

Guide to Risk and vulnerability analyses

Organisation

Guide to Risk and vulnerability analyses

Guide to risk and vulnerability analyses

Swedish Civil Contingencies Agency (MSB)

Editors: Jonas Eriksson, Anna-Karin Juhl.

Layout: Advant Produktionsbyrå AB Printing: DanagårdLiTHO

Publ.nr MSB366 - March 2012 ISBN 978-91-7383-208-3

Content

Foreword	7				
Introduction					
About this guide	10				
Outline	11				
Preventative and preparatory					
safety measures	13				
A comprehensive view in safety work	13				
The purpose of risk and vulnerability analyses	17				
Risk and vulnerability analyses and confidentiality	22				
Roles and areas of responsibility	25				
Government authority	25				
Risk and vulnerability analyses	26				
The county administrative board	27				
The county administrative board's geographic					
area responsibilities					
Risk and vulnerability analyses					
Municipality					
The municipality's geographical area responsibilities					
Risk and vulnerability analysis					
The county council					
Risk and vulnerability analysis					
Risk and vulnerability analyses					
What should a risk and vulnerability analysis contain?					
Working on risk and vulnerability analyses					
Risk and vulnerability analysis work as a process					
Support from the management Involvement					
Starting point					
Starting points					
The parts of the risk and vulnerability analysis					
Risk identification					
Risk analysis					
Probability assessment					
Consequence assessment					
Risk assessment	52				

Capacity assessment	56
Vulnerability analysis	56
Working with scenarios	57
Methods and tools	63
Seminar-based scenario methods	
MVA – multidimensional activity analysis	64
ROSA – Risk and vulnerability analysis	65
IBERO – instrument for preparedness evaluation of area responsibility	67
Traditional risk analysis methods	68
Broad analysis	69
'What if' analysis	71
Fault tree analysis	72
Other traditional methods	73
Other methods, models, and tools	73
Dependency analysis	73
Tools connected to risk management	76
References and further reading	78
Appendix - Terms and concepts	79
Picture listing	

Foreword

The development of society is characterised by such things as demographic and socio-economic changes, rapid technological development, specialisation, and globalisation. These trends together can lead to previously unknown risks appearing, but also new opportunities for increased safety and security presenting themselves. At the same time, this increased complexity makes it more difficult to get a picture of the threats, risks, and vulnerabilities found in our society.

Our knowledge of society's vulnerabilities and the threats and risks we are faced with affects the focus on crisis preparedness work, chiefly how practice and training is designed but also how means are used to strengthen our capacity and reduce vulnerability in society. We obtain this knowledge through things like risk and vulnerability analyses. Risk and vulnerability analyses, however, cannot be conducted independently of other work with crisis management and safety.

The analyses should be used as an initial step in a series that aims at reducing risks, decreasing vulnerabilities in society, and improving our ability to prevent, counteract, and manage crises and extraordinary incidents. It is our hope that this guide will contribute to this work.

Cecilia Nyström Head of Department, MSB



chapter 1 Introduction

Threats to our safety and the means for strengthening that safety are more complex and multidimensional than ever before. Strengthening safety in society requires that what is to be protected, what poses a threat, and the means for strengthening safety are seen in the same context. In the Defence Drafting Forum's (Försvarsberedningen) report 'A Strategy for Sweden's Safety' (Ds 2006:1) – and in this guide – emphasis lies on the safety of society.

This deals with incidents and circumstances that could damage vital societal functions and that particular individuals lack the qualifications to fully handle. According to the government letter, the general goals for the safety of society to protect are:

- the population's lives and health
- societal functionality
- the ability to maintain our basic values like democracy, the rule of law, and human rights and freedoms.

The democratic constitutional state, as well as health and medical care, information and communications systems, energy supply, the flow of goods and services, and other societal functions, are preconditions for a functioning society and cannot be allowed to break down.

Based on the general goals for society's safety, the government has also specified the goals for society's crisis preparedness. The government letter 'Society's crisis preparedness: Strong collaboration for increased safety' (Skr. 2009/10:124) states that the goal of society's crisis preparedness is to:

- reduce the risk and consequences of serious disruptions, crises, and accidents
- assure the health and personal safety of children, women, and men
- prevent or limit damages to property or environment.

In order to be able to work towards the general goals of safety strategy and the goals for society's crisis preparedness, it is important to try to create a picture of the threats, risks, and vulnerabilities that exist in our society. An important starting point is the work on risk and vulnerability analyses. In the government's budget bill, Prop. 2010/11:1, expenditure area 6, it states that the risk and vulnerability analyses are an important basis for the agencies' ordinary work on budget and operations planning, as well as for appropriation of funds from allocation 2:4, Crisis Preparedness. The opinion of the government is further that the risk and vulnerability analyses, along with capacity assessments from agencies, municipalities, and county councils are the most important basis for assessing society's crisis preparedness. The analyses are therefore important tools for efficient direction of society's crisis preparedness.

About this guide

State agencies must conduct a risk and vulnerability analysis according to the Emergency Preparedness Ordinance (SFS 2006:942). Municipalities and county councils have the same obligation according to the Act on Municipal and County Council Measures prior to and in the event of Extraordinary Incidents and during High Alert (SFS 2006:544). This guide is support for government authorities, county administrative boards, municipalities, and county councils in their work on risk and vulnerability analyses, and provides suggestions on how the analytical process can be managed. It is addressed primarily to those who are working with risk and vulnerability analyses, but could also be useful in a training context, and for those otherwise interested in the subject. With this guide, the Swedish Civil Contingencies Agency (MSB) contributes to strengthening society's crisis preparedness and supporting the actors who, according to legislation, are obligated to conduct risk and vulnerability analyses. The guide is neither authoritative nor regulatory, but should only be seen as support and a guide in the work. It replaces the earlier guides issued by the Swedish Emergency Management Agency (KBM). Lucram, at Lund University, has provided valuable contributions to this guide.

