CRISIS AND EMERGENCY MANAGEMENT GUIDANCE

for the Chemical Sector

2022

CHEMTREC® CONSULTING SOLUTIONS

Contents

LEGAL DISCLAIMER

This guidance is offered by CHEMTREC, LLC to provide some helpful ideas for development of an individual company crisis management program. It is necessarily general in nature and leaves product and site-specific circumstances to individual users. Different companies may vary their approach with respect to specific elements of the program based on site-specific circumstances, the practicality and effectiveness of particular actions and economic and technological feasibility. It is the responsibility of the user of this information to determine its own company crisis management needs and to accept, reject or modify the elements as appropriate.

This guidance is not designed or intended to define or create legal rights or obligations. Users should comply with applicable laws and regulations and should consult with legal counsel concerning such matters.

CHEMTREC, LLC does not make any warranty or representation, either express or implied, with respect to the accuracy or completeness of the information contained herein; nor does CHEMTREC, LLC assume any liability of any kind whatsoever resulting from the use of or reliance upon any information, procedures, conclusion, or opinion contained herein.

CRISIS AND EMERGENCY MANAGEMENT GUIDANCE

for the Chemical Sector

Introduction

Introduction

Purpose, Aim, and Objectives

This document provides an overview of the core components of a crisis and emergency management system and offers suggestions for organizations as they look to implement new protocols or improve existing ones.

Aim

To support organizations in the chemical sector by suggesting effective protocols for the management and preparation for crisis and emergency situations.

Objectives

To outline a framework of activities which supports organizations in preparing for the common consequences of emergency and crisis situations rather than for every individual emergency scenario.

To outline the need for and provide an explanation of the flexible, scalable, and adaptable protocols which can act as the basis for responding to a wide range of incident, emergency, and crisis situations.

To supplement these generic protocols, with hazard specific protocols through a program of risk reduction, monitoring, and implementing systems which support readiness.

Definition of Key Terms

Crisis Management: The process by which an organization prepares for and responds to a disruptive event which threatens to harm its people, environment, assets, or reputation.

Business Continuity Plans / Planning: Sometimes called COOP Plans (continuity of operations). These are plans and tools which aim to mitigate the impact of any incident on the businesses core functions. They help ensure that the business can continue to deliver key outputs to customers in the event of disruption.

Crisis Management Protocols: When we refer to crisis management protocols in this document, we refer to more than just the plan itself. Protocols entail everything required to prepare for and respond to an incident. They include the organizations plans and policies, but also their personnel and supporting infrastructure and equipment, such as Incident Coordination Centers.

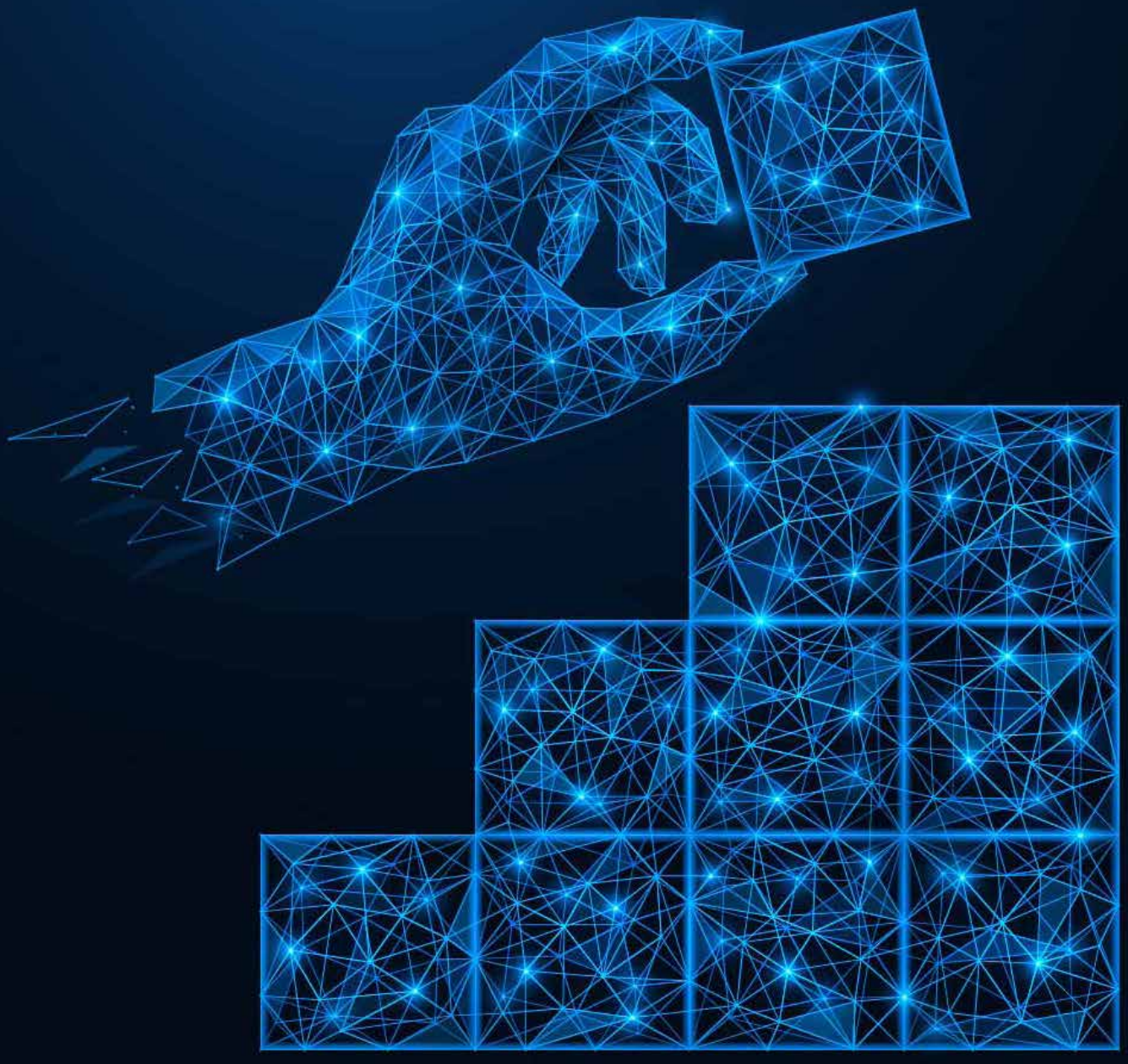
Incident Coordination Center: Sometimes referred to as Emergency Operations Centers or EOCs, Incident Coordination Centers provide a focal point for the coordination of the response and are where those with a strategic or tactical response role meet.

