and the implementation of national protection programs. It does this through a data-bank of information and through courses and workshops on protection and civil defense. The Secretariat organizes trainings for first responders, government experts and emergency response units designed to build and develop national and regional capabilities and emergency response systems against the use, or threat of use, of chemical weapons.
- **Supporting the victims:** This includes a Practical Guide for Medical Management of Chemical Warfare Casualties.
- **Preventing the re-emergence of chemical weapons:** Ensuring that all existing stockpiles of chemical weapons are destroyed, and by putting in place a framework – made up of a set of binding obligations on States Parties and a verification regime run by the Technical Secretariat – to ensure that chemical weapons do not re-emerge.: Ensuring that all existing stockpiles of chemical weapons are destroyed, and by putting in place a framework – made up of a set of binding obligations on States Parties and a verification regime run by the Technical Secretariat – to ensure that chemical weapons do not re-emerge.

- **OPCW Catalyst:** Online hub to connect representatives from Member States and scientific communities to OPCW online applications, official documents, and information on meetings, training opportunities, and events. Online hub to connect representatives from Member States and scientific communities to OPCW online applications, official documents, and information on meetings, training opportunities, and events.

3. Request Procedure

Article X. Assistance and Protection Against Chemical Weapons

- **Paragraph 7: Providing assistance**

  Each State Party undertakes to provide assistance through the Organization and to this end to elect to take one or more of the following measures:

  - To contribute to the voluntary fund for assistance to be established by the Conference at its first session;
  - To conclude, if possible not later than 180 days after this Convention enters into force for it, agreements with the Organization concerning the procurement, upon demand, of assistance;
  - To declare, not later than 180 days after this Convention enters into force for it, the kind of assistance it might provide in response to an appeal by the Organization. If, however, a State Party subsequently is unable to provide the assistance envisaged in its declaration, it is still under the obligation to provide assistance in accordance with this paragraph.

- **Paragraph 8: Request for assistance**

  Each State Party has the right to request and, subject to the procedures set forth in paragraphs 9, 10 and 11, to receive assistance and protection against the use or threat of use of chemical weapons if it considers that:

  (a) Chemical weapons have been used against it;

  (b) Riot control agents have been used against it as a method of warfare; or

  (c) It is threatened by actions or activities of any State that are prohibited for States Parties by Article I.

- **Paragraph 9: Request process**

  The request shall be submitted to the Director-General, who shall transmit it immediately to the Executive Council and to all States Parties. The Director-General shall immediately forward the request to States Parties which have volunteered to dispatch emergency assistance in case of use of chemical weapons or use of riot control agents as a method of warfare, or humanitarian assistance in case of serious threat of use of chemical weapons or serious threat of use of riot control agents as a method of warfare to the State Party concerned not later than 12 hours after receipt of the request.

  The Director-General shall initiate, not later than 24 hours after receipt of the request, an investigation in order to provide a foundation for further action. He shall complete the investigation within 72 hours and forward a report to the Executive Council. If additional time is required for completion of the investigation, an interim

report shall be submitted within the same time-frame. The additional time required for investigation shall not exceed 72 hours. It may, however, be further extended by similar periods. The investigation establishes relevant facts related to the request as well as the type and scope of supplementary assistance and protection needed.

Paragraph 10. Decision on providing assistance

The Executive Council shall meet not later than 24 hours after receiving an investigation report to consider the situation and shall take a decision by simple majority within the following 24 hours on whether to instruct the Technical Secretariat to provide supplementary assistance. The Technical Secretariat shall immediately transmit to all States Parties and relevant international organizations the investigation report and the decision taken by the Executive Council. When so decided by the Executive Council, the Director-General shall provide assistance immediately. For this purpose, the Director-General may cooperate with the requesting State Party, other States Parties and relevant international organizations. The States Parties shall make the fullest possible efforts to provide assistance.

Paragraph 11. Immediate action

If the information available from the ongoing investigation or other reliable sources would give sufficient proof that there are victims of use of chemical weapons and immediate action is indispensable, the Director-General shall notify all States Parties and shall take emergency measures of assistance, using the resources the Conference has placed at his disposal for such contingencies.

In addition, an Assistance Coordination and Assessment Team (ACAT) can be deployed. ACAT may be 1) deployed by the Technical Secretariat in response to a request for Assistance and Protection from Request SP (RSP), 2) Determine the type and scope of Assistance needed and to carry out assessment activities, which provided an important basis for decision making process of the Policy-Making Organs (PMO) OPCW, 3) Carry out assistance and protection coordination activities on-sit, if so requested by RSP. Such activities include: coordination of emergency response to use or threat of use of Chemical Weapons (CW) and/or Toxic Industrial Chemicals (TICs), provide expert advice to National Authority, consequence management measure related to the use or threat of use of CW, and deployment with PPE.