Outline

- Chapter 1 describes the general goals of society's crisis preparedness, and the role of the risk and vulnerability analyses in directing society's crisis preparedness. The chapter also describes the purpose of the guide and its intended target groups.
- **Chapter 2** deals with preventative work and describes the part of risk and vulnerability analyses in risk management, as well as broad preventative and preparatory safety measures. The chapter also contains a section on socially necessary work and issues of confidentiality.
- **Chapter 3** discusses the roles of the actors and division of responsibility in the work on risk and vulnerability analyses.
- **Chapter 4** describes the basic parts of a risk and vulnerability analysis.
- **Chapter 5** presents different methods and tools that can be used to conduct risk and vulnerability analyses. It should be pointed out that there is more, but MSB has selected the most frequent methods.

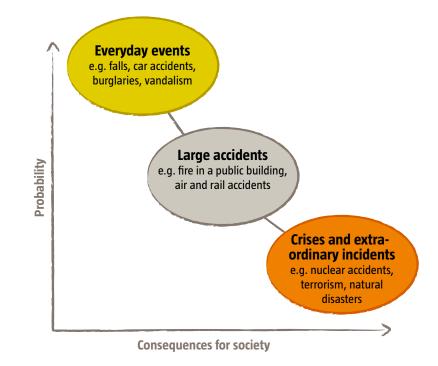


CHAPTER 2 Preventative and preparatory safety measures

The goal of preventative work is to minimise the number of accidents and crises, and their effects, through the actors concerned taking preventative measures designed to reduce vulnerability. It is therefore important to set the work on risk and vulnerability analyses in a context so as to obtain as effective a safety measure as possible.

A comprehensive view in safety work

Government authorities, county administrative boards, municipalities, and county councils manage safety work from different perspectives. All of them are unique based on the role and area of responsibility they have, as well as the environment they work in. The emphasis in safety work thus takes on different characteristics. There is, however, good reason to take a comprehensive view concerning safety work, since for reasons of efficiency it should be integrated with the organisation's other processes. The analyses, plans, and other work carried out in the field of safety should have clear connections with each other. Duplication of effort is avoided through such an approach, and resources are used efficiently, at the same time as the organisation's basis for decisions in risk management is improved. Moreover, there is no risk of important areas in safety work falling away, or of incorrect emphasis in the safety work. Smaller common accidents and their management can, for example, also form the basis for management of extraordinary incidents and more serious crises. The main source of information is mainly composed of mishaps and disruptions in daily operations, at the same time as it is difficult to get relevant information that could provide a basis for assessment of the most serious crises. Everyday events focus on relatively frequent accidents and incidents with limited consequences, for example workplace accidents and traffic accidents. These risks are, to a large extent, predictable and proceed from such things as reported accidents and statistical studies.



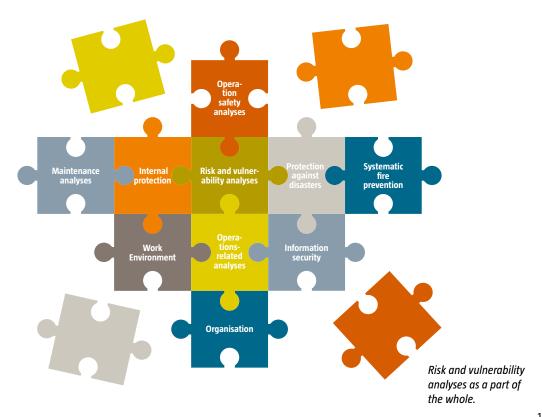
The risk scale.

Large accidents focus on accidents that occur infrequently, with moderate consequences. The risks are random and vary greatly. The benchmark lies in things like individual accident investigations and claims adjustments.

Crises and extraordinary incidents focus on events that occur rarely, with devastating consequences. Detailed risk analyses, especially qualitative risk analyses, are required in order to carry out analysis work. This occurs through estimation of the probability of a full-scale incident.

The actors must also take a position on various pieces of legislation that contain requirements for risk analyses. They are often connected to particular types of accidents, crises, risks, and threats. The pieces of legislation certainly have somewhat different starting points, but it is often the same risks and threats that must be analysed, and the consequences of the incidents are the same. There is, therefore, reason to coordinate the analysis work as much as possible based on several different pieces of legislation. The analysis work thus coordinated is adapted to individual needs and other conditions. In the preliminary work on risk and vulnerability analyses, it is therefore important to establish and define the starting points of the analysis. An important question is to determine which perspective the analysis is to have, and which legislation is thereby appropriate to work with in the risk and vulnerability analysis.

Apart from the risk analyses that follow from legislation, safety work that is not regulated in the statutes is also conducted. This concerns, for example, internal protection and municipalities' work on information security. It could be a good idea, for the purpose of adopting a holistic approach, to also coordinate this type of safety work with the work on risk and vulnerability analyses. The large gain in efficiency is found chiefly in the risk identification phase (see Chapter 4), since risk analyses can be coordinated based on various pieces of legislation and risk perspectives.

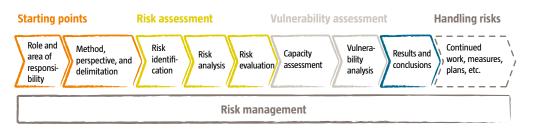


The points below show a few examples of statutes that can be coordinated with the risk and vulnerability analyses carried out in accordance with the Emergency Preparedness Ordinance (SFS 2006:942) and the Act on Municipal and County Council Measures prior to and in the event of Extraordinary Incidents and during High Alert (2006:544):

- Government Authority Risk Management Ordinance (SFS 1995:1300).
- Internal Governance and Control Ordinance (SFS 2007:603).
- Security Protection Act (SFS 1996:627) and Security Protection Ordinance (1996:633).
- Civil Protection Act (2003:778) and Civil Protection Ordinance (2003:789).
- Swedish National Board of Health and Welfare regulations and general guidelines on disaster medicine preparedness.
- Agency regulations in the field of information security.