Incident Command Post: A central point for the coordination of the operational response to an incident. These are usually set dynamically based on the location of the incident.

CRISIS AND EMERGENCY MANAGEMENT GUIDANCE

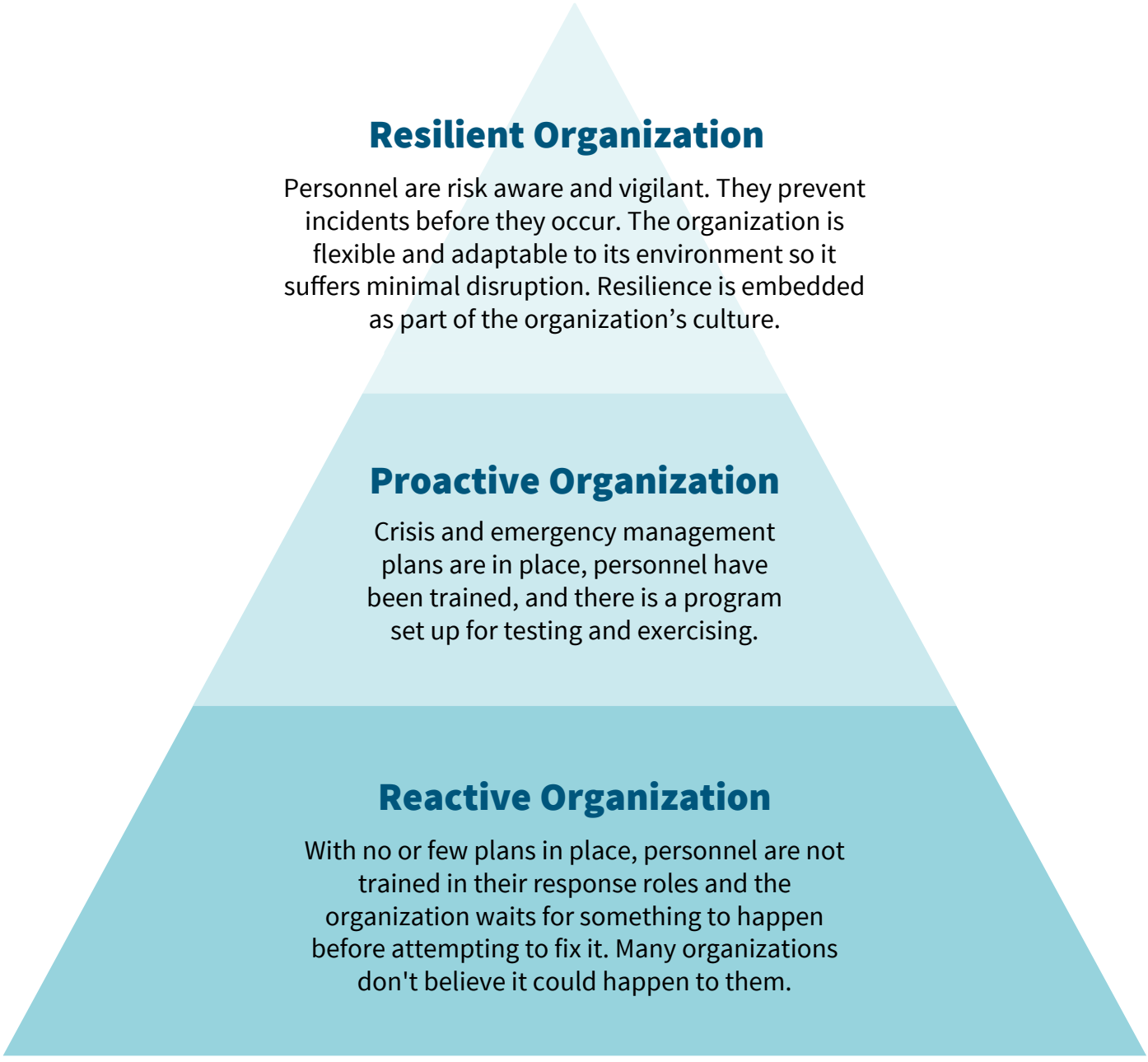
for the Chemical Sector

Chemical Sector Resilience Model



Chemical Sector Resilience Model

The aim of the program is to work with stakeholders to move the organization away from one which responds primarily reactively, to one which is proactive in its response. The longer-term goal is to develop systems and processes so that the organization is resilient. A resilient organization is able to adapt dynamically to a wide variety of situations to minimize disruption on its critical functions. This is not achieved alone - crisis and emergency management are not stand-alone concepts. To effectively prepare for a crisis or emergency situation and to achieve organizational resilience calls for working across the organization and involving a number of other departments and roles within an organization.



The Role of the Leadership Team:
The leadership team supports the crisis and emergency management program both financially and through the investment of time. They accept that crisis and emergency management is critical to the future survival of their business. The leadership team typically nominates a representative to support the crisis management planning team and receives regular reports on key risks and the status of crisis and emergency planning efforts.

The Role of the Communications Team:
The communications team plays a key role in protecting the reputation of the organization in the event of a crisis or emergency. They work with the crisis management planning team to develop a stakeholder matrix in the event of an incident, detailing key contacts and ways to contact them in an incident. They should also consider putting in place pre-set media statements to be used as a holding statement in the event of an incident.

The Role of Health and Safety in Crisis and Emergency Management:
The effective implementation of health and safety strategies, such as planned preventative maintenance and defect reporting, minimizes the chance of an incident occurring in the first place. Health and safety play a key role in the reduce stage of the planning cycle. Recording and investigating near misses can reduce the chance of a reoccurrence or an incident occurring on a larger scale.

