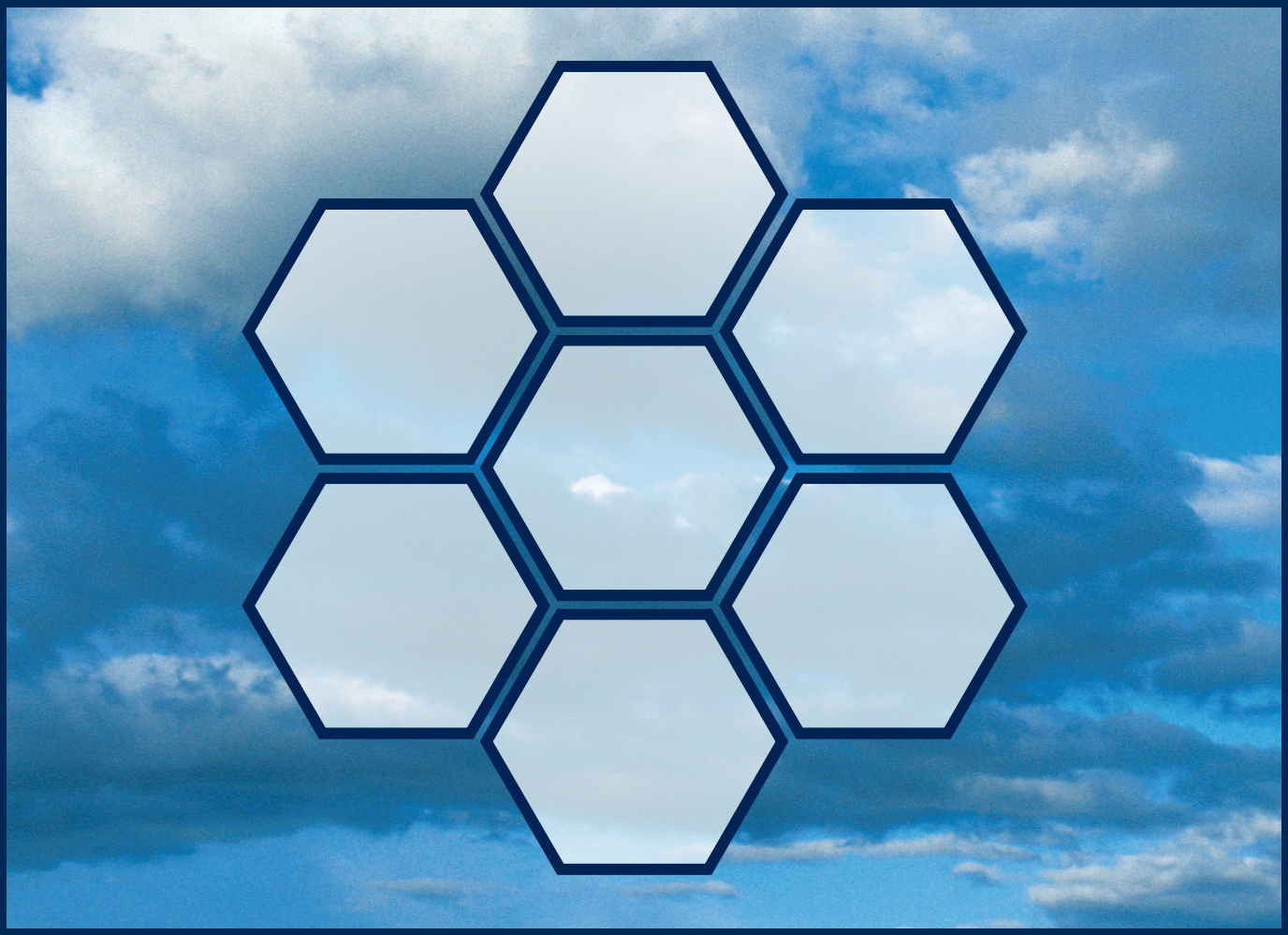
Comprehensive Preparedness Planning



DEMA
DANISH EMERGENCY MANAGEMENT AGENCY

Comprehensive Preparedness Planning

Published by: Danish Emergency Management Agency
Datavej 16
DK-3460 Birkerød
Tel. + 45 45 90 60 00
Fax + 45 45 90 60 60
E-mail: brs@brs.dk
www.brs.dk

Layout: Danish Emergency Management Agency
Print: Schultz Grafisk
B 2158
ISBN: 9788791590399

NORDISK MILJØMÆRKNING
TRYKSAG
541 176

Comprehensive Preparedness Planning

Danish Emergency Management Agency 2009

Contents

1 Introduction

The Danish Emergency Management Agency (DEMA) has developed this guide as a voluntary tool to improve the quality of existing preparedness planning or to start new planning activities.

The guide is an integral part of DEMA's webpage on comprehensive preparedness planning. Here, more inspiration, practical tools and suggestions for further reading can be found – although in Danish-language versions only. The address is www.brs.dk/hob. English-language material from DEMA that readers may find useful can be found at: www.brs.dk/uk and at www.brs.dk/fagomraade/tilsyn/csb/Eng/Civil_preparedness_division.htm.

The guide – like the contents of the webpage – will be revised as the need arises. DEMA attaches importance to dialogue in the further development of our material, and we encourage everyone to send comments and experiences to us on: csb@brs.dk.

1.1 What is comprehensive preparedness planning?

Preparedness planning is about preparing for extraordinary incidents that cannot be managed with ordinary resources and routines alone.

The purpose of the planning for each organisation is to strengthen its ability to prevent incidents, where it is possible, and to manage them, when it is necessary. In other words, preparedness planning is about creating resilient organisations.

As the logo for comprehensive preparedness planning illustrates, we divide the planning concept into seven general areas.

The seven areas of comprehensive preparedness planning – briefly explained:

1. **Programme management** – which should be the central, pivotal point of the planning.
2. **Planning assumptions** – analyses and ongoing activities that support planning in the remaining areas.
3. **Prevention** – measures that may prevent incidents or reduce their probability and consequences.
4. **Training** – for all employees who have a role in the organisation's emergency preparedness.
5. **Exercises** – which all organisations in the guide's target group should conduct and participate in.
6. **Evaluations** – in order to utilise the learning potential from incidents and exercises.
7. **Crisis management plans** – which describe how the organisation has prepared to respond to incidents.

The notion that the organisation's preparedness planning should be ''comprehensive'' does in this connection mean that:

- The organisation carries out planning activities within all seven areas.
- The planning activities are arranged according to the organisation's needs, rather than carried out in a particular order.
- The planning covers all the critical functions that the organisation is responsible for.
- The organisation's management is actively involved in the planning.
- Relevant employees throughout the whole organisation take part in the planning.
- The organisation involves relevant external partners in the planning.

Comprehensive preparedness planning focuses on the general build-up of capacities that can protect organisations' critical functions and values such as life, welfare, property, environment, reputation, etc., and is thus not limited to particular types of extraordinary incidents.

The seven areas of comprehensive preparedness planning are presented below, each in its own chapter, together with recommendations for good practice. One of the most central recommendations is that the planning process should result in three key documents:

- A preparedness policy (described in Chapter 2)
- A preparedness programme (described in Chapter 2)
- A general crisis management plan (described in Chapter 8)

1.2 The guide's target group and delimitations

The guide is addressed to all entities that play a part in society's ''collective emergency preparedness''.

The target group is primarily public sector authorities and companies – regardless of whether they are central government departments, agencies, state-owned enterprises, regional administrations, municipalities or underlying local institutions, etc. Private companies with critical functions are also welcome to use the guide – e.g. private owners and operators of critical infrastructure like energy supply, IT and telecommunications, hospital services, etc.

As the target group is very large, the generic term ''organisations'' will be used throughout the guide.

The guide contains suggestions for a concrete procedure for preparedness planning. It should be stressed, however, that specific preparedness planning initiatives always have to be adapted to each organisation's needs, and to the specific legal requirements and guidelines that the particular organisation must adhere to.

2 Programme Management

It is the management's responsibility to ensure that the organisation is able to perform its critical functions under normal circumstances. These functions must also be performed when the organisation is subject to extraordinary incidents like e.g. serious accidents or disruptions of critical infrastructure. Consequently, the management must ensure that the organisation has at its disposal a robust and flexible crisis management organisation that can be used when ordinary resources and routines are insufficient.