Risk and vulnerability analyses and risk management

Even if this guide primarily concerns risk and vulnerability analyses, it could be good to describe the entire risk management process, where the risk and vulnerability analyses comprise an important part. The totality, or risk management process, comprises the entire chain from the choice of benchmarks through risk assessment and vulnerability



The risk management process.

assessment, to handling risks. Risk management should always take place in a structured, systematic process, for the purpose of being a continual part of the operations. It's important to have an understanding of the entire risk management process before the work on the risk and vulnerability analysis begins, since the goal of the analyses is determined by the desired result. Knowing from the beginning what the analysis will lead to determines the focus of the work and the choice of method.

The figure shows a general picture of the various parts of the risk management process. The various sub-processes never proceed separately, but are instead dependent on each other and run in parallel. There is also a standard (SS-ISO 31000:2009) that describes principles and guidelines for the risk management process. The choice of benchmark, as well as the risk and vulnerability assessment, are described more thoroughly in Chapter 4. The part of handling risks in the process, on the other hand, is not dealt with, even if it is a very important part. The results and conclusions of the risk and vulnerability analysis should, however, describe overall how the continued work with handling risks is to take place, for example which measures should be implemented, division of responsibility, the need for continued analyses, and what plans the analysis forms the foundation of. Continuity plans, plans for crisis management and action programmes according to the Civil Protection Act are examples of plans that could have a risk and vulnerability analysis as a starting point.

The purpose of risk and vulnerability analyses

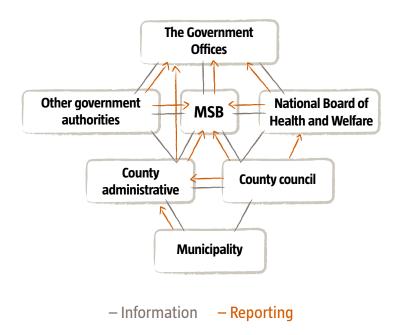
The purpose of risk and vulnerability analysis work is to increase awareness and knowledge for decision makers and those in charge of operations of threats, risks, and vulnerabilities within their own areas of operations, as well as creating a basis for their own planning. The basis, moreover, constitutes an important source of information for citizens and employees. The public actors' risk and vulnerability analyses also contribute to providing a picture of the risks and vulnerabilities that exist in society in general. Thus there are two perspectives that the risk and vulnerability analyses must accommodate: on the one hand for their own organisation or operation, and on the other to meet the need for providing a collective risk profile for all of society. The analyses thereby provide a proper basis for decisions on the objective of the work within the field of crisis preparedness and are used for things like the aim of practices, training, and appropriation of funds. The risk and vulnerability analyses thereby contribute to reducing society's vulnerability and increasing the ability to manage crises and extraordinary incidents.

Risk and vulnerability analyses provide important knowledge of how we prevent, prepare for, and manage crises. In summary, the purpose of risk and vulnerability analyses is the following:

- provide a basis for decisions to decision makers and those in charge of operations;
- provide the public with an informational basis of society's risks;
- provide basic data for community planning; and
- contribute to providing a risk profile for all of society.

A risk and vulnerability analysis can achieve these goals by being designed as support for a process or decision. In process support, focus lies on how the risk and vulnerability process is managed within an organisation. The process can, for example, be designed so that vulnerability in society decreases. As a suggestion, as many people as possible are involved in the organisation so that several are encouraged to start working with risks and vulnerabilities in their own operations. When focus lies on providing decision support, it is instead the result from the risk and vulnerability analysis work that is of interest. Usually this deals with placing demands on the design of the document where the analysis is presented. The document must be a basis for decisions for their own organisation and others in the work on reducing vulnerability in society and increasing the ability to manage crises. In order to achieve the four purposes described above, the risk and vulnerability analysis work should mainly be regarded from a decision support perspective.

The figure on the next page illustrates a comprehensive view, where all the actors together contribute to society's



Information exchange and reporting of risk and vulnerability analyses. It is important to note that the figure does not claim to show the subordinate relationships of the agencies, or their place in a hierarchical structure.

collective ability to identify, analyse, and evaluate risks and vulnerabilities. In connection with conducting risk and vulnerability analyses, the exchange of information should occur in two directions, where the individual organisation both contributes and gathers information and basic data.

One idea with the comprehensive view is that the various actors can accomplish together more than what would result if each of them conduct their own analyses in isolation. For example, it becomes much easier for a county administrative board to conduct their regional analysis if they use the analyses from the municipalities. If this opportunity disappears or becomes more difficult owing to the municipal analyses being designed in several different ways, the work of the county administrative board becomes more difficult. Designing uniform risk and vulnerability analyses also increases the opportunity to create overall pictures of risks and vulnerabilities at different levels, for example at the national and regional level.

Societal functions from a crisis preparedness perspective

Since no one knows in advance where, when, or how serious incidents occur, vital societal functions should always be

prepared for them and be able to handle them. When they occur, society must activate the functions at different levels that are particularly important in avoiding a crisis. These functions must also have the capacity to restore societal functionality, thereby contributing to society's ability to manage the incident or crisis.

Certain activities are especially significant for the lives and health of the population, societal functionality, and basic values. They are therefore necessary, or highly essential, for society's ability to prevent, withstand, and manage serious incidents and crises. Every such socially necessary activity should therefore be so robust, and maintain such continuity, that it can always continue, at least at a minimum level (basic security level, or GSN) regardless of incidents or the state of society.

Basic security levels in socially necessary functions and activities are the lowest level of functionality, capacity, or security that should prevail, regardless of incident or hardship in society. The government has stressed the significance of continuing the work on developing, and if possible establishing, basic security levels for societal functions. These levels can be established, for example, in the form of agreements, action programmes, plans, standards, agreements, or legislation.

Which activities are especially concerned in an extraordinary incident depends on the incident in question or how it develops. Prior to and during a pandemic, for example, health and medical care are particularly important activities, while an IT attack against financial systems means that other vital societal functions and activities can be affected by serious disruptions.