Additional considerations on offering and providing assistance

States Parties are also required to offer assistance to others, through the OPCW. This assistance can take three forms. First, States Parties may contribute to the Voluntary Fund for Assistance, as these are funds to be used to provide assistance if a State Party is attacked or threatened with chemical weapons.

Second, States Parties may enter into agreements with the OPCW regarding the provision of assistance upon demand. The first agreement of this kind-a memorandum of understanding between the Islamic Republic of Iran and the OPCW-concerned the provision of emergency medical assistance teams and facilities for treating chemical weapon casualties at Iranian hospitals.

Third, States Parties may decide to declare the kind of assistance they might provide in response to an appeal by the OPCW to support another State Party under attack with chemical weapons or under threat of attack.

Requesting international assistance from the World Health Organization (WHO)

General aspects

WHO plays an essential role improving local health systems and coordinating the global response to health threats. Geneva headquarters the 6 regional offices, 150 country offices and other offices around the world, making the WHO the most probably be the first international organization on site for the response. While WHO manages risks and emergencies due to all hazards especially as custodian of the International Health Regulations (2005) (IHR). WHO has a response capability including and operational CBRN capability, and works closely with Member States and partners, including through the internal emergency rosters, external emergency rosters, and Global Outbreak Alert and Response Network (GOARN) and other expert networks – to strengthen national, regional and global capacities to prevent, detect and respond to outbreaks, consistent with the IHR. WHO also has specific responsibilities and accountabilities within the global humanitarian system as the lead agency of the IASC Global Health Cluster. Similarly, WHO leads and coordinates the emergency medical teams (EMTs) initiative globally, and assists ministries of health in coordinating the arrival, registration, licensing, reception and tasking of emergency medical teams when necessary. Operational partnerships such as GOARN, the external standby partnerships through the international humanitarian partners, the Global Health Cluster and the EMT initiative have important roles in building national capacities for preparedness and response.

The World Health Organization (WHO) provides assistance to Member States under specific circumstances. Here are the general eligibility criteria for a country to request assistance from the WHO:

1. **Membership:** WHO primarily provides assistance to its Member States. However, WHO also extends support to non-Member States and other entities under specific circumstances to ensure global health security and address public health emergencies effectively.

2. **Compliance with International Health Regulations (IHR):** Both member and non-Member States are encouraged to adhere to the IHR to facilitate timely and effective responses to public health emergencies.

3. **Types of Assistance:** The types of assistance offered include: capacity evaluation and assessment through the IHR implementation (SPAR, JEE, NAHPS and the NSAT, capacity building, awareness provision and information sharing, and direct support during response.

4. **Means for Assistance:** Assistance can be requested in various forms, including:

- **International Health Regulations (IHR):** provide an overarching legal framework that defines countries' rights and obligations in handling public health events and emergencies that have the potential to cross borders. The IHR are an instrument of international law that is legally-binding on 196 countries, including the 194 WHO Member States. They create rights and obligations for countries, including the requirement to report public health events. The Regulations also outline the criteria to determine whether or not a particular event constitutes a "public health emergency of international concern". At the same time, the IHR require countries

to designate a National IHR Focal Point for communications with WHO, to establish and maintain core capacities for surveillance and response, including at designated points of entry.

- **Global Surveillance System:** Picks up public health threats 24 hours a day, 365 days a year. Once an event is verified, WHO assesses the level of risk and sounds the alarm to help protect populations from the consequences of outbreaks, disasters, conflict and other hazards.

  Within 48 hours (ideally) of an emergency, WHO might:

  - Grade the severity of the event if needed.
  - Activate the incident management system (IMS) with a designated team functioning out of emergency operating centres in Geneva, and in the regional and country offices.
  - Releases funds from WHO's Contingency Fund for Emergencies.
  - Deploy field teams (the CBRN surge capacity roster is deployed at this stage with CBRN protective equipment and decontamination means to support MoH in the Member State); and activates global stockpiles of essential supplies, including personal protective equipment, medicines, and vaccines.
  - Establish network communication systems and base camps, where needed.
  - Communicate the risk to the community and neighboring countries through official International Health Regulations (2005) procedures, Disease Outbreak News and social media.
  - Activate the Global Health Cluster, the Global Outbreak Alert and Response Network (GOARN) in case of non-deliberate events, emergency medical teams and standby partners.
  - WHO also develops new technologies to be able to detect and track new health events in the most difficult settings, such as the Early Warning, Alert and Response System (EWARS).

- **The Global Outbreak Alert and Response Network (GOARN):** Network of over 250 technical institutions and networks globally that respond to acute public health events with the deployment of staff and resources to affected countries. It aims to deliver rapid and effective support to prevent and control infectious diseases outbreaks and public health emergencies when requested in case of non-deliberate events.