The Role of Incident Response in Crisis and Emergency Management:
Proactive incident response is the first line of defense in preventing the escalation of incidents into emergency and crisis situations. Organizations should consider investigating all incidents and near misses with a view to preventing opportunities for future incidents to occur. Effective incident response includes clear lines of escalation, communication, command, and control, between incident response protocols and those in place for crisis and emergency management.

The Role of Business Continuity in Crisis and Emergency Management:
Business continuity protocols enable the organization to recover and restore its key services in line with pre-determined timescales. The ability to implement these strategies is integral to the wider financial, operational, and reputational impact of the incident. This is achieved with clear lines of escalation, communication, command, and control, between business continuity protocols and those in place for crisis and emergency management.

The Role of Cyber Security in Crisis and Emergency Management:
Your IT and OT teams play a key role in preventing a major cyber crisis or emergency from occurring. Where one does occur, it is vital that the organization's technical response plans (often referred to as IT Disaster Recovery Plans) dovetail with the organization's crisis and emergency management plans. While the technical response will try to contain any attack and bring systems back online, the crisis and emergency management protocols will deal with and respond to the operational

element of the response. Clear lines of escalation, communication, command, and control between cyber response protocols and those in place for crisis and emergency management are an important part of an effective response.

The Role of Physical Security in Crisis and Emergency Management:
Effective physical security mechanisms are critical in limiting the likelihood of an incident, emergency, and crisis on site. Consider clearly defining escalation protocols in a place where a security incident occurs, so that emergency and crisis management protocols can be enacted if needed. Recording and investigating near misses can reduce the chance of a reoccurrence or an incident occurring on a larger scale.

The Role of Chemical Emergency Response Services in Crisis and Emergency Management:
Ensuring the organization has ready access to advice regarding chemicals or other dangerous goods is a crucial step in minimizing crisis impacts and getting incidents under control. Acting without this advice may lead to an escalation in an incident's severity or duration. The coordination and routes for dissemination of advice from your emergency response provider also form a key consideration when developing your crisis and emergency protocols.

This list aims to demonstrate the importance of embedding crisis and emergency management across the organization. Crisis and emergency management is not a standalone task, but instead can be well-integrated as part of the day-to-day activities of the organization. While some special protocols may be required for the response to an incident, emergency, or crisis situation, they may be more effective when rooted in the day-to-day operations of the business. By building protocols which echo the day-to-day operations of the business, the organization is able to reduce the training load on employees and reduce the cognitive strain on responders. Rather than trying to implement new and different ways of working, they are able to build upon existing working practices when responding.

CRISIS AND EMERGENCY MANAGEMENT GUIDANCE

for the Chemical Sector

Planning

Planning

Organizations looking to implement or improve current protocols should understand that the act of planning is as important as the outcomes of the process. Regular consultation is often undertaken throughout the steps of the planning cycle to help ensure key stakeholders are engaged in the process, share key insights, and help ensure that the final product reflects the working practices and culture of the organization. Crisis and emergency management protocols are owned by all, not only those who lead the project.

Consider planning as an ongoing process. As the organization changes, it will grow, personnel will change, new hazards and threats will emerge, and new regulations will come into effect. Response protocols can be optimized when reviewed and updated to account for these changes. The review stage suggests some trigger points for the updating of protocols.

The Crisis Management Planning Team

Comprehensive crisis and emergency management generally cannot be achieved alone. Consider assembling a working group or planning lead consisting of representatives of the teams named in the Chemical Sector Resilience Model. A board level sponsor with budgetary authority to support the program can enable increased opportunities for success. A designated, suitably qualified, and experienced crisis management lead, available to support the group with specialist guidance, can also be beneficial. This group is tasked with supporting the organization through all elements of the planning cycle and benefits from monthly meetings.

Planning Cycle

The planning cycle aims to provide an overview of four key areas of activity to prepare the organization for an incident, emergency, or crisis situation. The aim should always be to avoid incidents in the first place. However, when they do occur, the organization should be prepared to respond effectively, limit the spread, and minimize the scale and impact of the incident so it does not escalate into an emergency or crisis situation. The planning cycle is set up to encourage organizations to take this proactive approach to crisis and emergency management – focusing on prevention, vigilance, and a proactive response wherever possible.

Review

Current Protocols: Conduct a regular review of your protocols to help ensure they meet quality practice and the needs of the organization. You should consider any changes to the organization or its operating environment.

Hazards and Threats: Conduct a review of hazards and threats which may have an impact on your organization. Consider this for each physical location the company operates. Consider the likelihood and impact of risks and pull together a risk register for the organization. There are a range of tools and resources available online to support the development of your initial risk register, also look for any local or national risk registers detailing risks in your locality. For example, in the U.S. the national risk index has local risk information (https://hazards.fema.gov/nri/). This review allows you to target specific risks during the reduce phase, and also determine any risks which warrant hazard specific plans. These can be developed where a specific response is required which can't be dealt with by the generic planning protocols.

Requirements: Determine that your protocols meet the minimum requirements of any local, federal, national, or international requirements. Regularly monitor these for updates. Review your protocols regularly and in particular:

- Following any incident or exercise which highlights the need for changes to the program.
- Following any changes to key personnel.
- Following any organizational changes or restructures, including a merger, acquisition, or disposal of businesses or business units.
- Following any changes to legal or regulatory requirements.
- If none of the above have occurred, consider reviewing protocols at least annually to help ensure they remain fit for purpose and that they reflect the current risk landscape.