The activities that are not subject to hardship in an extraordinary incident are, despite this, no less socially necessary. They could instead by affected by the next incident. This approach means that society plans for, and can maintain, a broad preparedness and ability to withstand various types of extraordinary incidents that otherwise could lead to a crisis.

Apart from societal functions, there may be important material and personal reinforcement resources that are not socially necessary in and of themselves, but which are important for being able to manage an extraordinary incident or crisis – for example expert functions, volunteer resources, protective aprons, and so on.

Examples of prioritising societal functions and users of electricity according to Styrel

MSB was tasked in a 2010 government letter with producing a policy document for electricity prioritisation. The work was a part of Styrel's planning and was managed in cooperation with the Swedish Energy Agency. The policy document provides a basis and guidance for assessing in which order of priority the limitation or discontinuance of the transmission of electricity to users must take place in a planned or sudden short-term power outage. The starting point was the general goals for Sweden's safety, to protect the population's lives and health, to protect societal functionality, and to protect our ability to maintain our basic values like democracy, the rule of law, and human rights and freedoms.

Proposal for the order of priority for limitation or discontinuance of the transmission of electricity as part of Styrel's planning.

Priority Class	Prioritisation Criterion	Comments	Example of activity
1	Lives and health of the population	Electricity users that even in the short term (hours) are of great significance for lives and health	Emergency medical care, emergency services, care for vulnerable groups
2	Societal functionality	Electricity users that even in the short term (hours) are of great significance for lives and health	Leadership functions, fuel supplies, water and sewage, certain financial systems, radio/TV, electronic communications, certain transports
3	Lives and health of the population	Electricity users who over the long term (days) are of great significance for lives and health	Primary care, daytime clinics, medical supplies
4	Lives and health of the population	Electricity users who over the long term (days) are of great significance for lives and health	Primary care, daytime clinics, medical supplies
5	Great economic values	Electricity users who represent great economic value	Paper and pulp industries; mines; refineries; iron, steel and large engineering industries
6	Great ecological values	Electricity users who are of great significance for the environment	Trash removal, chemical industries
7	Great social and cultural values	Electricity users who are of great significance for social and cultural values	Archives, museums, objects on UNESCO's World Heritage List
8	Other	Other electricity users; not identified at the object level	Residences, small to medium businesses

Risk and vulnerability analyses and confidentiality

Freedom of information is one of the cornerstones of a democratic society. This means that the activities of public actors must be as open as possible. To guarantee observation of all public activity, the principle of document publicity has been written into the Freedom of the Press Act, one of our fundamental laws. This gives each and every one of us the right to demand to be allowed to study the contents of public documents, usually without needing to explain why or showing identity. In special cases, however, there may be reason to limit public viewing of certain public documents. In Chapter 18, §13 of the Official Secrets Act (OSL) there is the possibility of protecting information in established risk and vulnerability analyses. Information that concerns an agency's activity and which consists of risk and vulnerability analyses regarding peacetime crisis situation, planning and preparations before such situations, or management of such situations are covered by confidentiality. The risk and vulnerability analyses aim at reducing society's vulnerability through such things as the capacity of agencies to anticipate and manage peacetime crisis situations. So that the information is not exploited for an attack against agencies, individuals, or society as a whole, it is necessary to limit public observation of this activity to some extent. Confidentiality applies only if it can be assumed that the public's opportunities to prevent or manage peacetime crises could be thwarted if the information is revealed.

'Crisis' means an incident that affects numerous people and large parts of our society, and which threatens basic functions and values such as our health, freedom, or electricity supply. Since confidentiality applies to information linked to the risk and vulnerability analyses, it follows with information that is submitted to another agency. The confidentiality regulations thus also apply in the receiving agency. Note, however, that each agency independently reviews a request for consignment and takes a position on whether there is any information that must be kept secret. A municipality can therefore submit its risk and vulnerability analysis, for example to the county administrative board, without the danger of sensitive information reaching the public. Nor does confidentiality hinder the information from being submitted to the government or to Parliament. Other confidentiality regulations may be applicable to information in risk and vulnerability analyses, for example Chap. 15, §2, and Chap. 18, §§ 8-9 of the Official Secrets Act.

There may, however, be a conflict of interest between limiting public viewing of risk and vulnerability analyses and meeting the purpose of the analysis work – that is, increasing awareness in decision makers and providing the public with a source of information on society's risks. This is a consideration that every organisation should take a position on.

The interest in preventing certain information from being revealed is sometimes regarded as having more weight than the interest in public observation of public functions. Professional secrecy that follows from Chap. 18, §13 of the OSL therefore has precedence over the freedom to disseminate information as enacted in the Freedom of the Press Act and the basic freedom of speech laws. The freedom to disseminate information implies a right to submit information for publication in the media, a prohibition against the public trying to find out who submitted the information to the media, and protection of sources, which means journalists do not need to reveal their sources. Confidentiality regulations having precedence over the freedom to disseminate information in certain cases means that a person who submits such information to the media violates professional secrecy, that the public may try to find out who submitted the information, and that journalists can be compelled to reveal their sources.



CHAPTER 3 Roles and areas of responsibility

Government authority

Each agency has a fixed area of responsibility and is responsible for an activity that is chiefly established through various legislative frameworks. The agencies' activities within the area of emergency preparedness is primarily regulated in the Emergency Preparedness Ordinance (SFS 2006:942), and often as part of the government's instructions to the authority.

Regarding crisis preparedness and risk and vulnerability analyses, the agencies' areas of responsibility can somewhat simply be divided into two parts: on the one hand, their own activities; on the other, the sections of society or the sector within which they have particular responsibility.