- **Early Warning, Alert and Response System (EWARS):** An application designed to improve disease outbreak detection in emergency settings, such as in countries in conflict or following a natural disaster. Specifically, EWARS consists of an online, desktop, and mobile application that can be rapidly configured and deployed within 48 hours of an emergency being declared.

- **Public Health Emergency Operations Centre Network (EOC-NET):** Created to promote best practice and standards, support EOC capacity building in countries and to strengthen collaboration and coordination between EOCs and response partners for effective response.

- **Emergency Medical Teams Initiative EMT:** The purpose of the EMT initiative is to improve the timeliness and quality of health services provided by national and international Emergency Medical Teams and enhance the capacity of national health systems in leading the activation and coordination of this response in the immediate aftermath of a disaster, outbreak and/or other emergency.
  - It enables countries to improve their own national capacity, which they are then able to use to assist other countries in emergencies.
  - It enables affected countries to accept and use EMTs in a timely, coordinated manner.
  - Host governments and affected populations can depend on EMTs from the list to arrive trained, equipped and capable of providing the intervention promised. Victims and their families can expect the clinical teams treating them to be of a safe minimum standard.
  - Each team has unique individuals with various skill sets. Identifying these differences and placing them into the field requires coordination and communication to ensure the correct gaps are filled. EMT staff help facilitate and coordinate this placement.
  - Guidance on aspects related to biological weapons, chemical incidents, radiation emergencies, and deliberate events.

Other support means

- **The Health-Security Interface Technical Advisory Group (HSI-TAG):** Provides independent advice to WHO related to strategic priorities and plans of action on specific topics relating to the health-security interface. Some of the areas include:
  - Public Health Intelligence
  - Chemical and Biological preparedness and readiness
  - Civil-military relations
  - Risk communications
  - Misinformation/disinformation
  - Biosafety and biosecurity
  - National and international policy, regulation and guidance.
- **Joint External Evaluation (JEE):** Voluntary, collaborative, multisectoral process to assess country capacities to prevent, detect and rapidly respond to public health risks whether occurring naturally or due to deliberate or accidental events. The JEE helps countries identify the most critical gaps within their human and animal health systems in order to prioritize opportunities for enhanced preparedness and response.
- **National Self-Assessment Tool (NSAT):** this tool is based on the JEE tool and is intended to support WHO Member States by providing an evaluation of national capacity to manage the risks posed by Biological, Chemical and Cyber Deliberate Events (DEs), including the ability to mount a well-coordinated, multisectoral response. This tool could be used in conjunction with or independently of the JEE tool depending on the will of the MS.

Preparedness material

- Training platforms:
  - OpenWHO: Deliberate Event channel.
  - WHO Academy: chemical training.
- WHO Deliberate Event webpage with factsheets, Q&As and useful material.
- Simulation exercise

United Nations
Interregional Crime and Justice
Research Institute

ROADMAP

on effective CBRN planning and response for policymakers and CBRN managers

INTRODUCTION

Responding to chemical, biological, radiological, and nuclear (CBRN) incidents poses complex challenges due to their potentially severe and long-lasting consequences. These incidents can trigger health crises, social disruption, psychological trauma, environmental degradation, and significant economic losses. They also may disrupt critical infrastructure, essential services, and trade, creating instability and fostering fear and mistrust within affected communities.

To effectively mitigate CBRN risks, a comprehensive, multidimensional strategy is essential, encompassing prevention, detection, planning, response, and recovery. This requires integrated risk assessment, policy development, resource allocation, technological innovation, and specialized expertise, alongside coordinated efforts across agencies. A robust legal framework is also crucial to clearly define responsibilities, authorize emergency actions, and ensure the swift and effective deployment of emergency powers when needed.