Reduce

Once you have identified hazards and threats, you should consider next looking to reduce their likelihood or impact, or better still, prevent them from occurring. Things to consider:

Take steps to mitigate risks:

- **Terminate:** Can you remove the risk by changing or stopping the risky activity? This may mean moving sites from an area which is more hazard prone or stopping a process or activity because the risk of an incident, outweighs the benefits of continuing the activity. Consider if there are any activities which could be stopped to lower your risk exposure or the impact of risks.
- **Treat:** If termination is not feasible, consider what treatments you might be able to apply to lower the risk. This can include bunding of tanks, flood protection of sites or other physical measures. It can also include a review and redesign of equipment or processes to reduce the chance of human error.
- **Transfer:** Consider whether the risk can be transferred to another party. Can a process be conducted by a sub-contractor or other party so that they carry the risk? Can you insure against the financial risk? Explore which risks can be transferred.
- **Tolerate:** Some risks may have to be accepted. It may not be possible to apply the other mitigation strategies, or it may not be deemed cost effective. For those risks which can't be terminated, treated, or transferred, we tolerate them and move onto the next step of preparing for them.

Work with your health and safety team to embed a safety culture throughout the organization. The aim of this is to prevent human error and create a culture of proactive maintenance and error identification. Investigate near misses and lessons learned. Aim to identify potential errors and rectify them before they become an issue, which then has the potential to result in an incident, an emergency, or crisis situation.

Work closely with other key disciplines as outlined in the chemical sector resilience model to mitigate risks across all key departments.

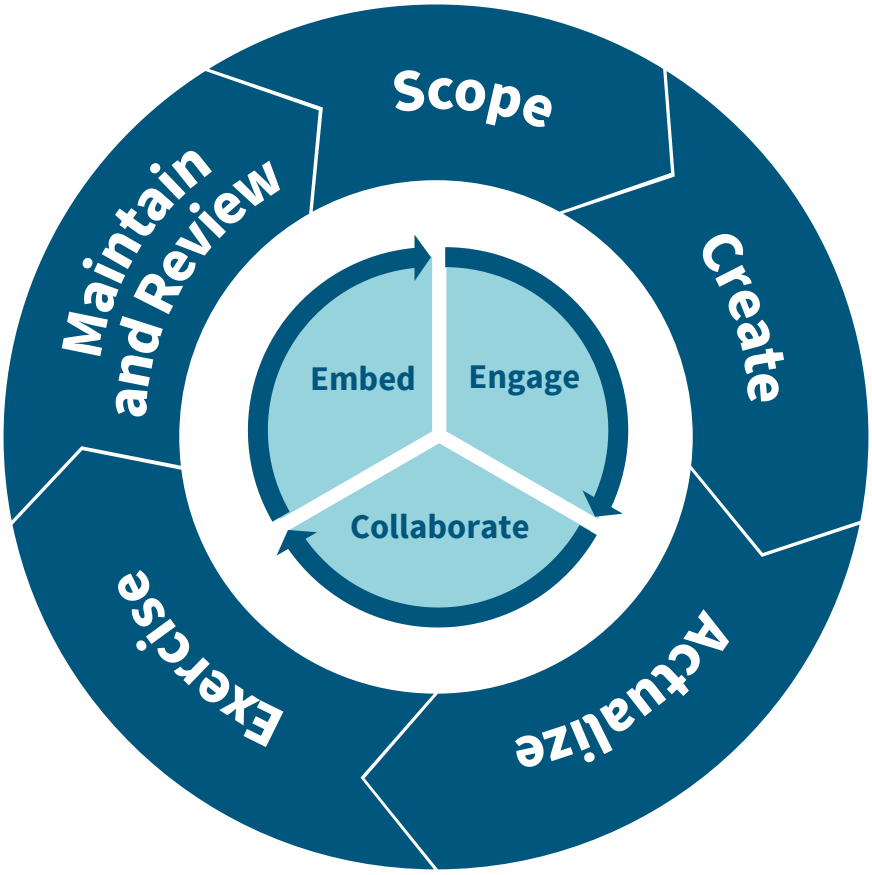
Readiness

Once you have reduced the likelihood or impact of risks, you should then prepare the organization, so it is in a state of readiness, ready to deal with any residual or unexpected risk events. Readiness involves four key streams:

- Planning
- Training
- Exercising
- Monitoring and Vigilance

Planning

The planning cycle demonstrates a process of developing new incident, emergency, and crisis management plans. At the heart of the cycle are three crucial activities: engage, collaborate, and embed. As per the wider focus of the planning cycle, it is critical that employees are engaged and have a chance to collaborate throughout the plan development process. Consider embedding the final product within the organization so that people have a clear understanding of the plan and how it operates.



Scope: The first task when developing a new plan is to set the scope. The plan should have a clear purpose and a set of aims and objectives. The plan should be clear if it is designed to cover a single site, part of a site, or the wider organization and the audience for the plan. Consider whether the plan will operate at the operational, tactical, or strategic level. Tailor aims and objectives to help ensure the organization responds in a manner which protects people (staff, customers, and wider communities), the environment, the organization's assets, and its reputation. At this stage, also determine whether you are writing a generic crisis, emergency, and incident response plan, a hazard or threat specific plan, or a plan for a specific purpose (i.e., DOT Transport security plan or a Seveso compliant on-site or off-site plan). Hazard or threat specific plans should be built upon the core principles in your generic protocols such as your command structure. It is therefore beneficial to create your generic response plan first, before considering hazard or threat specific responses. Consider having these specific hazard plans sit as an annex of the more generic protocols. Take additional care that plans for specific purposes meet any regulatory or legislative requirements. **For the coordination and response to incidents, consider having what is referred to as a suite of plans:**

- ***A Crisis Management Plan*** for the strategic coordination of an incident.
- ***An Emergency Response Plan*** for the tactical coordination of an incident.
- ***Incident Response Procedures*** for the operational response to an incident.
- ***Business Continuity Protocols*** to help ensure key services can continue or be recovered within pre-agreed timescales.

A coordinated response to the incident leverages clear links between these plans.

Create: Once you have scoped the plan, work with teams to start creating it. The plan essentially outlines who is doing what, when, where, and how. Below is a good overview of what a crisis or emergency management plan may include:

- Clear command and control structures with links to other plans.
- Escalation processes and criteria.
- Notification and activation processes.
- Communication processes, including stakeholder management and media requirements.
- Action cards for each function within the plan.
- Clear aims and objectives to protect the organization's people, environment, assets, and reputation.
- Scalable and flexible protocols for a range of scenarios.