The principles for active involvement of the management in preparedness planning do not differ from other areas of responsibility. Also in this context, it is managers who must determine objectives, set overall priorities, delegate tasks, allocate resources and follow up on the planning.

2.1 Key management documents

In connection with the ''programme management'' area of comprehensive preparedness planning, we recommend that managers and preparedness planners produce two central documents:

- An overall preparedness policy
- A more detailed preparedness programme

Before writing the two documents, it is an advantage to examine the amount and status of existing planning, so that new efforts can be concentrated in areas, where the organisation has the biggest needs. A questionnaire to key members of staff may be a useful tool in this respect.

Preparedness policy

The aim of the preparedness policy is to determine the overall framework for the organisation's preparedness planning. The quality of the work within the seven areas depends on clear objectives and sound organising principles. The preparedness policy should therefore ideally be a short document where the following aspects are adressed:

- Objectives for the emergency preparedness: What does the organisation want to achieve with its emergency preparedness capacities?
- Formal requirements: What laws and regulations on emergency preparedness must the organisation adhere to?
- Summary of preparedness responsibility: What are the critical functions that the organisation is responsible for maintaining? (See section 3.1.)
- Overall prioritisation: Which of the seven areas should be emphasised the most?
- Expectations for participation: Whom in the organisation does the management expect to contribute actively to the ongoing development of the emergency preparedness?

Once completed, the management should approve and communicate the preparedness policy to the whole organisation.

Preparedness programme

The purpose of the preparedness programme is to expand upon the preparedness policy, so that the management's general priorities can be translated into concrete activities. Thus, the programme sets out concrete direction for the organisation's preparedness planning – for example, for the next 12 months or a longer period. In comparison with the policy document, the preparedness programme should be open to adjustments during the specified period – i.e. flexible enough so that new activities can be added, resource allocations changed etc.

We recommend that the preparedness programme contains a general part that briefly describes:

- Prioritisation for the coming time period: Which areas should be worked on in particular?
- Designation of responsibility: Which organisational unit (e.g. an emergency management office or a risk management section) is responsible for coordinating preparedness planning activities internally and with relevant external public or private sector partners?
- Management involvement: How should managers be involved in the ongoing planning process?

Hereafter, the preparedness programme should briefly describe for each of the seven areas:

- What the organisation wishes to obtain within each area.
- Which concrete tasks should be carried out to reach the objectives.
- Which units are responsible for what tasks, and which of the organisation's additional units and personnel should contribute.
- Which activity and time schedules apply for the prioritised tasks.
- Which resources are made available (see section 2.2).
- How to follow up on the results (see section 2.3).

In this way, the preparedness programme should reflect the prioritisation of organisational needs and will – if regularly revised – improve possibilities for coherence, continuity and momentum in the preparedness planning work.

In the following chapters, we elaborate further on each areas of comprehensive preparedness planning, and each chapter can thus provide input to the descriptions in the organisation's preparedness programme.

2.2 Resource prioritisation

The organisation's management must – in close connection with the preparedness programme – ensure that there is an appropriate allocation and use of resources devoted to emergency preparedness. Preparedness planning is not something that only takes place on paper, nor is it free. Requirements may continuously arise for specific equipment, personnel, facilities, systems, etc. Because of this, it is necessary to make decisions relating to aspects such as procurement, development, maintenance, composition and geographic distribution.

Good practice for resource prioritisation in preparedness planning is to a great extent identical to what applies to other goods and services. Among other things, the organisation must use transparent purchase processes, estimate costs and benefits of products and services, and choose reliable suppliers, who live up to current quality requirements. However, the management must pay attention to particular conditions including:

1. It is difficult to estimate the costs vis-à-vis the benefits gained from an improved ability to prevent or manage incidents. Preparedness planning is therefore similar to considerations about insurance, where premium payment is compared to possible losses. The organisation invests in capacities it hopes will rarely be needed and where the real value is hard to assess.

2. Only for some emergency preparedness measures (e.g. fire prevention equipment) can acquisition and operating costs be attributed exclusively to the ''emergency preparedness account''. On the contrary, many measures serve several purposes. For example, a crisis control room can also be used for meetings under normal circumstances. SCADA-systems (Supervisory Control and Data Acquisition) have both preparedness and operational roles for power stations, water works, and other types of critical infrastructure.

3. Unexpected expenditures often occur during crises, where the organisation's decision-makers must prioritise sparse resources under time pressure and without accurate information. As a general rule, it is better to establish a preparedness level that is a little too high rather than too low during a crisis. Yet, the organisation must also be able to quickly downscale the preparedness level in order to avoid waste of resources. Normally, it is easier to adjust preparedness levels in a downward direction than in an upward direction.

In connection with the organisation's preparedness programme, it may be an advantage to prepare a specific procurement policy for emergency preparedness purposes. Such a policy can for example include guidelines for authorising staff to make extraordinarily expensive or urgent purchases during crises. If possible, high-value items of expenditure that are known in advance might also be described directly in the organisation's preparedness programme.

2.3 Follow-up

Management must make sure that planned activities are carried out, and that results live up to the objectives, requirements and agreements determined in the organisation's preparedness policy and preparedness programme. To do this efficiently, management should consider:

- Who will follow-up on the planning in general and within each individual area?
- Which activities must be especially closely supervised?
- How should the different forms of follow-up be carried out?

The term ''follow-up'' must be broadly understood in this context. From a central management level, routine advice and guidance will often be sufficient – perhaps combined with voluntary self-evaluation and assurance amongst organisational units and subordinate institutions.

In other cases, more formal internal or external supervision should be carried out to control what is accomplished, how it is accomplished, and how well it is accomplished. Such supervision improves coordination and is particularly relevant for larger organisations with many levels and decentralised units that conduct independent preparedness planning. For government authorities, the supervision – whether it is voluntary or compulsory – can be a means to exercise their sector responsibility and keep checks on private companies that hold preparedness obligations as a result of contracts, outsourcing, privatising, etc.

Examples of follow-up methods

- Quality assurance of crisis management plans.
- Result and effect measurements after the launch of information campaigns.
- Monitoring of the abidance of rules for information security.
- User satisfaction polls.
- Formal auditing.

Finally, the follow-up are in some instances carried out as external audits based on specific legislation, guidelines or criteria established by authorities.

3 Planning assumptions

Work in the area ''planning assumptions'' can help the organisation reach a sound knowledge base, which can in turn feed into the work within the other areas of comprehensive preparedness planning.

In the planning assumptions area, the organisation should consequently acquire an overview of:

- Which of the organisation's functions are critical?
- Which threats are relevant for the organisation?
- Which threats constitute the biggest risks, and where is the organisation most vulnerable towards the threats?

3.1 Mapping of critical functions

The purpose of mapping critical functions is to assure that the organisation has recognised which activities, goods and services it must be able to maintain, even when the organisation is affected by extraordinary incidents. The organisation must in this connection identify:

- Which critical functions the organisation has operational responsibility for.

- Which critical functions the organisation has overall political, legislative or administrative (sector) responsibility for.

- Which resources the organisation is particularly dependent on in order to maintain its critical functions with none or only minimal disruptions. Such resources may include:
  - Employee profiles (e.g. specific leaders and technical specialists).
  - Infrastructure (e.g. buildings, installations, networks, and means of transport).
  - Goods and services (e.g. power supply, raw materials, equipment, spare parts, IT services, and guard duty). The organisation must both identify dependence on the actual resources and the internal and external suppliers of the resources in question.

What constitutes a critical function for a given organisation depends on the nature and purpose of that organisation. At higher level of analysis, critical functions are those activities, goods and services that form the basis for society's ability to function. These include, among others, energy supply, IT and telecommunications, transportation, water and foodstuffs, financial services, police, rescue services, health services, and social services.

The mapping can in practice be performed by writing lists of critical functions, key employees, infrastructure, and other critical resources. To avoid unnecessary long lists, the selection must focus on what is truly critical rather than what is ''merely'' important.

3.2 Identification and monitoring of threats

An organisation with preparedness responsibility should keep up do date with the spectrum of threats that can affect its critical functions and values like life, welfare, property, environment, reputation, etc. The identification of new threats and the monitoring of known threats is useful as a separate activity but also as input to subsequent risk and vulnerability analyses.