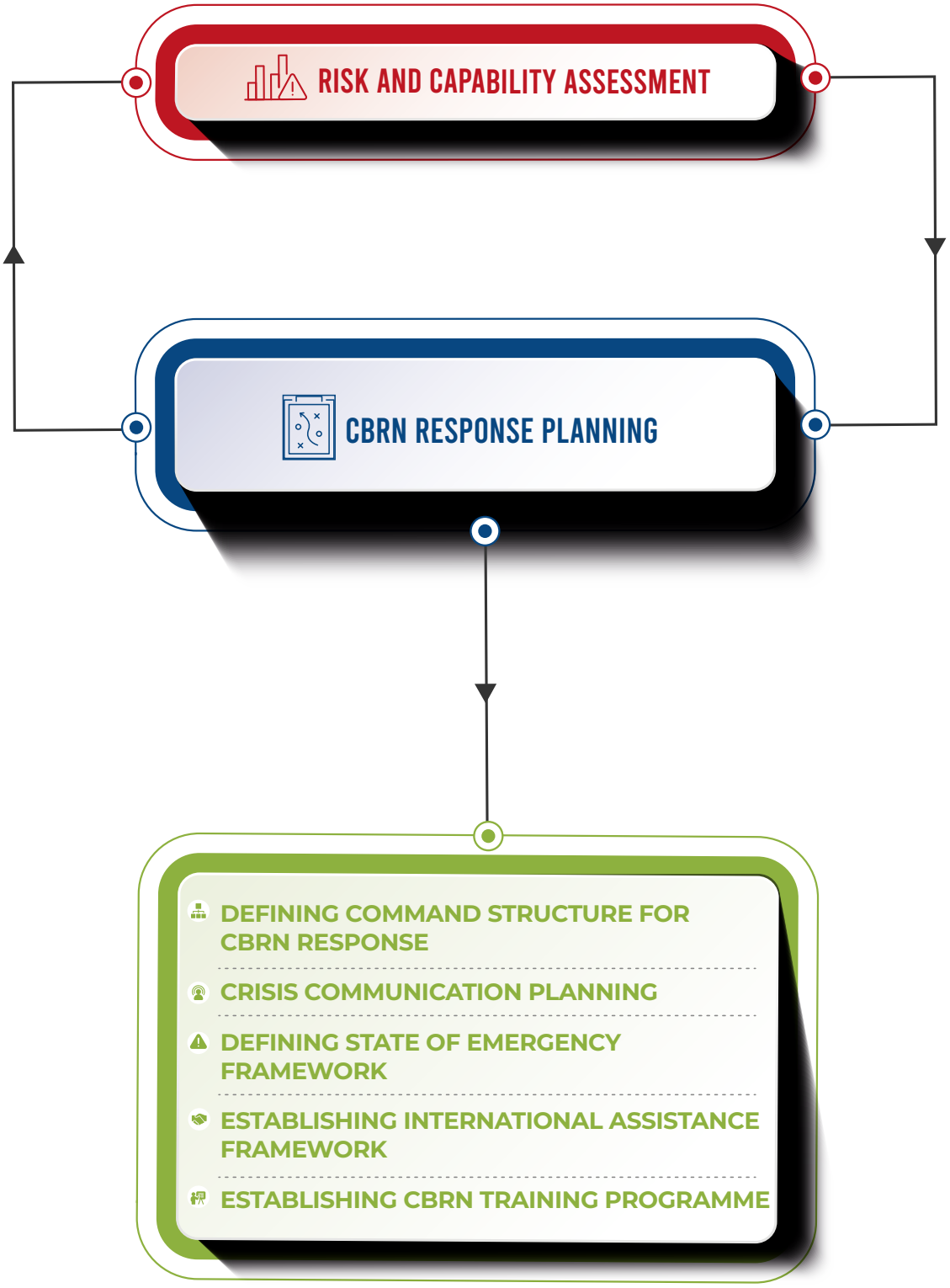
UNICRI, with financial support from the U.S. Department of State, has developed *The Toolkit on Effective CBRN Planning and Response for Policymakers and CBRN Managers* to support these efforts. The document provides practical guidance for strategic-level decision-makers, including policymakers, emergency management officials, and CBRN managers responsible for planning and overseeing responses to CBRN incidents.

As a companion to the Toolkit, UNICRI has also developed this *Roadmap on Effective CBRN Planning and Response for Policymakers and CBRN Managers*, designed as a quick reference guide for policymakers and managers responsible for CBRN planning and response. While the Toolkit provides structured steps—including key actions, challenges, and good practices—to guide complex decision-making at the strategic level, the Roadmap distills the key steps helping users identify gaps and set priorities regarding response strategies, plans, and procedures. More specifically, the Roadmap summarized the Toolkit's key actions into a streamlined reference, ensuring that policymakers and managers can quickly grasp and apply the most critical aspects of CBRN planning and response.

Divided into two main sections, the Roadmap covers both CBRN planning[1] and response, breaking down complex processes into structured steps to support strategic decision-making.

1 Since the Roadmap is designed for policymakers and CBRN managers, the term "CBRN planning" is used instead of "CBRN preparedness." The Planning Section of the Roadmap aims to guide the development of strategies, policies, and procedures to address potential CBRN threats, whereas "CBRN preparedness" focuses more on ensuring the readiness and capabilities necessary to effectively implement those plans during a CBRN incident.