More detail on the processes above is outlined in the response section.

Actualize: Make the plan more than words on a page. Bring it to life as a decision support tool and be readily available to support and guide personnel when responding to an incident. Once you have created the plan, consider ways to bring the plan to life. This could include:

- ***Dissemination of the plan and specific parts of the plan.*** Keep copies of the plan at key locations (incident command posts/coordination centers). Also consider providing personnel with a response role with access to their action cards 24/7. You may wish to distribute laminated copies of their action card or create crib sheets for them to carry.
- ***Training and workshops are a key part of bringing the plan to life.*** Give staff with a role in the plan

training as soon as practicable after the plan has become operational. Carry out training following updates and consider a refresher training at least once a year or more. Consider the wider training needs of the organization as well to help ensure those not tasked with a response role to understand how to notify the response team of an incident, or potential incident, so they can be activated in a timely manner. This broader awareness can be essential. See the section below for more information on training.

- ***Critical event management platforms can make the actualization of plans simpler and more streamlined.*** Consider the use of a platform so that relevant parts of your plan can be disseminated to responders at the touch of a button when an incident occurs. Critical event management platforms can also support effective decision making during a response by promoting shared situational awareness and enhancing communication lines.

Exercise: Exercise a new plan to validate that the protocols are fit for purpose and give personnel a chance to rehearse their roles. In addition to an initial exercise, regularly exercise plans to optimize effectiveness. Consider doing this when any changes or updates are made to the plan, or where no changes are required, once a year or more. Consider keeping a record of exercising with the plan so that it is clear when the plan was last validated. See the section below for more information on exercises.

Maintain and Review: Thus begins the cycle of continuous improvement. Exemplary practice includes regular review in line with the system criteria outlined above and the consideration of new threats and lessons from previous incidents incorporated. Remember to learn from others as well.

Training

Effective crisis, emergency, and incident management programs generally include a strong training component. Organizations within the chemical sector are often familiar with operating in high-risk environments and may have experience dealing with minor incidents. However, emergencies and crisis situations are normally rare occurrences. For staff to respond to an incident proactively, effectively, and safely, they need the skills, knowledge, and tools to do so in line with their assigned role. This may be effectively facilitated through training and exercising.

To understand who needs training, consider conducting a training needs analysis. This will identify the staff within the organization and determine their training needs. Consider the following as part of your training:

- ***Training for those with a response role.*** Consider both technical and non-technical training (see below). Consider training responders once the plan launches, offering refresher training annually, or following major changes to the plan. Give responders the chance to rehearse their roles as part of the exercising program.
- ***Wider awareness training.*** Awareness training for staff helps so they are able to spot and report defects before they become incidents and understand how to escalate issues. This can be a good course to add to introductory training for new staff with an annual refresher.
- ***Role specific training.*** (E.g., safe shut down of a facility or specific machine). Where there are specific tasks to undertake, consider running regular practical drills where responders walk through the process of safe shut down or part of it. If it is safe and appropriate to do so, consider making it a live drill. If it is not safe to do so, you may ask responders to walk and talk through the steps they would take. These live walk on location exercises may be more effective for role specific technical training. Monthly can be a good frequency for this, more technical training, depending on the needs of the organization.

- ***Hazard specific training.*** Provide hazard specific training for responders that have specific tasks to undertake. Like role specific training, this is likely to be a technical role. Consider conducting drills/ live walk throughs.

Crisis, emergency, and incident management training has traditionally focused on the acquisition of technical knowledge. Whether it is procedural knowledge (such as the contents of the crisis, emergency, or incident management plan), or technical skills and knowledge related to a specific process (such as operating a fire extinguisher or safely shutting down a machine). While this knowledge is highly important and a key part of the organization's training regime, there is also an opportunity to upskill responders in non-technical skills. These non-technical skills can be the foundation of an effective response and support application of the technical skills. They also support a responder's ability to think on their feet and make effective and dynamic decisions to respond quickly and decisively to get the incident under control, thus helping to minimize escalation and maximize success. **When designing your training program consider both technical and non-technical elements. Specifically, the following:**

Technical:

- Procedural Requirements: roles and responsibilities within plans, policies, procedures, SOPs etc. Activation of the plan, setting up incident command posts/Incident Coordination Centers etc.
- Technical skills and knowledge related to the individual's role, such as how to operate a machine.

Non-Technical Skills

Consider including underpinning skills required for the dynamic response to an incident. These skills include:

- Situational Awareness
- Decision Making
- Communication
- Leadership
- Teamwork
- The ability to cope with stress and mental fatigue

Exercising

Exercises have three main functions: they validate plans; they develop competencies for those who have specific roles and responsibilities and provide an opportunity to practice these roles (training); and test well-established procedures to help ensure they are fit for purpose. Consider conducting training before an exercise, rather than treating an exercise as an introduction to crisis, emergency, and incident management. This will give participants awareness of their roles and the opportunity to be reasonably comfortable with them before they are subject to the stresses of an exercise. Plans developed to allow organizations to respond efficiently and effectively can be tested regularly using a variety of processes, such as tabletop and live play exercises. Roles within the plan, not individuals, are exercised to help ensure they are fit for purpose and incorporate the necessary functions and actions to be carried out in an incident. The outcome (log) of testing and exercising identifies and records whether it worked and what may need changing. The log also identifies what has changed.

Through the exercising process, individuals can practice their skills and increase their knowledge, confidence, and skill base in preparation for responding to a live incident. This is a key part in building a resilient workforce.

As appropriate, organizations should consider exercising with partner agencies and contracted services. This is beneficial where the identified risks are shared and may require the involvement of partner organizations in a response capacity, particularly where organizations have mutual aid agreements in place. Learning from exercises can be cultivated into developing a method that supports personal and organizational goals and is part of an annual plan validation and maintenance program.

Consider conducting the following:

Communications Exercise
Frequency to consider – every 6 months

Communication exercises test the activation and communication protocols of the organization. They test the organization's ability to contact staff and key stakeholders 24/7. They enact the organization's call cascade. Communications exercises make clear that the call is part of an exercise. Communications exercises are optimally staged both in and out of normal operating hours.