In practice, identification and monitoring threats requires the organisation to collect reliable information that can illustrate:

- The character and causality of individual threats.
- What the comprehensive, current threat picture for the organisation looks like.
- What the potential threat picture might look like in the near future or in the longer term, including:
  - If experiences from similar organisations nationally or abroad indicate that there are threats, which the organisation should pay more attention to.
  - If the development of society in general or changes in the organisation itself mean that new threats become relevant, or that others become irrelevant.

Identification and monitoring of threats can be integrated in the general information gathering performed by the organisation's employees on a daily basis via the media, special literature, networking activities, etc. In some cases, this is supplemented by reception of specific security intelligence and threat assessments. The organisation must then assure that the relevant information is passed on to the appropriate persons.

Certain threats will be relatively easy to identify and monitor, because they often result in incidents, or because they for other reasons are already subject to great attention in the organisation. In other cases good imagination is needed to predict new threats or new ways that well-known threats can develop. A creative process with brainstorming can help, and can for example be systematised via workshops or interviews with managers and key employees.

Could it happen to us?

Experiences from incidents elsewhere can be used in connection with the identification and monitoring of threats. Examples from Denmark:

- Industrial fires in harbour facilities in Århus (2008).
- Contaminated drinking water in Køge (2007).
- Evacuation of flooded residential neighbourhood after heavy rains in Greve (2007).
- Gas explosion at racecourse in Århus (2007).
- Explosion at fireworks factory in Kolding (2004).
- Power outage in eastern parts of Denmark and southern Sweden (2003).
- Oil pollution at Grønsund (2001).
- Leak of poisonous smoke with PVC during fire in plastic product factory in Allerød (2000).

The outcome of the identification and monitoring process can be a ''threat catalogue'' (i.e. a list of man-made, natural and technological threats) or a ''scenario bank'' (i.e. a collection of descriptions of potential incidents) that the organisation wants to prepare itself for. These documents can then subsequently be used directly in risk and vulnerability analyses.

3.3 Risk and vulnerability analyses

The threat picture is complex for many organisations. In addition to this, it is neither practically nor economically possible to mitigate all threats. The purpose of risk and vulnerability analyses is therefore to create an overview of the threats that constitute the biggest risks, and the vulnerabilities the organisation has in relation to these threats.

Risk and vulnerability analyses can hereby form the basis for proposing countermeasures against the threats. If carried out regularly, the analyses can also enable considerations about preparedness to become integrated in the organisation's various other planning tasks.

Risk and vulnerability analyses are for example used in relation to:

- Dimensioning of municipal rescue services.
- Maritime port facility security assessments.
- Preparedness planning within the electricity and natural gas sectors.
- Compliance with IT security standards.
- Financial sector reviews of operational risks.

Risk and vulnerability analyses can be handled in different ways according to which specific method the organisation uses. We recommend that the analyses cover the following elements:

1. Selection of analytical focus – e.g. continuity of the organisation's critical functions.

2. Selection of threats to be analysed – e.g. using a threat catalogue or a scenario collection.

3. Assessment of the probability that the chosen threats could turn into real incidents.

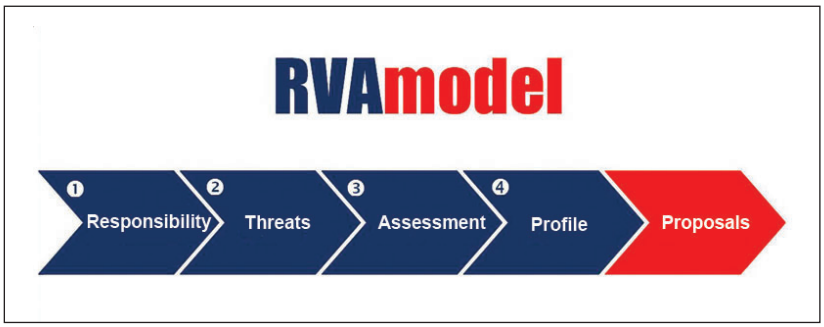
4. Assessment of the possible consequences, if the threats result in incidents, including:
- Effects on the organisation itself and its critical functions – e.g. consequences for employees, buildings, equipment, IT, products, finances, reputation, etc.
- Effects on societal values, which the organisation share responsibility for protecting – e.g. loss or damage to life, welfare, property, environment, security of the population, critical infrastructure, etc.

5. Assessment of vulnerabilities, internally in the organisation, towards the threats that constitute the biggest risks. The analysis can for example expose:
- What measures have been implemented to prevent a particular incident.
- If training and exercises empower employees with competences to handle incidents.
- To which extent existing crisis management plans have prepared the organisation.
- If sufficient operational capacity is at disposal for response, relief and recovery.

6. Weighing the analysed threats, risks, and vulnerabilities in relation to each other. Graphic representation like a risk matrix (see page 16) and a vulnerability index can be used.

7. Reporting and listing proposals for potential initiatives to reduce risks and vulnerabilities.

An example of a general tool is the Danish Emergency Management Agency's model for risk and vulnerability analysis: the RVA model. It is a user-friendly electronic tool consisting of four templates, which can be freely adapted to sector specific or individual organisations' needs.



The RVA model can be found at:
www.brs.dk/fagomraade/tilsyn/csb/Eng/RVA/the_RVA_model.htm.

4 Prevention

The organisation must implement preventive initiatives and integrate them in the organisation's other planning initiatives. The objective is to either completely avoid extraordinary incidents; reduce the probability that they may occur; or bring the potential consequences down to an acceptable level, where they can be handled by normal operating procedures rather than require activation of crisis management plans and emergency operational response.

Prevention is relevant in all areas of society, and plays an important role within for example town planning, construction works, operation of critical infrastructure, information security, traffic safety, handling of hazardous substances, fire protection, health and safety in the workplace, etc.

Preparedness planning in the area of prevention should be done via a risk based approach, where the organisation's tolerance towards different incidents determines which initiatives it chooses to implement. We therefore recommend focusing on the following three questions:

Examples of prevention

- To position dangerous industry far away from residential neighbourhoods, schools, hospitals, rest homes, etc.
- To dimension drainage systems and limit construction in low-lying areas, in order to reduce the consequences of flooding or extreme rain.

- Which incidents does the organisation aim to prevent?
- How can the incidents be prevented?
- How can prevention be integrated in the organisation's other planning initiatives?

Based on its answers to the three questions, the organisation can opt to produce an action programme which outlines future prevention work to be carried out.

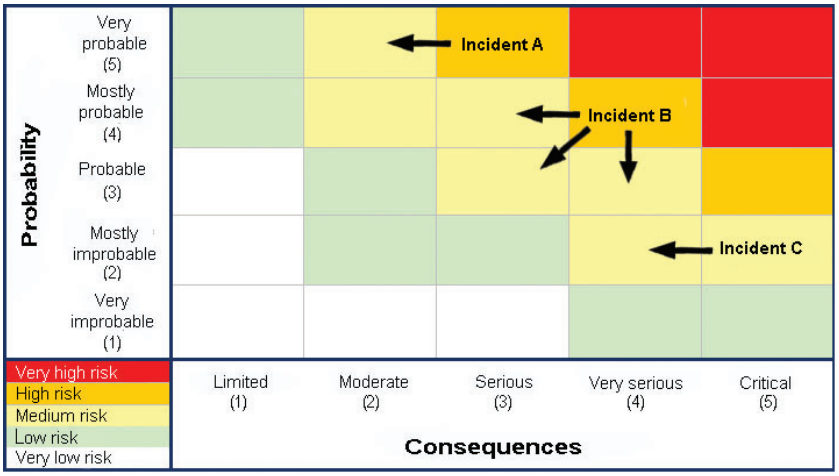
4.1 Which incidents does the organisation aim to prevent?

Prevention presupposes an up-to-date overview of the threat picture facing the organisation, and the risks associated with it. Identification and monitoring of threats, risk and vulnerability analyses, and other forms of experience collection can help generate such an overview (cf. Chapter 3 on Planning Assumptions). On this basis, the organisation can then evaluate:

- Which particular threats constitute unacceptable risks for the organisation? Whether or not the risk level for a given threat is unacceptable is determined from the probability for, and the possible consequences of that threat resulting in an incident.
- Which of the unacceptable risks the organisation is able to influence – either by measures that reduce the probability of incidents occurring, or by measures that limit the possible

consequences of incidents that do occur? Preventive measures will often work in the interest of reducing both probability and consequences.