SECTION I - PLANNING



RISK AND CAPABILITY ASSESSMENT

Calculate the risk:

- ☐ **Identify threats:** Understand potential CBRN threats, their sources, and possible impacts by analyzing structured interviews, affinity grouping, risk source analysis, checklists, scenario analysis, intelligence reports, historical incidents, and expert judgment.
- ☐ **Assess vulnerabilities:** Examine critical systems and population weaknesses, focusing on components that are more likely to fail under extreme conditions in relation to the identified threats.
- ☐ **Evaluate impact:** Analyze the magnitude and scope of likely outcomes of an event and the availability of backup resources by using impact rating scale (1-5) to assess the severity of possible impacts: Minimal (1), Minor (2), Moderate (3), Major (4), and Catastrophic (5).
- ☐ **Determine likelihood:** Assess the probability of threats materializing using likelihood rating scale (1-5): Very Low (1), Low (2), Medium (3), High (4), and Very High (5).
- ☐ **Calculate risk:** Determine the overall level of risk by applying a risk matrix that integrates threats, vulnerabilities, and the likelihood of each threat materializing.

Assess the capabilities:

- ☐ **Assess capabilities:** Examine the availability of trained personnel, specialized equipment, operational plans, and infrastructure required for an effective response.

CBRN RESPONSE PLANNING

CBRN planning is a cycle that includes the following actions:

- ☐ **Develop response plans:** Create CBRN response plans that clearly define roles and responsibilities among stakeholders, outline specific actions and Standard Operation Procedures (SOPs).
- ☐ **Manage resources:** Ensure that the CBRN response plans are equipped with the necessary resources, including personnel, equipment, supplies, facilities and financial resources. Develop and maintain a comprehensive interagency database that collects information on available resources for responding to CBRN incidents.
- ☐ **Build capacities:** Prepare staff and agencies to respond effectively to CBRN incidents by focusing on specialized and interagency training to enhance skill sets, operational compatibility, and equipment interoperability. This includes competency assessments, leadership development, and well-being support.
- ☐ **Evaluate plans:** Analyze the components of response plans, assess performance during incidents or exercises, and recommend improvements to enhance preparedness and effectiveness.

DEFINING COMMAND STRUCTURE FOR CBRN RESPONSE

- ☐ **Define roles and responsibilities:** Define a Unified Command Structure (UCS) and clearly select stakeholder roles to provide overall response direction and make critical decisions. The UCS can operate at three incident management levels – strategic, tactical, and operational – depending on the scale and complexity of the incident.
- ☐ **Set activation thresholds:** Define risk-based indicators for activating the UCS such as threat indicators, confirmed or suspected releases of hazardous materials, potential for widespread contamination, credible intelligence reports, multiple casualty reports with consistent symptoms, and breaches of containment in high-risk facilities.
- ☐ **Pre-identify incident commanders:** Select potential incident commanders (and their successors) based on factors such as the scale and complexity of potential incidents, the nature of the CBRN threat, geographic considerations, and the expertise required for specific response functions.
- ☐ **Define communication protocols:** Establish protocols for real-time information exchange during incidents. Use secure, redundant communication channels to prevent disruptions, and ensure standardized terminology and predefined reporting formats to minimize misunderstandings and enhance operational efficiency.
- ☐ **Define inter-agency collaboration mechanisms:** Establish robust interagency coordination mechanisms to integrate resources, expertise, and capabilities from multiple stakeholders.
- ☐ **Regular review:** Periodically update the UCS and ensure it remains aligned with current risk landscapes, operational capabilities, and stakeholder needs.

CRISIS COMMUNICATION PLANNING

- ☐ **Assess the existing communication structure:** Use a checklist of indicators (e.g. existence of communication plans, spokespersons, verification and clearance protocols, et) to identify gaps or weaknesses in current public communication systems.
- ☐ **Develop a communication plan:** Create an effective CBRN communication plan that clearly assigns responsibilities, establishes verification protocols, and defines authorities for releasing information. This plan should include the establishment of a joint information center, training for spokespersons, and the use of diverse communication methods.
- ☐ **Raise public awareness:** Strengthen community preparedness by engaging trusted community leaders, conducting drills, providing accessible educational materials tailored to local contexts, and fostering two-way communication through feedback mechanisms.

DEFINING EMERGENCY AUTHORITIES AND THE LEGAL FRAMEWORKS FOR DECLARING A STATE OF EMERGENCY

- ☐ **Establish legal clarity:** Define the legal basis for declaring a state of emergency to ensure legitimacy, clarity, and alignment with national laws and international standards.
- ☐ **Define the process for the declaration of the state of emergency:** Determine the conditions, authorities, and procedures for declaring a state of emergency.
- ☐ **Specify emergency powers:** Clearly define the scope, limitations, and safeguards of the powers granted during the state of emergency, including requisitioning resources, enforcing quarantines, implementing curfews or evacuations, and restricting travel or assembly.
- ☐ **Prevent abuse:** Implement oversight and accountability measures to safeguard against the misuse of emergency powers.
- ☐ **Specify trigger conditions:** Identify the specific conditions under which a state of emergency can be declared such as overwhelmed response capabilities, severe risks to public health or infrastructure, potential for significant casualties, or the necessity for extraordinary measures.
- ☐ **Assign authority:** Define who holds the authority to declare an emergency and under which conditions.
- ☐ **Outline implications:** Define temporary restrictions, such as movement controls or quarantines, to protect public safety and prevent escalation.
- ☐ **Outline post-declaration procedures:** Establish measures for extending, modifying, or terminating a state of emergency.