Drills
Frequency to consider – monthly

Drills tend to be well suited for testing operational processes and procedures. They can offer practical tests and run throughs. Consider a rolling program of drills focusing on specific elements of the organization's response. If site applicable, these may include evacuation drills for the site (or part of a site), security drills for the lockdown of site, specific safe shut down of machinery and processes, and the operation of specific tools and technology deployed in an incident. List the processes which may be enacted in response to an incident and include these as part of the organization drill program.

Tabletop Exercise
Frequency to consider – every quarter and on completion of a plan or following any significant update

Quarterly tabletop exercises bring key responders together to discuss a scenario or specific element of a response and work through the plan. They allow responders to interact and share their knowledge and perspectives on risks and offer a chance to validate plans. A tabletop exercise can range from an hour to a day and can be a cost-effective means of refreshing the plan and the knowledge of staff in their response roles. Consider inviting partner agencies and key stakeholders to take part in these exercises.

Command Post and Simulation Exercise
Frequency to consider – every 12 months

It is important to regularly test the functionality and suitability of any command post that is utilized during an incident response. Consider a live, practical test of processes, protocols, equipment, and facilities which will be used in an incident, emergency, or crisis using a simulated crisis scenario. The command post exercise can also provide an opportunity for those with a response to familiarize themselves with the set up and operation of the space. Exercise Incident Coordination Centers and Incident Command Posts, either as part of a single exercise, or as part of an ongoing program of exercises. Consider conducting command post exercises with other organizations to test communication protocols and information flows. Command post exercises may be combined with other exercises; you can utilize them as part of drills, tabletop exercises, or live play exercises. While the whole space may be exercised annually, it is also important that equipment in the ICC is audited and tested, consider doing this monthly.

Live Exercise
Frequency to consider – every 3 years

A live exercise is a live test of crisis, emergency, and incident response capabilities. For example, a live full site shut down or evacuation or a simulated spill/release resulting in a need to respond including casualties. The exercise should be played out in real time and as in a "live" environment as is possible and safe to do so. Actors, mockups of scenes, and injects fed in through phone, email, and other means are examples of scenarios that can be used to make the incident feel as real as possible. These exercises are typically the most expensive and disruptive to day-to-day operations of the site and are therefore generally conducted less frequently than other exercises. However, if run correctly, they may be the closest thing your organization will get to a real and robust test of its plans and planning protocols. While not preferable, a real incident could replace the need for a live play exercise, if properly and effectively debriefed.

Debriefing and Post Exercise Reports

Fully debrief the exercises following the processes outlined in the response section, with a full report written up post exercise.

Monitoring and Vigilance

Once the organization has plans in place and its teams are ready to respond, remain vigilant and monitor hazards and threats which may become incidents, emergencies, or crisis situations. The aim here is to eliminate risks before they become incidents and help ensure if an incident were to occur, systems are in place to offer warnings at the earliest opportunity, and preferably in advance of the incident escalating. The earlier the incident teams are activated, the better chance they have of bringing the incident under control early, limiting its scale and impact on the organization. Review your risk assessment and consider any early warning systems you can implement for each risk. Establish clear links between these early warning systems and the escalation and activation processes for your crisis management team. Early warning systems may include:

- Monitoring local weather forecasts.
- Reviewing planned maintenance schedules.
- Identifying periods of heightened error potential throughout the organization as noted in the organization's health and safety records.
- Reviewing project or construction work which may alter the site's risk profile.