When choosing the risks that are unacceptable for the organisation, focus must primarily be directed towards the relatively rare but potentially most serious individual incidents. More commonly occurring incidents must also be considered, however, if they collectively result in unacceptable consequences when added over a certain period. Many organisations live with risks that they might be able to reduce relatively easily, but which they nonetheless accept because the risks, when viewed separately, are not perceived as particularly dangerous.



4.2 How can the incidents be prevented?

When considering which initiatives will be most effective vis-à-vis the incidents that have been singled out as warranting preventive efforts, these may be chosen within two general categories:

- Physical measures
- Influencing behaviour

Physical measures

This technical-oriented category of prevention serves the purpose of protecting or making facilities, systems, equipment, etc., more resilient. There exist a wide range of measures with varying characteristics to choose from. Physical measures can, for instance, be:

- Directed at preventing one specific type of incident (e.g. smoke detectors and fire doors) or directed towards several types of incidents simultaneously.
- Automated (e.g. standby power generators and back-up servers) or require human action.
- Used in a stand-alone or combined manner. For example, protecting an installation against unauthorised access can be achieved via physical barriers (fences, gates, locks, guards, etc.) as well as electronic security (alarm systems, surveillance cameras, etc.).

Prevention by means of physical measures is often regulated by legislation, directives, technical codes, etc., and in certain areas it is subject to frequent control (e.g. fire inspections, health and safety inspections, foodstuffs control). In such circumstances, each organisation may consider if it is in its own interest to adopt even more extensive preventive measures than those that are made mandatory by authorities. In addition, there is a need for close collaboration between organisational units in order to ensure a coherent prevention strategy, e.g. among local government departments which administer different laws and regulations.

Influencing behaviour

This type of prevention is directed at building, maintaining, or changing people's knowledge and attitudes – and though that – their behaviour. An important intermediate aim is to strengthen each person's own ability to prevent or react appropriately to undesirable incidents.

The target group can be the organisation's own employees, external partners, clients, costumers or the general population. When the target group is the organisation's own employees, training and exercises play an especially important role (cf. chapters 5 and 6). Two other means – both internally and in relation to the surrounding society – are rules and information activities.

Only authorities may issue legally binding rules for the behaviour of companies and citizens. However, all organisations can lay down rules for their own employees' behaviour in the workplace. This may for example include an IT security policy with rules concerning the use of passwords, administrator rights to networks, storage and sharing of sensitive data, etc.

Information activities to influence behaviour can also take many forms, including for example:

- Guides, reports, strategies, educational material, etc. Sector responsible authorities can for example issue publications to guide other organisations in fulfilling the conditions stipulated by legislation.
- Purposeful prevention campaigns, for example workshops, teaching, TV and radio features, advertisements, competitions on the internet, local community meetings and other public arrangements.
- Publishing relevant preparedness information on the organisation's webpage and intranet.

Prevention through physical measures or influencing behaviour can both be resource intensive and measurable results are difficult to obtain in the short run. When the organisation chooses between alternative initiatives in the area of prevention, it must therefore compare their costs with expectations of how well the initiatives in question will work. In cases where the organisation due to practical, economic, or other reasons cannot or will not invest in prevention, it must rely solely on capacities for operational emergency response. An alternative option can be to transfer risks by taking out insurance against incidents, but this is by no means always possible and, in any case, insurance policies only cover purely financial consequences.

4.3 How can prevention be integrated into other planning?

The prevention area of comprehensive preparedness planning must be viewed in close connection with the organisation's planning for operational emergency response, which is further described in the guide's Chapter 8 on Crisis Management Plans.

Prevention can drastically reduce the dependence on and costs of operational response capacities. On the other hand, the necessity of operational emergency response capacities illustrates that incidents can never be completely avoided despite preventive measures. Hence, the organisation's preparations to manage incidents complement its work in the area of prevention.

Furthermore, many initiatives have qualities that are relevant to both prevention and operational response, and this illustrates that there is no sharp line separating the two preparedness planning areas. A mobile generator can for example simultaneously be viewed as a preventive measure to limit the consequences of a power outage and as a piece of equipment to be deployed as part of the operational response to a power outage.

Similarly, prevention should, as far as possible, be considered on equal terms with quality standards, cost efficiency, etc., in the organisation's various other planning activities. In for example a municipality there will be numerous activities where considerations about prevention are relevant. Examples include everything from the day-to-day crime prevention collaboration between schools, social services and the police, to the current efforts to include calculations of future climate changes into municipal zoning plans for urban and rural areas.

5 Training

The organisation must ensure that the people, who are a part of its emergency preparedness, possess the necessary competences to perform their emergency preparedness tasks. This applies to all employees regardless of their specific functions.

To ensure that relevant competences are developed and maintained, the organisation's management and preparedness planners should systematically consider three questions:

- Which competences should the organisation have at its disposal?
- Who among the employees should be trained/ improve their competences further?
- How should the training/competence improvement be conducted and sustained?

5.1 Which competences should the organisation have at its disposal?

The organisation should first acquire a general overview of competences it must have at its disposal in connection with preparedness planning and crisis management. This includes considerations about whether people with these competences must be employed directly in the organisation or if the competences can be procured from external sources.

The organisation might on this basis create a dedicated training programme. Such a programme could for example include a catalogue of training activities offered to employees.

As a starting point, all employees involved in the emergency preparedness should have solid knowledge of the organisation's preparedness policy, preparedness programme and general crisis management plan. In this respect, special emphasis should be on employee awareness regarding the crisis management unit and the procedures for the five core tasks of crisis management (read more in Chapter 8). Some functions in the organisations emergency preparedness may demand that certain employees have security clearances from the authorities.

For some employees it is relevant to supplement the general training with more specialised training courses. For people with specific tasks during crisis, relevant course topics may for example include:

- Strategic/operational/tactical crisis management.
- Staff participation.
- Use of relevant information technology for crisis management.

- Crisis communication and press liaison work.
- Operational emergency response within the organisation's preparedness responsibility areas.

Individuals who are responsible for or involved in the organisation's more general preparedness planning can benefit from specialised training in subject matters like:

- Risk and vulnerability analysis.
- Prevention.
- Exercise planning.
- Evaluation of operational responses during real incidents and exercises.
- Production of general crisis management plans, auxiliary plans, contingency plans, action cards, etc.

5.2 Who among the employees should be trained?

Based on its identification of competence needs, the organisation must choose the employees who are to be offered special emergency preparedness training. The training should include initial training of new employees as well as maintenance and improvement of long-term employees' skills. When planning training activities, it is therefore necessary to consider staff turnover, shifts in job functions among co-workers, etc.

It will usually be beneficial to offer training to the following personnel:

- Operative employees – who must solve specific operational tasks during crisis, e.g. frontline responders in rescue services, hospitals, municipal health care, elder care, public transport companies, etc.
- Crisis managers – who have the overall responsibility for the organisation's crisis management.
- Chiefs of staff, staff participants, and liaison officers – who are to take part in the organisation's own crisis management unit or in multiparty crisis management staffs, e.g. at the local, regional, or national level of society's collective emergency preparedness.
- Communication specialists – who must communicate with the public and the media during a crisis.
- Employees in support functions – IT support, secretarial staff, drivers, cafeteria staff, etc.
- Preparedness planners – people with responsibility for the various other areas of the organisation's comprehensive preparedness planning.

No matter which precise function an individual employee has to master, the training should, as far as possible, build on his/her existing competences, so that the available time for training is not misused on subject matters that he/she is already familiar with.

5.3 How should the training be conducted and sustained?

The training options cover a wide spectre: from short, internal introduction courses about the organisation's emergency preparedness to longer, qualifying education. The choice of training forms depends on, among other things, the requirements for employees' competences (specified by external authorities or the organisation itself), ambitions, and available finances.

Many courses with emergency preparedness content are on offer both within the public sector and from specialised private companies.

Preparedness relevant themes are also part of certain subjects at universities, vocational colleges, and other educational institutions. In some countries, there are complete masters degree programmes devoted to emergency preparedness. Moreover, training can be conducted via distance learning and e-learning, just as the organisation can improve competence levels by recommending literature to its employees.