The agency's own activity can consist of managing or commanding a socially necessary activity, resource, or function, for example operation and management of infrastructure or facilities, and storage and distribution of materials. Certain agencies also have an extended responsibility within a particular section of society that is defined in instructions and other policy documents. The responsibility often means the exercise of authority as a right to issue injunctions and supervise, but it can also imply control, approval, inspection, authorisation, and other direction. Certain agencies are specially designated and have a particular responsibility to promote a comprehensive view within



Areas of government authority responsibility. certain particular areas, according to the Emergency Preparedness Ordinance (2006:942). These agencies are divided up into six areas of collaboration:

- technical infrastructure
- transport
- hazardous substances
- economic security
- geographic area responsibilities
- protection, rescue, and care.

The agencies represented here contribute their unique skills so as to reduce vulnerability and improve the capacity for crisis management within their respective areas.

Risk and vulnerability analyses

To strengthen their own and society's emergency preparedness, every agency must, according to §9 of the Emergency Preparedness Ordinance (SFS 2006:942), annually analyse whether there are such vulnerabilities or such threats and risks within the agency's area of responsibility as can quite seriously impair the capacity for activity in the area.

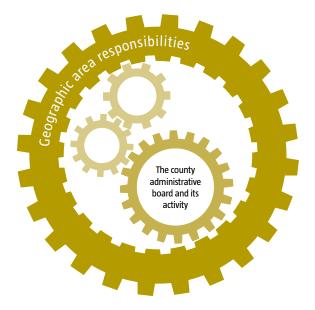
During this analysis the agency must especially note

- situations that arise quickly, unexpectedly, and without warning, or where there is the threat or risk that such a situation could arise
- situations that require urgent decisions and collaboration with other actors
- that the most necessary functions in societal functions can be maintained
- the ability to manage extremely serious situations within the agency's area of responsibility.

State agencies must evaluate and compile the results in a risk and vulnerability analysis. The agencies with particular responsibility according to the Emergency Preparedness Ordinance (2006:942) and the agencies that MSB decides on, must submit a report based on the analysis to the Government Offices and to MSB. More detailed regulations can be found in MSB's rules on risk and vulnerability analyses from state agencies (MSBFS 2010:7). A government authority must also, above all, take into consideration the needs of the county administrative boards for obtaining a suitable basis for regional risk and vulnerability analyses. The latter can, moreover, form a basis for the risk and vulnerability analyses of the government authorities.

The county administrative board

The activities of the county administrative board within the area of emergency preparedness are primarily regulated in the county administrative board instruction by-laws (2007:825) and the Emergency Preparedness Ordinance (SFS 2006:942). As with other state agencies, the area of responsibility for the county administrative board concerning risk and vulnerability analyses can be divided into two parts: its own activities and the geographic area responsibility. The absolute emphasis lies in the geographic area responsibility.



The county administrative board's areas of responsibility

The county administrative board's geographic area responsibilities

Geographical area responsibilities are found on the local, regional, and national level. At the local level it is used by the municipality, at the regional level by the county administrative board, and at the national level by the government.

A geographic area responsibility means that there is a body responsible for focus, prioritisation, and coordination of cross-sector crisis management measures within a geographic area. Responsibility for coordination means that the county administrative board must initiate and facilitate the collaboration needed so that the resources of the actors concerned can be properly used during crisis management. This responsibility exists during planning and preparation work as well. Responsibility for coordination, however, does not mean that the county administrative board takes over the ordinary responsibilities of the other actors. There are exceptions to the rule; for example the possibility of the county administrative board taking over responsibility for comprehensive rescue efforts that affect several municipalities. This is regulated in the Civil Protection Act (SFS 2003:778).

Risk and vulnerability analyses

In accordance with §9 of the Emergency Preparedness Ordinance (SFS 2006:942), the county administrative board must analyse whether there is such vulnerability or such threats or risks within the agency's area of responsibility as can quite seriously impair activities in the area. This means that the county administrative board is responsible for compiling regional risk and vulnerability analyses which are based on things like the risk and vulnerability analyses from the county councils and the municipalities. The county administrative board thereby takes on an important unifying and supporting role in the work on risk and vulnerability analyses within the geographical area, especially concerning support for the analysis work of the municipalities and the county council. The county administrative board should also provide a briefing and communicate the county's risks and vulnerabilities. For the purpose of reducing the county's

Coordination and collaboration in the county

A county administrative board conducts a regional risk and vulnerability analysis in cooperation with the municipalities, the county council, government authorities, and private actors in the county. Selected scenarios that could strike the county are studied in common. All municipalities and the county council report their overall county risk and vulnerability analysis to the county administrative board, and since the entire county is working with the same scenarios, the municipal risk and vulnerability analyses form the basis for the overall regional analysis.

vulnerabilities, the county administrative board must also see to it that risk and preparedness considerations are made in community planning.

The county administrative board must, in accordance with the county administrative board instruction by-laws (2007:825), also follow up on the municipalities' application of the Act on Municipal and County Council Measures prior to and in the event of Extraordinary Incidents and during High Alert (SFS 2006:544). This includes the municipalities' work on risk and vulnerability analyses.

The important unifying function of the county administrative board within its geographic area means that it should take an active, supporting role in the work of the municipalities and county councils on risk and vulnerability analyses. The county administrative board should also, to the greatest extent possible, obtain a suitable basis for analysis work from the actors that municipalities and county councils normally do not have access to, for example government authorities and businesses. Apart from obtaining a basis from municipalities and county councils, the county administrative board must also assist with suitable basic data on the risks in the region. More detailed regulations can be found in MSB's rules on risk and vulnerability analyses from state agencies (MSBFS 2010:7).

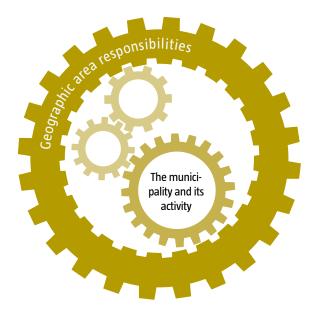
Example

From the county administrative board instruction by-laws (SFS 2007:825)

\$54 Regarding emergency preparedness, the county administrative board must be a unifying factor within its geographical area and before, during and after a crisis work for coordination and common focus of the measures that must be taken.