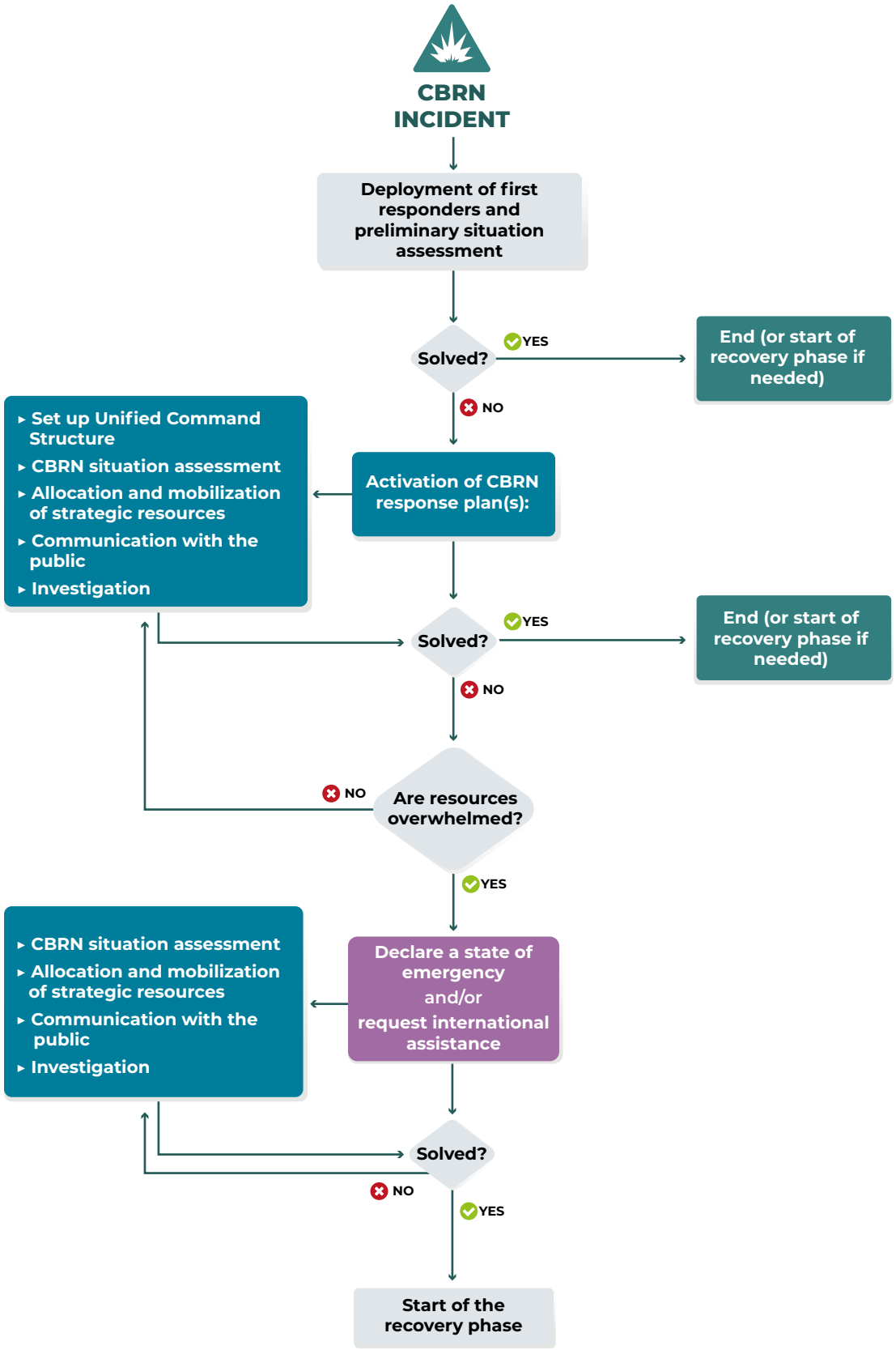
ESTABLISHING INTERNATIONAL COOPERATION AND ASSISTANCE FRAMEWORKS

- ☐ **Identify potential international partners and their capabilities:** Engage countries and regional/international organizations to foster proactive collaboration. This includes establishing resource-sharing agreements, joint research initiatives, and standardized protocols for communication, training, and equipment compatibility.
- ☐ **Establish mechanisms and create tools for requests for assistance:** Create resources and systems in advance to streamline the process of requesting assistance. This involves establishing a database of international contacts and resources, designating trained points of contact, and defining clear communication protocols.
- ☐ **Promote cooperation for capacity building:** Strengthen regional and international cooperation through joint training exercises, online resources, and targeted capacity building programs