Training of course also results from employees' participation in various coordination forums, conferences, seminars, workshops, etc.

Finally, a large part of the training should take place on the job (''learning-by-doing''). By giving employees new tasks – or letting them perform existing tasks in innovative new ways – the organisation helps to ensure that new knowledge and new skills are developed. The organisation may for example increase the number of employees with preparedness relevant competences by involving more people in the work to keep crisis management plans up-to-date; by letting less experienced staff participate in exercises; or by encouraging ''apprenticeships'' among veteran and novice co-workers who must be able to replace each other at short notice in case of an incident.

6 Exercises

The organisation should exercise regularly and in a diversified manner as preparation for managing extraordinary incidents. The purpose is to test and help develop the organisation's:

- Employees
- Plans and procedures
- Equipment and technology
- Cooperation with external partners

This best way to achieve this is for the organisation to arrange its own internal exercises as well as participate in multi-party exercises arranged by others, with focus on cooperation during crises.

Keeping the above purpose in mind, the organisation should primarily consider the following three questions when planning its exercise activities:

- What should the organization exercise?
- Who should participate in exercises?
- How should the organisation conduct exercises?

6.1 What should the organisation exercise?

The content of the exercises should be arranged in a manner that relates to the organisation's emergency preparedness responsibilities, its objectives, and the particular threat picture that it faces. Typically, an exercise will concentrate on the organisation's handling of a specific type of incident, as described in an exercise scenario. Alternatively, an exercise may – independent of incident type – be designed to train employees' competences in relation to one or more of the five core crisis management tasks (cf. Chapter 8).

What each organisation should exercise depends on its needs for development. Exercises can be used to reveal what works well, and should therefore be maintained, and what does not work well, and thus should be changed. In addition, exercises can be used to improve the emergency preparedness through testing of new techniques, procedures, etc. in a controlled environment. If the organisation only trains the functions it already knows it performs well, exercises risk becoming showcases, with limited benefits in the form of training or new knowledge.

Exercises are carried out in a controlled environment, but as a main rule they should be as realistic as possible. Realism can for example be enhanced by basing the exercises on previously experienced incidents or incidents, which the organisation fear could take place in the foreseeable future. Moreover, there must be consistency between those plans, etc., that are used during the exercises, and those that are used during real incidents.

6.2 Who should participate in exercises?

As a starting point, exercises must involve organisational units and individuals who carry out crisis management and operational response during real incidents. However, the group of potential participants will vary – depending on the content of a specific exercise, and on whether it is purely an in-house exercise or a joint exercise with other organisations. The participants can for example be members of the organisations crisis management unit or liaison officers; employees from communication departments, IT-departments, and other support positions; or selected groups of staff in decentralised units with operational tasks.

To make sure that the right people participate in a specific exercise, particular attention should be paid to the employee turnover that has occurred since the last, similar exercise. Moreover, participation in exercises should, as far as possible, be coordinated with the wider training of staff with a role in the organisation's emergency preparedness (see Chapter 5 on Training).

6.3 How should the organisation conduct exercises?

Depending on objectives, ambitions, and available resources, the organisation can choose between different forms of exercises. Here, we divide them into four overall types: Procedure exercises, dilemma exercises, crisis management exercises, and full-scale exercises. Note that other designations exist, which are close to these, and which varies in use from organisation to organisation.

The organisation can benefit from producing a specific exercise calendar or action plan as a part of its preparedness programme (cf. Chapter 2), where the resources dedicated to one or more of the four types of exercise are spread over a period of several years.

Procedure exercises

The purpose of procedure exercises is to test, whether one or several specific procedures in the organisation's emergency preparedness work as intended, or if improvements are needed. Procedure exercises can normally be conducted without extensive prior planning or expenses.

A variant of the procedure exercise is a warning or alarm drill. In its shortest form, this can be a test to see if relevant members of the organisation's crisis management unit can be reached by telephone or other means. In an extended form, it can be a test to see if employees physically show up where they should according to the crisis management plan. In this manner, the organisation can make sure that its procedures are adequate; that contact information is complete and up to date; and that communication technology for alerting people is working.

Another variant of the procedure exercise is the evacuation drill, where the organisation tests if staff and guests at a given time exit the building quickly and in an orderly fashion in the event of fire, bomb threats or other serious incidents.

Dilemma exercises

Dilemma exercises are also called discussion exercises or table-top exercises. The organisation can conduct this kind of exercise by gathering the appropriate participants to ''role play'' how they would handle different aspects of one or more incidents in real life. The participants can either play themselves or they can play another role, e.g. a different staff category from within the organisation or an external partner organisation. Dilemma exercises typically last approximately half a working day, but can also just be brief discussions of how the crisis management unit would handle a specific task – e.g. how to prepare a combined situation picture or set in motion a crisis communication strategy.

If the organisation has not held a dilemma exercise before, it is recommended to conduct it with a timeframe that gives participants ample time to find acceptable solutions. More experienced organisations can conduct dilemma exercises where more pressure is put on the participants by introducing some of the limitations or problems that exist during real incidents. This may for example include time pressure, incomplete information, overfilled rooms, long work hours, unexpected changes in personnel, intense media attention, etc.

Crisis management exercises

During crisis management exercises the participants must rehearse their actual roles during crisis in their normal work situation. Usually, the participants do not know in advance to what extent they must take part in the exercise, and they will have to attend their normal duties at the same time. Crisis management exercises can thus, to a higher degree than dilemma exercises, test practical aspects of crisis management, even though decisions are only made on paper – i.e. nothing happens in the field. Another significant advantage is that participants get to know more thoroughly the people and organisations they must cooperate with during real crises.

In comparison with dilemma exercises, crisis management exercises require more extensive planning, including among other things exercise regulations, an exercises script, an exercise management cell and a team of observers. Crisis management exercises also vary more in size.

Full-scale exercises

Full-scale exercises are directed towards the operational level and typically include emergency response activities at a simulated accident site (e.g. putting out fires, erecting barriers, evacuating affected citizens, etc). Full-scale exercises are therefore primarily relevant for organisations that perform operational tasks during real incidents – in addition to any general crisis management tasks these organisations may perform at the central or strategic level.

A full-scale exercise can contain all of the elements that are relevant in an operational emergency response context, including raising the alarm; dispatching personnel and equipment; and coordinating the activities of several different organisations during the operational response phase. Full-scale exercises therefore provide the most intensive training and testing of operational staff. However, it is also a type of exercise that necessitates many resources and extensive planning. In addition to the same elements required for a crisis manage-

ment exercise (exercise regulations, script, etc.), a full-scale exercise imposes larger financial, logistic and personnel needs, including figurants to play victims and relatives at the simulated accident site.

7 Evaluation

The organisation should always evaluate its conduct – both crisis management and operational emergency response – following extraordinary incidents within its area of responsibility. Likewise, the organisation should evaluate its performance after all exercises – both those held internally and after participating in joint exercises arranged by others.

The purpose is to simultaneously uncover things that worked well during the incident or exercise in question, and should therefore be upheld, and things that did not work so well, and should therefore be changed to improve future conduct.

The three questions that the organisation should focus on in connection with evaluations are:

- What can the organisation attain through evaluations?
- How can evaluations be initiated and carried out?
- How is knowledge accumulated from evaluations?

7.1 What can the organisation attain through evaluations?

Evaluations of organisational conduct during extraordinary incidents and exercises can deliver useful, experience-based input to the other areas of comprehensive preparedness planning. Through evaluations the organisation can for example search for answers to questions like:

- Have the appropriate preventive measures been initiated or are there better alternatives?
- Have employees acquired the necessary competences via training, exercises, and praxis?
- Do general crisis management plans, auxiliary plans, contingency plans, action cards, etc., need adjustments?
- Does equipment and technology in the emergency preparedness work as intended?
- Are current standard operating procedures optimal or should they be altered?

When the organisation carries out its evaluations, the focus should be on ''learning'' rather than merely ''describing''. A high-quality evaluation documents the course of events (who did what, when, how, and to what effect?). However, these descriptions are made to identify leaning points, not simply for their own sake.

An emergency preparedness evaluation is:

A systematic examination of organisational conduct during an incident or an exercise with a clearly formulated purpose, a targeted collection of data, a focused analysis, and an independent assessment of the conduct according to explicit criteria, which have been determined in advance.