The county administrative board must, in particular:

- 1. be responsible for compiling a collective regional overview in crisis situations
- 2. support the actors responsible for emergency preparedness in the county as regards planning and risk and vulnerability analyses, as well as instruction and training
- 3. have a regional council for accident protection and emergency preparedness, in which representatives from the county administrative board and actors concerned should be included, so as to create the necessary collaboration
- 4. establish regional risk and vulnerability analyses that can be used as a basis for their own emergency preparedness measures, as well as those of other actors concerned
- follow up on the municipalities' application of the Act on Municipal and County Council Measures prior to and in the event of Extraordinary Incidents and during High Alert (SFS 2006:544)
- report annually to the Swedish Civil Contingencies Agency on what preparedness preparations the municipalities and county councils have taken, at the same time reporting an assessment of the effects of the preparations taken, and
- working to make it so the activities regarding emergency preparedness pursued in the county by actors concerned contribute to achieving a basic capacity for civil defence. Ordinance (2008:1346)ning (2008:1346).



The municipality's areas of responsibility.

Municipality

Responsibility for activities and the responsibility principle are the starting point for the tasks of the municipality in society's crisis management system. This means that the responsibility for various socially necessary tasks under normal circumstances also applies during extraordinary incidents. The municipality must be able to maintain societal functions, regardless of the scope and character of the situation, and meet the special needs for information and support for individuals that arise in connection with a crisis. To manage responsibility for activities, the municipality must have a crisis management organisation, plans, and prepared locations, among other things. The responsibility also includes continuously instructing and training the crisis management organisation.

The municipality's geographical area responsibilities

The municipality's geographical area responsibilities are regulated in Chap. 2, §7 of the Act on Municipal and County Council Measures prior to and in the event of Extraordinary Incidents and during High Alert (SFS 2006:544).

In accordance with the Act on Municipal and County Council Measures prior to and in the event of Extraordinary Incidents and during High Alert, the municipality must analyse which extraordinary incidents could happen in the municipality in peacetime, and how these can affect their own activities. MSB rules state that the municipality must identify and evaluate risks, vulnerabilities, and critical dependencies within its geographical area. This gives the municipality the background to work towards:

- different actors in the municipality collaborating and achieving coordination in planning and preparation work;
- coordinating the crisis measures taken by different actors during such an incident; and
- coordinating information for the public under such circumstances.

In preventive and preparatory work, the municipality should include important actors outside their own organisation. Examples of such actors are other municipalities, the county administrative board, the county council, food and fuel dealers, electricity and telecommunications companies, the transport industry, the rest of the business world, volunteer organisations, and so on.

Often, however, there is a reason to collaborate around common issues, and the geographical area responsibility in this case means that the municipality must take the initiative for such collaboration. It can be a question of activities, objects, systems, or environments that are important to maintain from a municipal perspective. It can also concern an extraordinary incident that requires the municipality and other actors to act in common.

Risk and vulnerability analysis

The 2004 document between the state and the Swedish Association of Local Authorities and Regions, known as the Municipal Agreement, states that the municipalities must conduct risk and vulnerability analyses. An agreement was also signed with the county councils later on. The main parts of the agreements were subsequently laid down in the Act on Municipal and County Council Measures prior to and in the event of Extraordinary Incidents and during High Alert. In accordance with the Act on Municipal and County Council Measures prior to and in the event of Extraordinary Incidents and during High Alert, the municipality must prevent and prepare itself for extraordinary incidents through work on reducing risks and vulnerabilities. According to the responsibility principle, the municipality – as previously mentioned – has the same responsibilities under normal circumstances as during extraordinary incidents. It is important that the municipality's crisis management preparations take place in the context of the entire risk scale: accident – crisis – war. The starting point must be the ability to withstand serious disruptions in the vital societal functions that must always be maintained.

In accordance with Chapter 2, §1 of the Act on Municipal and County Council Measures prior to and in the event of Extraordinary Incidents and during High Alert, the municipality must establish a plan and an organisation for how extraordinary incidents are to be managed, based on the results of the risk and vulnerability analysis. The plan includes having prepared locations, as well as a trained and drilled crisis leadership organisation. The plan must be confirmed by the members of the municipal council for every new term of office. The risk and vulnerability analysis must be based on the geographical area and the prevailing risk profile.

The municipality's risk and vulnerability analysis is an important basis for the analyses at the county and national level, and contribute to a comprehensive picture of the risks and vulnerabilities found in society as a whole. The analyses must also encompass activities which are managed by a fully or partially municipally-owned business, and which could be affected by an extraordinary incident, just like any contractors the municipality has agreements with. More detailed regulations can be found in the MSB rules for municipal and county council risk and vulnerability analyses (MSBFS 2010:6).

From the Municipal Agreement:

The municipality must work towards coordinating the preparations for managing an extraordinary incident, which are carried out within the municipality's geographic area by state authorities, the county council, and organisations and businesses.

When an extraordinary incident occurs, the municipality must work towards coordinating crisis management within the municipality's geographic area. In summary, this geographic area responsibility means that the municipality must:

- conduct a collective analysis of such risks and such vulnerabilities in the municipality as can lead to an extraordinary incident and make this analysis known to actors concerned;
- 2. be a unifying factor for a crisis management council (or similar) with representatives of the local crisis actors;
- 3. work towards coordinating the local crisis actors' preparations for managing an extraordinary incident
- 4. work towards coordinating local crisis actors' measures during an extraordinary incident
- work towards coordinating information for the public during an extraordinary incident
- be able to submit collected information to the county administrative board on the situation in the municipality on the question of risks and vulnerability, and on the local crisis actors' preparations for managing an extraordinary incident; and
- 7. be able to provide the county administrative board with a collected report on the situation in the municipality during an extraordinary incident, and on measures taken and planned by the local crisis actors in connection with managing the incident.
- 8. All actors concerned do not have such representation in the municipality that they can contribute to coordination. This applies to such entities as state agencies and stateowned companies. In certain regards, coordination must therefore take place through the county administrative board.