ESTABLISHING A CBRN TRAINING PROGRAMME

- ☐ **Develop training curriculum:** Define a CBRN training curriculum tailored to the specific needs of the target audience, including policymakers and CBRN managers, aligning it with national security goals and international frameworks.
- ☐ **Implement and evaluate training program:** Select relevant content and methodologies tailored to stakeholders' roles, considering practical feasibility. Continuously refine the program based on evaluation to ensure training effectiveness. Methodologies can include classroom sessions, tabletop exercises, simulation drills, and joint exercises – each offering unique benefits and requiring specific evaluation approaches to measure their impact effectively.
- ☐ **Certification and accreditation:** Define mechanisms to validate the knowledge, skills, and competence of individuals participating in CBRN training. This includes certification and accreditation processes to ensure the quality, credibility, and sustainability of CBRN training programs.
- ☐ **Making training sustainable:** Develop mechanisms to ensure that CBRN training initiatives have a long-term and meaningful impact. This includes establishing partnerships with training academies, forming local trainers, fostering collaboration with international organizations, and creating feedback loops for continuous improvement.

SECTION II - RESPONSE



ACTIVATION OF CBRN PLAN(S)

ACTIVATE THE UNIFIED COMMAND STRUCTURE

- ☐ **Activate the Unified Command Structure:** Activate the pre-established Unified Command Structure (UCS) to ensure cohesive leadership and streamlined decision-making across all response levels.
- ☐ **Appoint incident commanders at each level:** Assign pre-designated leaders to strategic, tactical, and operational positions from a pre-identified pool, selected based on the incident's scale, complexity, and operational needs.
- ☐ **Establish command posts:** Set up fully equipped and adaptable command posts (whether physical or virtual) that serve as critical hubs for coordination and decision making at strategic, tactical, and operational levels.
- ☐ **Staff each level of the command post:** Deploy trained personnel to manage responsibilities at all levels of the command post. Staffing should be tailored to the incident's type and needs, ensuring flexible, efficient coordination while minimizing duplication and delays.

CBRN SITUATION ASSESSMENT

- ☐ **Activate an inter-agency group responsible for assessing the CBRN incident:** Engage a multi-disciplinary team to provide expert analysis, guide decision-making, and facilitate cross-agency collaboration during incident assessment.
- ☐ **Ensure the timely and accurate collection of data:** Implement robust data-gathering processes from multiple sources to capture critical information and maintain situational awareness.
- ☐ **Analyze data and prioritize the most critical information:** Assess and analyze collected data and prioritize the most critical information. This ensures response priorities are effectively directed, and resources are optimally utilized.
- ☐ **Produce regular situation assessment reports:** Provide all agencies involved with structured and regular reports containing critical information on the evolving situation. These reports should be clear and easy to read and include details such as the nature of the incident, current status, population and environmental profiles, incident impact, risk projections, response status and ongoing needs and challenges.
- ☐ **Continuously reassess and update the situation assessment:** Regularly review and update situation assessment reports to inform decision-making at all levels. By analyzing the latest information, necessary adjustments can be made to overall strategies and plans for managing the CBRN incident.

ALLOCATION AND MOBILIZATION OF STRATEGIC RESOURCES

- ☐ **Prioritize ongoing resource requirements:** Use prioritization models to assess ongoing resource needs based on CBRN situation assessments. Identify and categorize resource requirements in priority order (e.g., categorize required resources as “critical”, “high-value” and “complementary”).
- ☐ **Assess available resources:** Conduct a gap analysis to compare available resources against prioritized requirements. Utilized an interagency CBRN resource database to determine if the requested resources are: immediately available, not immediately available but procurable at national level, unavailable at national level but accessible internationally.
- ☐ **Formulate options:** Develop options for optimal resource allocation. Each option should include key details such as potential course of action, estimated resource allocation, expected outcomes and identified limitations.
- ☐ **Determine optimal resource mobilization:** Analyze and select the most suitable option for resource mobilization. Factors to consider include durability of each option, scalability, adaptability, complementarity with ongoing response efforts, logistical feasibility, public safety, risk of secondary exposure, regulatory compliance, and cost-benefit analysis.
- ☐ **Resource deployment:** Ensure the timely delivery of essential resources. Assign specific responsibilities, activate pre-planned logistics protocols, initiate mobilization processes, and establish a timeline with checkpoints to ensure efficient and coordinated implementation.
- ☐ **Monitoring and adjustment:** Continuously evaluate resource allocation strategies and make real-time adjustments based on updated information to respond effectively to changing incident dynamics.