A short written account or oral debriefing, where the participants talk about their experiences, can be part of an evaluation but does not in itself constitute an evaluation.

In order to assess concrete potential for improvements, evaluations must account truthfully for vulnerabilities in the organisation's emergency preparedness. For example, if significant deviations have been made from the organisation's crisis management plan during an exercise, or if someone has made serious mistakes whilst responding to a real incident. In other words, the organisation must be willing to admit weaknesses to pinpoint where its emergency preparedness can be improved and strengthened.

7.2 How can evaluations be initiated and carried out?

An evaluation should be commenced and completed shortly after the specific incident or exercise in question. This is partly because the quality of the evaluation is strengthened when experiences are fresh in participants' minds; partly because decision-makers are less likely to use the conclusions and recommendations of the evaluation if too much time has passed.

To reduce reaction time, the organisation can benefit from preparing a general evaluation concept with guidelines for how the organisation intends to launch and carry out evaluations. Aspects that the organisation should consider in its general evaluation concept include:

- Who should undertake the evaluations? An evaluation can be done by people, who were performing tasks during an incident. At other times it is preferred that the evaluation is undertaken by co-workers who were not directly involved (e.g. in order to avoid bias). Finally, it may in some cases be appropriate to use external consultants (e.g. to guarantee formal independence, resource optimisation, or when specialist knowledge is required).
- Evaluation criteria. Estimations of suitability, efficiency, etc., can be related to many different aspects of the organisation's conduct during an incident or an exercise. We recommend that evaluations take as their point of departure one or more of the five core tasks of crisis management (cf. Chapter 8). These are: 1) Activation and operation of the crisis management unit; 2) Management of information about the crisis; 3) Coordination of actions and resources; 4) Crisis communication; and 5) Operational response.
- The evaluation process. Any evaluation must be designed according to the incident or exercise in question. Different elements of the process can be tackled in different ways.

7.3 How is knowledge accumulated from evaluations?

As a distinct area of the comprehensive preparedness planning, evaluations are not only about starting up one project after another. It is just as important that the organisation remembers to utilize the knowledge gained from previous evaluations. When a new evaluation is carried out, we therefore recommend revisiting existing evaluation reports, among other things to be able to systematise experiences, conclusions, and recommendations regarding the organisation's conduct across incidents and exercises. Similarly, the organisation can often extract valuable learning by examining evaluation reports written by other national and international entities.

8 Crisis management plans

Organisations with responsibility for critical functions must have a general crisis management plan. The purpose is to give the organisation's executives and employees a practical tool, which they can use when extraordinary incidents occur. Hence, the plan must describe how overall crisis management should be carried out, and how emergency preparedness capacities should be prioritised, in situations where ordinary resources and routines are no longer sufficient.

8.1 What characterises a good crisis management plan?

To fulfil its purpose as a practical tool, the organisation's crisis management plan must be:

- Action-oriented – The plan must contain clear guidelines outlining how the organisation intends to manage extraordinary incidents. That is: Who does what, when, and how?

- Comprehensible – The contents of the plan must be logically arranged and quick to search through. It should be written in plain language and not be longer than necessary.

- Up-to-date – The plan should be revised when:
  - It is mandated by legislation
  - There are indications that the threat picture has changed significantly.
  - Experiences from an incident, exercise, or risk and vulnerability analysis call for it.
  - The organisation's structure or area of responsibility changes.

- Accessible – Authorised users should have access to the plan anywhere and at all times.

- Realistic – The emergency preparedness resources designated in the plan must correspond to the resources that will actually be available during real incidents.

- Read and understood – All potential users should have studied the crisis management plan carefully in advance – i.e. before they need to use it in praxis during a real incident.

- Tested – The organisation must regularly test the plan in its entirety or essential parts of it. The plan must be evaluated thoroughly after its use during exercises and real incidents.

8.2 How can the crisis management plan be structured?

The way the contents of crisis management plans are structured differ from organisation to organisation, depending on areas of responsibility, organisational culture, traditions, etc.

We recommend that the organisation produces a single, general crisis management plan supplemented by a number of auxiliary plans, contingency plans, action cards, templates, etc.

If this advice is followed, the crisis management plan should begin with brief descriptions of:

- The plan's purpose vis-à-vis the organisation's emergency preparedness responsibilities.
- The plan's scope (e.g. validity in an organisational, sector-wise, or geographical sense).
- The plan's central premises as regards the organisation's emergency preparedness.
- The organisational unit responsible for keeping the plan up to date and testing it.
- When the plan was last updated and tested.

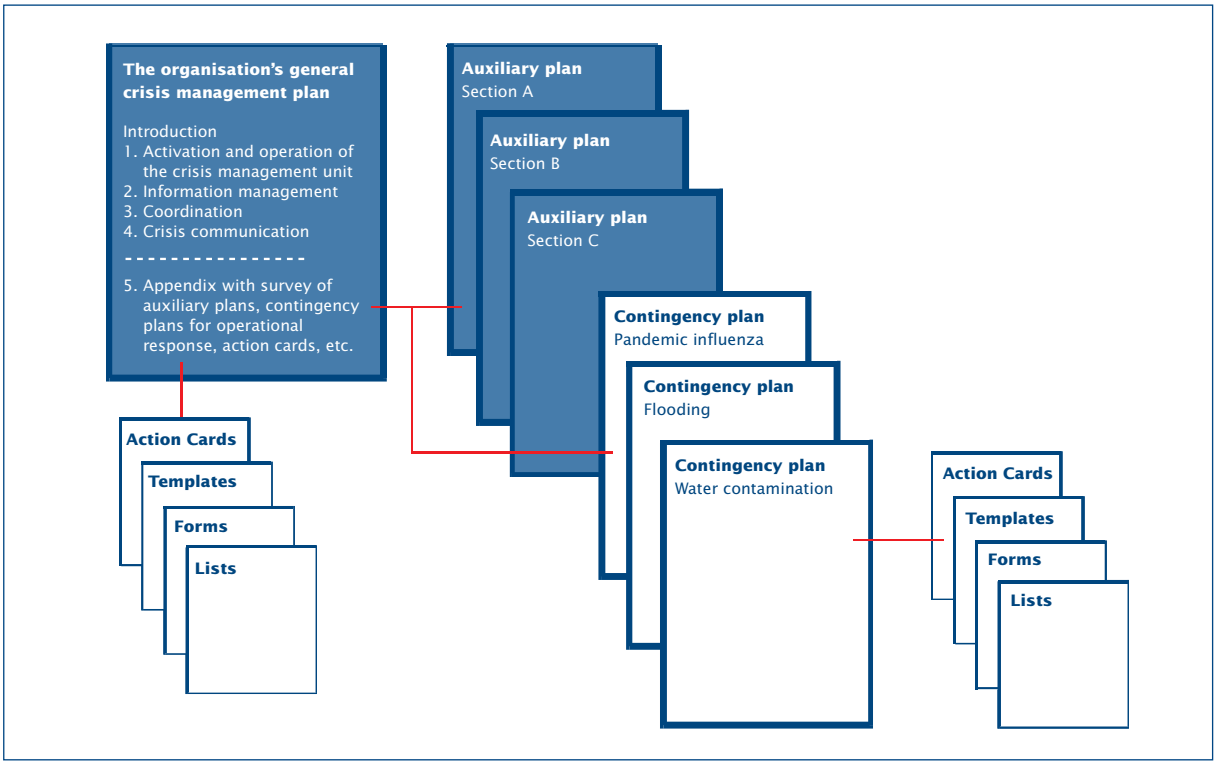
To meet the criteria of being action oriented and comprehensible, we advice against letting the crisis management plan begin with a lengthy description of the organisation (e.g. detailed facts on the structure and activities of a government agency, municipality, company, etc.). In depth information of this sort can instead be integrated in the planning assumptions (cf. Chapter 3).

Following the short introduction, we recommend a simple structure for the crisis management plan with one chapter for each of the five core tasks of crisis management:

1. Activation and operation of the crisis management unit.
2. Management of information about the crisis.
3. Coordination of actions and resources.
4. Crisis communication.
5. Operational response.