The county council

The county council is responsible for tasks that are common to large geographical areas and which require great financial resources. The most important area of responsibility is medical services, including disease control, which represents approximately 80 percent of the costs. Other county council areas are public dental services, nursing education, culture, support of county businesses, and responsibility for regional development. A county council can either pursue activities under its own management, or under contractual agreement with another performer but with the responsibility retained. The responsibility for public transportation in a county can be shared among the municipalities and the county council, or rest entirely with the county council or the region.

According to the responsibility principle, the county council is responsible for its own area of operations even during serious extraordinary incidents. This means on the one hand that societal functions must be maintained regardless of the scope and character of the situation, and on the other that sufficient amounts of correct information on the incident and responsibility for the activities is provided to the public and the media.

Risk and vulnerability analysis

According to the Act on Municipal and County Council Measures prior to and in the event of Extraordinary Incidents and during High Alert, the responsibility means having crisis management planning and organisation, prepared locations, and a properly trained crisis management organisation. The plan must be based on a risk and vulnerability analysis of which extraordinary incidents could happen in the county council in peacetime, and how these can affect their own activities. The plan must be confirmed by the county council for every new term of office. Since the county council conducts operations in the county's municipalities, they are dependent on the municipalities' and county administrative board's risk profiles and analyses in the work on their own risk and vulnerability analysis. The county council's risk and vulnerability analysis is an important basis for the analyses at the county and national level, and contribute to a comprehensive picture of the risks and vulnerabilities found in society as a whole. The analyses must also encompass fully or partially county-owned businesses whose activities could be affected by an extraordinary incident, as well as any contractors the county council has agreements with. The basis for the circumstances outside the county council organisation that could entail an extraordinary incident and which could affect county council activities must primarily be gathered from the municipalities and county administrative board. According to the Health and Medical Service Act (SFS 1982:763), the county council must also plan on maintaining disaster medicine preparedness. This is also regulated in the rules and general guidelines of the Swedish National Board of Health and Welfare, on Peacetime Disaster Medicine Preparedness and Planning for Increased Preparedness (2005:13 M) which state that each county council must have a regional disaster medicine plan. The plan must cover chemical, biological, radiation, and nuclear incidents, as well as evacuation between care units. There must also be similar plans for the hospitals and primary care areas that are covered in the disaster medicine planning. The latter should be based on the risk and vulnerability analyses that follow on from the Act on Municipal and County Council Measures prior to and in the event of Extraordinary Incidents and during High Alert. More detailed regulations on municipal and county council risk and vulnerability analysed can be found in MSB 2010:6.



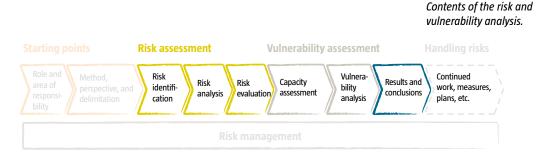
CHAPTER 4 Risk and vulnerability analyses

What should a risk and vulnerability analysis contain?

A risk and vulnerability analysis contains several different parts, and there are a number of different methods that facilitate the work. Regardless of which method is used, certain fundamental parts should be included in the final analysis. This is an issue of systematically identifying all undesirable incidents, assessing how likely it is that the incidents will occur, assessing the immediate negative consequences, analysing the vulnerability of the activity, and assessing the ability to handle different hardships.

How the information can be produced and presented in a risk and vulnerability analysis is described in more detail below. Before the work of designing the analysis is described, it is necessary to account for why the analysis should look this way. The starting point is the purpose of the risk and vulnerability analysis (see Chapter 2), which deals with reducing risks and vulnerabilities, as well as the analysis functioning as a basis for planning and being used for dissemination of information. Moreover, it they should contribute to providing a risk profile for the whole of society.

The work on risk and vulnerability analyses must be adapted to the current needs and conditions of the organisation. For example, both needs and conditions vary between large and small municipalities, as well as between municipalities, county councils, county administrative boards and government authorities. In one county there may be a



nuclear power plant that affects the risk and vulnerability analysis, while in another county there could be great risk for floods.

Another way of looking at what a risk and vulnerability analysis is and what it should contain is found in the report "Crisis management and civil defence in municipalities and county councils" (SOU 2004:134, p. 90). The text states that a risk and vulnerability analysis should contain answers to a number of questions. The three most important in this context are:

- What could happen?
- Why could it occur and how often?
- What are the consequences for society?

Working on risk and vulnerability analyses Risk and vulnerability analysis work as a process

It takes time to establish a functional process for risk and vulnerability analyses. The process could be described as going up an evolutionary staircase. The goal is to establish and maintain a culture of security in the organisation, and for the municipality and the county administrative board to get all the parties affected by area responsibilities in the work to come along.

It is important to have a process leader whose task is to work across management or operations boundaries, as well as to set aside the time required for the process.

Support from the management

It is worthwhile to ensure early on in the work that the result can be properly taken charge of, for example that the work is suitably supported and organised right from the start.

There should be a decision on the organisation as focus for the work. The decision should show what results the management expects, and which resources are available. In addition, it should be indicated when and how the results are to be reported, what the purpose is, and what the work must lead to.

Involvement

The work on risk and vulnerability analyses should be carried out so that it involves activities from different parts of the organisation. For this reason, many actors have established a risk management group with representatives from the entire operation. Members in the group function as 'ambassadors' of the work in the respective activities. The people selected to participate in the risk management group must be able to participate over longer periods. Continuity in the work is an important factor.

For example the municipality, as entity in charge of the geographic area, must set a goal of having the whole area responsibility (including for example businesses, the county council, the county administrative board, and government authorities) represented in the work.