COMMUNICATION WITH THE PUBLIC

- ☐ **Activate existing communication plans:** Implement pre-established communication plans and select appropriate risk communication strategies to ensure timely and consistent information dissemination during all phases of the incident.
- ☐ **Initiate a joint information center:** Establish a joint information center to coordinate communication efforts across all agencies and stakeholders, ensuring a unified and consistent public messaging.
- ☐ **Use pre-prepared message templates:** Adapt pre-prepared communication materials to deliver initial guidance, even when incident details are limited. These templates should outline key public actions and allow for updates as more information becomes available.
- ☐ **Create clear messages:** Formulate clear and concise messages that provide actionable guidance. Ensure these messages are adaptable for updates as the situation evolves and more information becomes available.
- ☐ **Consider other reliable information sources:** Integrate insights from diverse and reliable information sources to enhance the accuracy and credibility of public messaging.
- ☐ **Engage with the community:** Foster two-way communication to address public concerns, reinforce trust in response efforts, and ensure accessible communication across various channels.
- ☐ **Monitor and address misinformation (non-intentional) and disinformation (intentional):** Actively identify and counter false narratives using verified information. Safeguard public perception, prevent misinformation and disinformation from influencing decision-making, triggering panic, or hindering effective crisis management.

INVESTIGATION, INTELLIGENCE GATHERING, AND FORENSICS

- ☐ **Containment, scene security, and initial assessment:** Adapt and implement pre-established measures to secure the area, prioritizing civilian and responder safety through perimeter control, site evaluation, hazard containment and efficient resource allocation.
- ☐ **Evidence collection and preservation:** Follow established protocols to ensure the integrity and admissibility of collected evidence. Prioritize high-yield locations, maintain proper handling and chain of custody, adhere to approved procedures, and mobilize necessary expertise and resources.
- ☐ **Intelligence gathering and analysis:** Determine the most critical intelligence needs for the investigation, authorize, and oversee the execution of investigative measures to uncover critical information about the incident's origin and potential escalation. This includes analyzing open-source intelligence (OSINT), communication intercepts, and social media to develop leads and establish timelines for urgent priorities.
- ☐ **Forensic analysis and attribution:** Apply forensic techniques – such as source tracking, microbial forensics, chemical fingerprinting, and nuclear forensics – to determine causation and support accountability measures.

DECLARE A STATE OF EMERGENCY

- ☐ **Convene a meeting to consider declaring a state of emergency:** Assemble key leaders to evaluate the necessity and scope of emergency measures in accordance with established protocols.
- ☐ **Evaluate the need to declare a state of emergency:** Analyze CBRN situational assessments to balance the benefits of emergency powers against risks. Apply pre-established criteria, evaluate the incident's potential impact, weigh benefits against drawbacks, and formulate a recommendation through consensus.
- ☐ **Declare the state of emergency:** Issue a formal proclamation to activate emergency protocols, ensuring alignment with the legal framework. This may trigger pre-determined response measures and enable the allocation of necessary resources.
- ☐ **Terminate the state of emergency:** Transition back to standard operations once the threat subsides and the situation stabilizes, guided by predefined criteria and procedures

REQUEST FOR INTERNATIONAL ASSISTANCE

- ☐ **Evaluate the need for international assistance:** Assess gaps in response efforts by analyzing national resources and capabilities to determine if external support is needed.
- ☐ **Identify stakeholders capable of providing assistance:** Identify international organizations and regional partners equipped to address specific gaps related to the CBRN incident, ensuring effective collaboration and support.
- ☐ **Activate international notification systems:** Use pre-established communication channels to alert relevant entities and initiate assistance protocols promptly.
- ☐ **Formally request for international assistance:** Draft clear and detailed requests, including the precise incident location, type of CBRN agent, specific resource needs categorized by priority, current national response efforts, urgency, and a designated point of contact. This ensures clarity and expedites support.
- ☐ **Evaluate incoming offers of assistance:** Analyze incoming offers of assistance to verify alignment with needs and ensure compatibility with existing systems and operational frameworks.
- ☐ **Coordinate deployment and integration:** Facilitate the deployment and integration of international assistance through predefined communication channels. Coordinate logistics for personnel and equipment, prioritizing resource allocation based on the evolving needs assessment.
- ☐ **Continuously reassess assistance needs:** Monitor the evolving situation, reassess requirements, and adjust external assistance requests to align with the incident's progression.
- ☐ **Maintain communication and information sharing:** Ensure continuous communication with partners through regular updates on the evolving situation. This fosters mutual understanding, enhance coordination, and support effective collaboration.

unicri
United Nations
Interregional Crime and Justice
Research Institute