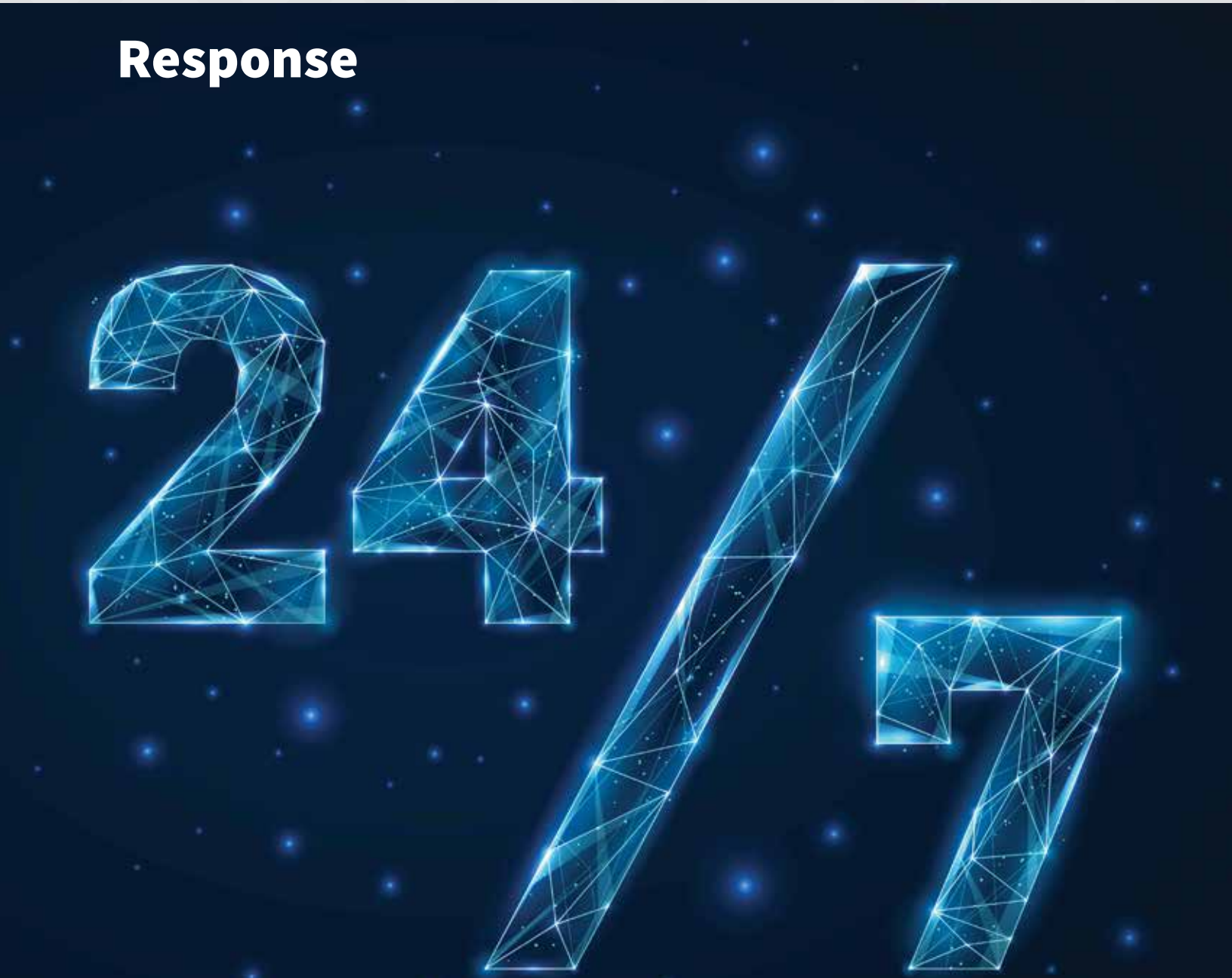
Respond And Rebound

The final stage in the planning process is to respond and rebound. The response section outlines some suggested steps and capabilities for an effective response to an incident. This stage is included in the planning cycle, as the response and rebound section feeds back into the review of the organization's capabilities. Once an incident has taken place, consider conducting debriefs, reviewing responses, and then updating capabilities, plans, and training to address any gaps in the response. The cyclical process is crucial and should be evidenced in the organization's plans and protocols –record any updates made to plans and record the rationale for these changes. Also create an action plan, post incident, to log change requirements to the crisis and emergency management program and track progress against these changes.

CRISIS AND EMERGENCY MANAGEMENT GUIDANCE

for the Chemical Sector

Response



Response

Timely, coordinated, and proactive actions are key to optimally respond to a crisis situation. The structures and processes detailed in this section aim to deliver this. Put these structures and processes in place prior to an incident and detail them in the organization's crisis and emergency management plans.

Activation and Notification

The rapid activation of response teams and plans is critical in supporting the organization to deliver a rapid and proactive response. The earlier that response teams are notified of an incident, the faster they can start to address the incident and minimize any impact. Consider having triggers in place which make it clear when to activate the response teams. In some cases, such as a major explosion, this may be obvious. For smaller incidents, which have the potential to escalate, it is not always as clear, which is why these activation triggers are important. Triggers may include:

- An incident which has the potential to affect the operations of the site.
- An incident which has the potential to cause serious injury to an employee or member of the public.
- An incident which has the potential to impact beyond the boundaries of the site.
- An incident which has the potential to cause media interest or reputational damage.
- An incident which has the potential to cause environmental damage.

Once a trigger is met, establish clear routes and methods to activate the relevant response personnel. Consider enacting a call cascade. This can either be a manual cascade or an automated one using incident notification software. You can also tie this into your chemical emergency response provider who may be able to provide a 24/7 single point of contact for notification and automatic activation in the event of an incident

Concepts Of Command And Control

Command and control are a key part of effective crisis management. For many corporate organizations, operating more flat management structures, the move to a hierarchical structure may feel unfamiliar, however it can be essential for the proactive management of incidents. In an incident, there is rarely time to make decisions in a collaborative manner, so clear tasking of employees offers a clear leadership structure.

There are three key tiers of response in an incident:

- **Operational:** This is often referred to as incident response. It is where the "hands on" work is completed. The operational lead will concentrate their efforts and resources on specific tasks within a defined area (this may be a functional area or a geographic area).
- **Tactical:** Often referred to as emergency response, this is where the coordination of the operational response takes place. Tactical leads help ensure that the response is coordinated, coherent, and integrated and that the operational teams have access to the resources they need.
- **Strategic:** Often referred to as crisis management, the strategic leads look at the incident in its widest sense. Focus is not on the immediate response, but on the wider reputational, financial, and operational impacts. The strategic team considers business continuity and recovery planning and handles the media. The strategic team sets some overall aims and objectives for the response and also supports the tactical team by making money and other resources available.

The tiers in the command system may want to operate in line with FEMA's Incident Command System. For more information on the ICS model, visit https://emilms.fema.gov/is_0100c/curriculum/1.html

The Incident Command System offers clear chains of command and supervision, provides clear

reporting lines, and offers a common, scalable, and flexible structure which can be used for a variety of incidents, expanding, and contracting depending on the needs of the incident. The ICS model also supports multi-agency working, helping sites coordinate with the wider response community who may be required on site to support a response.

The Incident Command System can be a central part of an organization's crisis, emergency, and incident management plans, and form a key part of training for responders.

Communication and Coordination

The ICS model offers clear lines of communication; however, it is optimized when supported by appropriate tools and infrastructure.

Consider having a pre-defined communication tool which is used for briefing at the start and throughout an incident response. This can speed up communication and deliver information in a standard format allowing for a short, smooth, succinct flow of information to be passed where time criticality is often key. Leads can request an update, using this tool from tactical or operational leads. These tools are often called SITREPS (Situational Reports). A battle rhythm is a term to describe the flow and frequency of reports and should be set for SITREPS. For example, a battle rhythm may consist of an initial report at the start of the incident, followed by regular SITREPS every 30 minutes. As the incident progresses and slows, this may only occur every hour.

To provide a coordinated response, the organization should consider establishing command posts and incident coordination centers. Command posts are used at the operational level and are more likely to be designated dynamically and will depend on the location of the incident. They should be close enough to see the incident and allow the coordination of the operational response, but far enough away so that responders are safe.