For each of these five core tasks the organisation should supplement its general crisis management plan with more detailed planning. This is best done by means of:

- Auxiliary plans for decentralised organisational units and subordinated institutions.
- Contingency plans with guidance for the operational response to specific incidents.
- Action cards with short and precise instructions regarding specific tasks.
- Templates, lists, fact sheets, and other documents that can support crisis management.



To enhance clarity, auxiliary plans, contingency plans, action cards, templates, etc. can accompany the organisation's general crisis management plan as appendixes. Alternatively, they can simply be noted in a reference index at the end of the general plan, if the number of documents is large.

The general crisis management plan and the supplementary documents in the ''combined plan complex'' should be made accessible to users in electronic form on the organisation's network as well as in paper versions. There are advantages to both formats, and the preferred format will vary from person to person, (e.g. easy to find a paper version on an office shelf vs. easy to search for a particular section of the plan in electronic format on a personal computer).

Examples of supplementary plan documents:

- Auxiliary plan for an individual municipal administration supplementing the municipality' general crisis management plan.
- Contingency plans for responding to a natural disaster, water contamination, power outage, work site accident, criminal damage, release of hazardous substances, disease outbreak, or other threats that are relevant for the organisation in question.
- Action cards with instructions for initiating warnings and alarms.
- A template for the agenda to be used during meetings in the organisation's crisis management unit.
- Templates for writing and updating situation reports.
- Lists with contact details for crisis management unit members.
- Draft versions of press releases to be concluded during crises.
- Lists generating an overview of relevant external crisis management plans, used by partner organisation.

In the following sections, the content of the five core tasks of crisis management is explained.

Core task 1: Activation and operation of the crisis management unit

All organisations should be able to set up a crisis management unit. The purpose is to give the management a fixed organisational setting with well-known and tried procedures, as soon as it is realized that an extraordinary incident has occurred, which requires crisis management.

The crisis management plan and supplementary documents should describe the following aspects regarding the crisis management unit's composition, support functions, activation, activation levels, meetings, meeting facilities, liaison officers, and substitution procedures.

Composition of the crisis management unit

Effective crisis management requires the presence of people in charge. The permanent members of the crisis management unit can be executive board directors, line managers, heads of communication sections, etc. The crisis management plan should identify these members and their possible substitutes in case of illness, absence due to travel, etc. Additionally, the plan should identify possible ad-hoc members (e.g. functional specialists) who it may be relevant to include in the crisis management unit, depending on the characteristics of the particular incident.

Support functions of the crisis management unit

The plan should identify key employees in support functions that the crisis management unit will depend on during crises, and which must therefore also be able to work outside normal hours and in holiday periods. Examples include IT-support staff, communication staff, secretarial staff, and logistical staff to arrange meals, overnight accommodation, transport, etc.

Activation of the crisis management unit

Given that the crisis management unit must be able to convene quickly in the event of a crisis, the organisation's crisis management plan should describe the following concerning activation:

- How warnings and alarms should be received and forwarded in situations that may justify activation of the crisis management unit.
- Who decides if the crisis management unit shall be activated (e.g. a senior executive), and who carries out the activation in praxis (e.g. a guard or a key employee on call).
- How permanent members, ad-hoc members, and employees in support functions should be summoned. Consequently, the crisis management plan should contain an up-to-date organisational diagram and a contact list with phone numbers (work, mobile, private) and email-addresses. The most important contact information may for example be printed in a credit card size format, for key individual to carry with them at all times.
- How to confirm that the right people have received the activation call and will show up.
- Which information that, as a minimum, should be evident from the activation call (time and place for the first meeting, participants, agenda, and initial data about the incident).

The activation levels of the crisis management unit

The crisis management plan should describe the different levels at which the crisis management unit must be able to perform its duties – e.g. via skeleton crew or a fully established unit. The appropriate activation level can often only be determined at the first meeting and must

then be adjusted upwards or downwards between meetings, depending on how the crisis develops.

The meetings of the crisis management unit

The organisation should in advance have prepared a template for the agenda to be used during the first and subsequent meetings in the crisis management unit. It can also be advantageous to describe how often the crisis management unit will typically meet, and with which assignment of roles. For example, should the meetings be led by a director or an appointed chief of staff?

The meeting facilities of the crisis management unit

The crisis management plan should describe where the crisis management unit intends to hold its meetings, and which physical and technical means it must have access to. For many organisations the crisis management room can be an ordinary meeting room that is also used for day-to-day activities. Other organisations choose to establish dedicated ''situation centres''.

The crisis management room should be of sufficient size. It should be equipped with computers, television and other IT and communication equipment, but also with more simple remedies like whiteboards, maps and written works of reference. The technical equipment must be well-known and reliable. Adequate IT security must be in place, and alternative ways of communication must have been thought through, if for example the internet connection, email, or telephone system is disrupted. The crisis management room should also – like other important facilities – be equipped with a stand-by power apparatus. Pay particular attention to how much time the emergency power supply can be expected to last.

The crisis management plan can be accompanied by instructions for maintaining the crisis management room and its equipment under normal circumstances, and an action card stating how it must be prepared at short notice in the event of a crisis. Additionally, there should be action cards for logistical matters such as rest facilities, catering, transportation, etc.

It might also be relevant to designate an alternative meeting place in the crisis management plan. A few organisations even maintain a parallel crisis management room at a different location (''second site'') in case of incidents so serious, that regular facilities cannot be used.

The liaison officers of the crisis management unit

Procedures for the operation of the crisis management unit must ensure that agreements are honoured regarding liaison officers to/from external partner organisations, cross-government crisis management staffs, etc., and that potential requests for ad hoc participation can be met.

Procedures for relieving the crisis management unit

The crisis management plan should include a procedure for how members and support staff of the crisis management unit can be relieved or replaced during particularly lengthy incidents. Exhausted people are less efficient and more likely to make wrong decisions. Substitution should ideally always include personal briefings on priority tasks, hand-over of documents, etc.

Core task 2: Management of information about the crisis

The ability to make the right decisions at the right moments depends on the crisis management unit's ability to form a shared and comprehensive overview – a ''combined situation picture''.

For this purpose, it is necessary to collect, analyse, and distribute relevant information about the crisis in all of its phases. However, a constant high level of information is demanding on both originators and recipients. The organisation must therefore prepare for an efficient management of the information flow, including making sure that the most important information will be written down, so as not to be lost or forgotten during the crisis.

In this connection, the crisis management plan and associated documents should consider the following:

Intensified monitoring

Relevant information can come from many different sources. As soon as a potential crisis situation has been recognised, the crisis management unit should initiate intensified surveillance of media coverage as well as the incoming communication to the organisation by telephone, email, fax, and, possibly, secured communication systems.

Where it is relevant, the organisation should also obtain situation reports (SITREPS) from decentralised units, liaison officers, employees involved in the operational response, and others. Both the reporting and the information management at central quarters will be easier if a common template for situation reports is used.

Registration of essential communication

The organisation should register all important written and oral communication concerning the crisis in an electronic log or journal, so that it is clear what has been said and what has been decided. Keeping such a record is not only vital for the actual crisis management, but also makes it possible to document events for subsequent evaluation purposes (cf. Chapter 7).

The registration of essential communication should begin as soon as it has been decided to activate the crisis management unit. If official journalising via day-to-day routines is slow, and if the organisation does not have a specific log system, a simple method can be to send all relevant emails c.c. to a single address kept under constant observation.

The organisation's combined situation picture

The organisation's combined situation picture is a central document for the crisis management. It must contain reliable information, which in a concise format, creates a general overview of:

- The incident – What has happened, where, when, and why?
- The media coverage – How is the media reporting on the situation?

- Risk assessment – Are there indications that the situation could get worse? Do changes since the last version of the combined situation picture was formulated influence ongoing activities or create a need for new activities?

- Actions – Who has done/is expected to do what, where, when, and how?

- Resource use – which resources are applied where, and which resources are still available?

- Crisis communication – How are the organisation's messages communicated externally?

The combined situation picture can consist of both written text and information in visual form – e.g. photos, video recordings, maps, or geographical information system (GIS) entries showing the physical location of infrastructure, buildings, vehicles, etc.

The organisation's crisis management plan must establish who has the responsibility for producing the combined situation picture (e.g. a particular office or certain members of the crisis management unit). The task is substantial and several people should be allocated to the task.