Incident Coordination Centers are used at the tactical and strategic level and provide support to the operational response through the functions of the Incident Command System. Incident Coordination Centers provide a focal point for the coordination of the response and are where those with a strategic or tactical response role meet. The ICC has five main tasks:

- *Coordination* – to help ensure all responders are working together to deliver an effective response.
- *Decision making* – provide a central point for making key decisions as needed for the incident.
- *Operations* – coordinate and monitor the implementation of decisions.
- *Information gathering* – provide a central hub of information to enhance situational awareness of decision making.
- *Dispersing information* – agreeing on and disseminating information to key stakeholders.

Consider having pre-defined facilities which can serve as the Incident Coordination Center in the event of an incident and keep these rooms in a state of operational readiness. Consider making separate rooms available for the tactical and strategic teams, although in larger organizations, the strategic team may operate remotely. There should also be a backup ICC identified in case the primary site is affected by the incident. The ICC should be resilient to the loss of utilities, including telecommunications. Consider testing ICC equipment every three months. See Appendix 1 for a list of equipment you may want to include in an ICC.

Business Continuity

Business continuity management forms a key part of the organization's response. As with crisis and emergency management, consider having pre-defined business continuity plans. Business continuity plans detail the organization's key products and services and examine the activities which support these products and services. They are designed to help ensure that these products and services can still be delivered to customers, in line with their expectations, even where the organization suffers a crisis or emergency. Have backup strategies

in place to help ensure this continuation of service. Business continuity plans are typically activated as soon as a crisis or emergency occurs, where there is potential for the incident to affect the organization's products or services. A separate business continuity team can be formed to oversee this element of the response and the team lead can regularly liaise with the Incident Commander.

Handling the Media and Stakeholders

Keeping the media and key stakeholders informed about the incident and the organization's response to the incident is a key part of an effective response. Failure to do this can cause major reputational damage to the organization. Retaining the confidence of the public and key stakeholders is a key aim of the response. This is largely achieved through regular and effective communication. Consider having ready:

- A 24/7 response to any incident which may garner media attention. Provide the organization with access to a communications representative 24/7.
- Accurate and timely statements. In the initial stages of the incident, the organization may wish to release a media holding statement, simply confirming the incident has occurred and promising a future update. Following this, frequent updates may be needed to the media, staff, and other key stakeholders. Consider regularly updating social media and websites.
- Competent spokespeople capable of speaking to the media. Depending on the scale of the incident, the organization may wish to hold a press conference or speak to the media. This is typically a specialist skill and the organization may want to have pre-defined and trained spokespeople for this role. Consider training senior leaders in the organization for this job.

De-Escalation and Recovery

Have mechanisms in place to recognize the end of an incident and to support the transition to recovery. Consider forming a team to support this recovery as soon as possible, particularly during the response phase, so that the recovery can be managed and coordinated. Recovery may include:

- Rebuilding any damaged infrastructure.
- Restoring key services provided by the organization, in line with business continuity arrangements.
- Rehabilitating staff who have been involved or affected by the incident. Consider staff welfare as part of the organization's recovery plan.

Debriefing

Following any incident, consider holding a debrief to identify lessons from the response and recovery. The debrief also offers a chance for staff to decompress after a response and identify any staff welfare needs. To the extent practicable, hold a debrief immediately after the response, or in the event of a prolonged response, after the response team's shift. A longer-term cold debrief can then be held later, within two weeks of the incident. This gives staff a chance to reflect on the incident and share additional meaningful insights on areas which could have been improved. Consider preparing a final, written post-incident report, within four weeks of the incident. This can capture salient facts about the incident and identify potential areas for improvement in the response. Support it with an action plan with clear timescales for rectifying any identified issues. Regularly monitor and update this plan to make sure that actions are completed.

Appendix 1: Incident Coordination Center Criteria For Consideration

An ICC is a facility which supports the coordination of an incident and enables shared situational awareness and collaborative decision making.

Consider having the following:

- ☐ A main area (e.g., a meeting room) large enough for the Incident Management Team to meet.
- ☐ A smaller, quiet room for decision makers to consider key decisions or take key phone calls.
- ☐ A fallback ICC, in the event that the primary is unavailable.

For the main area:

- ☐ Enough workstations for everyone with a role in the plan.
- ☐ A large meeting table for IMT meetings.
- ☐ Hard wired telephone lines with sufficient incoming and outgoing lines –with numbers that can be diverted if the primary ICC needs to be evacuated. Host some of the lines outside of the switchboard system.
- ☐ Mobile telephones.
- ☐ 5g Wi-Fi Dongle or other backup internet provision.
- ☐ Laptops or computers for those with a role (many people will bring their own laptops but in an unannounced incident this may not always be the case).
- ☐ A printer and photocopier – to print media statements, SITREPS and other key information.
- ☐ TV with news channel access.
- ☐ Stationery– pens, pencils, notepads, whiteboards/ flipcharts, and whiteboard pens.
- ☐ A clock.
- ☐ Tabards to identify key roles (e.g., Incident Commander, Operations Section Chief).
- ☐ Access to a restroom and refreshments.
- ☐ Hard copies of plans.
- ☐ Maps of the site and wider area.
- ☐ Access to electronic copies of plans and key documents.
- ☐ Access to any site monitoring system or CCTV.

About the Authors:

Chris Scott *has been working in the field of crisis and emergency response planning, training, and exercising for over 33 years and is a pioneer in the field. His 22 years of military experience coupled with studies in human intelligence, linked with an understanding of a person's ability to manage unwanted events has seen outstanding results. Chris has a degree in leadership and management and a master's degree in Emergency Planning and Disaster Management, carefully linking with and complementing business continuity arrangements. He has worked around the globe for a wide range of organizations and well-known companies and extensively with UK emergency services.*

Gareth Black *is a thought leader in the field of crisis management, emergency response, and human factors. Gareth's master's degree in Homeland Security and Crisis Management, alongside his lecturing work at Coventry University mean he is at the cutting edge of developments in the field. He has a unique ability to turn his wealth of academic experience into simple, practical, and intuitive solutions for clients, ensuring they remain at the forefront of crisis management practice. Gareth has received accolades for his work with the National Health Service, preparing for, responding to, and recovering from a wide range of incidents whilst also working on policy and procedural developments of national and international significance.*