The combined situation picture will be used during every meeting of the crisis management unit and updated between the meetings. Consequently, there should be a fixed template for its structure, an instruction for contributions, and a list of recipients. These documents should be prepared in advance either as part of or as supplements to the general crisis management plan.

The organisation should be able to share its own situation picture with partner organisation and joint crisis management staffs in an attempt to reach a ''common'' situation picture.

Given that the organisation's combined situation picture is not necessarily only meant for internal use, technical terms and abbreviations specific to the organisation should be avoided.

Minutes from crisis management unit meetings

Minutes should be taken during all crisis management unit meetings, reflecting the agenda. Particular emphasis should be on recording all concrete action points and decisions reached during the meetings. Given that the minutes will function as working documents during the crisis, they must be concise and distributed quickly following each meeting. The organisation can benefit from preparing an action card that determines who takes the minutes, who proofreads and quality checks them, who approves them, and who they must be distributed to.

Management of sensitive and classified information

Information management during a crisis will often require balancing between the need to protect sensitive information from unwanted disclosure and the need for swift and smooth exchange of information. As regard classified information, however, rules regarding reception, storage, and distribution must always be adhered to. Clear instructions for correct handling of sensitive and classified documents should be evident from the general crisis management plan.

Core task 3: Coordination of actions and resources

Crisis management never takes place in a vacuum. There will always be a need for coordination of actions and resources – both within the organisation and vis-à-vis external partners. As regards the internal coordination, the organisation's crisis management plan should include:

- Procedures for generating a collective overview of ongoing actions and resource allocation at the central level and in decentralised units. To this end, the organisation may for example use a resource database, survey, or list to sum up personnel and equipment that are either deployed, ready for immediate deployment, or form non-activated reserves. Such a resource account is useful in its own right, and will at the same time contribute to the organisation's work when formulating a combined situation picture.

- Instructions for how employees and other resources can be transferred between different units during a crisis (e.g. via secondments). In this connection, its is important to consider not only the crisis management needs, but also the fact that the ''basis organisation'' – independently of the crisis – must uphold other critical functions at an acceptable level, whilst the crisis management takes place (business continuity planning).

- Principles for decision-making competence, including how such competence is delegated from the strategic to the operational level. The people responsible for the operational response should, as a general rule, be authorised to allocate available resources as they see fit. They should have a mandate to make all operational decisions, as long as the crisis management unit is kept informed. The organisation may want to adopt some guidelines for how to side-step normal decision-making procedures, if these have the potential to inhibit crisis management in situations that require urgent decision-making.

- Procedures for authorising executives to obtain and allocate extraordinary large sums, so that crisis managers are not forced to act on an uncertain or insufficient financial basis.

As regards the external coordination of actions and resources, the organisation's crisis management plan should primarily consider:

- Which entities the organisation will usually have to coordinate with during crises, and how to initiate bilateral cooperation immediately from the onset of a particular crisis.

- How to find out which actions other organisations are planning or have already set in motion to deal with the crisis. An overview of this improves the organisation's chances of optimising its own resource use, and makes it easier to evaluate if specific resources can be recalled or reallocated without weakening the collective emergency response.

- How the organisation intends to handle requests from others for emergency assistance, and what the procedure is in case the organisation itself has to ask for outside assistance.

- Which particular joint crisis management staffs, if any, the organisation must be able to participate in, who will function as liaison officers, and what their mandate will be.

Core task 4: Crisis communication

During a crisis, a massive and sudden pressure for information typically rises from the media, citizens, partner organisations and other stakeholders. A crisis therefore put demands on the organisation's communication which by far exceeds what it is used to in day-to-day operations.

It can be necessary to set up a dedicated crisis communication team, that can ensure a timely, reliable, and open crisis communication through the organisation's own and external channels. Such a team can also help lay the foundations for constructive relations with the news media.

The following conditions regarding the crisis communication team should be described in the organisation's general crisis management plan and related documents:

- Tasks – An instruction or action card outlining the team's various tasks, such as:
  - Updating the organisation's webpage with information on the crisis management.
  - Responding to inquiries from journalists, concerned citizens, etc.
  - Press releases and interviews for radio, TV and internet news media.
  - Direct warning of affected/threatened citizens via available media and technology.
  - Information in foreign languages for tourists, ethnic minorities, and foreign media.
  - Coordination of information to the public with external partners that are also involved in responding to the crisis in question.

- Management – The head of the crisis communication team (often the head of the normal communication unit) must be a member of the crisis management unit. Competences vis-à-vis the person leading the crisis management unit must be described clearly.

- Organisation – It should be clear if the individual members of the crisis communication team are expected to stay at their normal work stations, or if they should work directly from the crisis management room or an adjacent room.

- Staff – The crisis communication team will typically be a strengthened version of the normal communication unit, but the group of people and the allocation of roles will not necessarily be the same. In addition to the ''usual'' communication employees there can for example be a need for leaders and experts tasked with making live media statements.

- Resources – A resilient webpage that can manage many simultaneous visitors is one of the most important resources for updated crisis communication. More specialised means can be the setting up of a press centre or a call-centre with dedicated telephone lines and an advertised e-mail address for questions and answers. In this case the organisation needs instructions for activating and manning rooms and technical facilities, standard reply guides for operators that can be adapted to the particular crisis, etc.

- Procedures – Additional action cards, templates, etc. can lay down procedures for:
  - Activation of the crisis communication team (preferably before but otherwise immediately after the first meeting of crisis management unit).

- Establishment of systematic media monitoring and media analysis – partly to contribute to the combined situation picture, partly as basis for press strategies and to ensure that any errors in the media's coverage of the organisation are corrected.
- Agendas for internal meetings in the crisis communication team.
- Involvement of the crisis communication team in the crisis management unit meetings. Press strategy and media coverage should be a fixed item on the agenda.
- Permanent contact person for journalists with a fixed telephone number during the crisis (press duty officer).
- Contact details for persons in charge of communication at partner organisations.
- Prepared drafts for press releases, fact sheets with background information, etc.
- Distribution lists for press releases and communication briefings (email).
- Instructions regarding who can speak to the media on behalf of the organisation (spokesman hierarchy), specifying who in the organisation journalists may quote directly, and who are only allowed to provide background information to the media.
- Procedure that, if necessary, dictates a centralisation of all crisis communication to ensure, that the organisation speaks with one voice only.

Core task 5: Operational response

In view of the many and very different organisations in this guide's target group, the phrase ''operational response'' must be interpreted as covering a very wide spectrum of emergency activities. In most circumstances, however, operational response is either about deploying personnel and equipment in the field or performing tactical/operational crisis management, as opposed to the more ''strategic'' aspects of crisis management inherent in core tasks 1 - 4.

When the organisation activates its general crisis management plan, the first four core tasks will usually be relatively similar, regardless of the specific type of incident that has occurred. The operational response, on the other hand, will be different from one incident to another.

To avoid an unnecessarily long general crisis management plan, we recommend that only the most universal principles for operational response are described directly in the plan.

Detailed planning for operational response should instead appear in customized contingency plans for different incidents. Each contingency plan should deal with the central aspects of a specific operational response, including:

Examples of operational responses:

- Visits to elderly or otherwise vulnerable people by municipal care personnel in the event of extreme weather, power cuts, etc.
- Provision of clean drinking water after contamination accidents.
- Control centres' diversion of mass traffic after serious accidents.
- Resumption of the electricity grid following serious disruptions.
- Re-establishment of compromised IT systems and networks.
- Psychological first aid following serious accidents, violent episodes, or neglect in schools, day care centres, rest homes, etc.
- Putting down animals during outbreaks of veterinary diseases.
- Containing and cleaning out hazardous substances as a result of environmental pollution.

- Tasks – Which primary and secondary tasks must be tackled as a part of the response?

- Management – Who is in charge of the operational response and with which mandate?

- Organisation – Which units should be involved in the operational response, and how might the existing organisation be adapted in order to perform a satisfactory response?

- Personnel and equipment – How much personnel and equipment is needed for the operational response, where and when should it be deployed, and who should do what?

- Procedures – How should the tasks be carried out concretely, and how should they be coordinated with other organisations' operational responses?

The contingency plans can be attached to the general crisis management plan as appendixes. Alternatively – if there are many contingency plans – they can be stored separately and referred to in index form within the general crisis management plan.

Danish Emergency Management Agency
Datavej 16
DK-3460 Birkerød

www.brs.dk