Starting point

Some choose to start with an overall analysis with the help of a risk management group in order to then go further with the analyses in the activities. Others have already set up work in the activities that they expand to also include extraordinary or serious incidents for the activities. The next step is then to go further and conduct and overall analysis with the risk management group. There is great value in starting with an overall analysis and then introducing it into the work in the activities. Right from the start, it provides a picture of the problem areas that come up in joint discussions.



Benchmarks.

Starting points

Every risk and vulnerability analysis produced by different actors within the crisis management system must be seen as a part of something greater. The analyses should be designed in such a way that other actors can also make use of them. With this as a background, it becomes important to describe the benchmarks in the work and what delimitations have been made. This information is valuable and helps other actors see how the information in the current analysis fits in with their own analysis. Among other things, this deals with describing what role and area of responsibility the actor in question has, and what legislation has influenced the production of the analysis (see Chapter 2). The choice of method or methods, as well as the working method considered, should also be clarified in the starting points of the risk and vulnerability analysis.

An important starting point for the work is which perspective was used in the analysis. This deals primarily with which risk perspective the risk and vulnerability analysis will concern - that is, which risks and incidents the analysis will cover. The perspective can also cover the values the analysis builds on, especially what are regarded as negative consequences in the analysis work. In this context, values are used as principles to evaluate how serious a specific scenario is. The value of protecting the lives and health of the population means, for example, that a risk scenario where their lives and health are damaged is seen as worse than a scenario where property and the environment are damaged. Note, however, that regardless of which perspective – and thus which types of risks – are to be noted in the analysis, the chief starting point should be dealing with risks that can lead to an extraordinary incident or crisis arising.

Delimitations deal with clarifying the system within which the focus of the analysis lay. Note that the concept of 'system' does not necessarily relate to a technical system, but could be any type of system at all – a municipality, for example. A system should rather be interpreted as if there were a number of elements that hang together and form a totality. Delimitations may often be more or less obvious. It is, for example, common that a municipal risk and vulnerability analysis focuses on the municipality in question. For the sake of clarity, it is still important to describe the delimitations chosen. Moreover, there may be parts of the organisation that were not included in the risk and vulnerability analysis; it could then be good to emphasize this.

There is often a reason to come back to the starting points during the work on the risk and vulnerability analysis – for example, for further delimitation or to make changes in the working method or choice of methods.

In summary, the starting points of the risk and vulnerability analysis should make clear:

- roles and areas of responsibility
- methods and working methods
- delimitations
- perspectives.

The parts of the risk and vulnerability analysis

With a starting point in the proposed risk management model, this chapter describes the different elements in the risk and vulnerability analysis.

Risk identification

Risk identification deals more with scenario identification – that is, to try to find out what could happen. The reason is that it is difficult to identify sources of risk without thinking in terms of potential risk scenarios. In practice, this means identifying sources of risk, for example a tank with



Risk evaluation.

poisonous gas, and risk scenarios, for example a release of poisonous gas. In connection with identifying sources of risk, it is important to describe how the identification was carried out, and if it led to any delimitations. Thus it is not only the final result that is important – that is, which scenarios have been identified – but also how the results were produced. The reason the documentation is important is that the analysis may be used by others than those who took part and produced it, and that an analysis may need to be updated at a later time. The process used is therefore important, since it provides valuable information on how careful the scenario development was, and how relevant the scenarios are for the actors who want to use the results in their own analysis.

In identifying different sources of risk or risk scenarios, support can be found in many of the risk analysis methods available (see next chapter). Essentially, most methods deal with systematically starting from a description of the system. Descriptions of systems are often done with the help of two types of models: structural models and functional models. The structural models describe a structure, for example the different organisational parts of an agency. The functional models focus more on certain functions, for example the societal functions of an agency. The different models can be used by themselves or together, depending on what is suitable for the agency's own organisation. In a systematic review of, for example, an agency's organisation, it is good to gather information that could support the systematic security work, for example information on internal protection or information security, regardless of how the information is connected to the risk and vulnerability analyses. To avoid duplication of work and make the security work more efficient, there is reason to coordinate risk identification based on several pieces of legislation and other parts in the systematic security work. It is also good to gather the information needed to be able to conduct a vulnerability analysis, for example assessing the dependence or ability to handle a given incident.

By reviewing the different parts where the system is described, the identification process will be systematic. It may also be

Incident/circumstances

Can be inventoried based on: Geographic information systems Qualitative descriptions Statistics Mapping etc.Natural disastersStorm Flood Landslide and avalanche Forest fireAccidentsDangerous facilities Hazardous goods Fire CBRN Train accident Air accident		Can be inventoried regarding: Activity description Socially necessary activity Dependence Internal protection Security aspects Information security Fire prevention Identified risks Capacity assessment etc.			
		The municipalFinancesmanagementStaffofficeInformation			
		Technical management	Parks Road works Water and waste Trash removal		
Technical infrastructure and support systems	Water shortage Telephone outage Power outage District heating outage IT outage Fuel shortage	Education management	Schools Preschools		
Antagonistic threats and social unrest	Crime Terror Subversive activity	Nursing and care management	Elder housing Elder care		
Illnesses	Social unrest Hacking Pandemic	Municipal companies	Energy company Housing company		
111(23)23	Epidemic Influenza Epizootic	Emergency services	Preventive emrg svc Operational emrg svc Training		

Organisation/function

Example of municipal risk investment.

suitable to try to identify different incidents and circumstances outside the organisation that could damage the system. These can then be divided into different classes – for example accidents, natural disasters, technical infrastructure and support systems, antagonistic threats and social unrest, and illnesses. The results of risk identification are setting up sources of risk or roughly described risk scenarios. The information must then be further developed in the risk analysis. The figures on the next page show examples of how the inventory could look in a municipality, with a starting point in incidents or circumstances, and organisation.

The risk identification section of the risk and vulnerability analysis is important, especially for all municipalities and county administrative boards that have geographic area responsibilities. It can be advantageous to coordinate this identification at the municipal level with the work that forms the basis for the municipalities' action programmes in accordance with the Civil Protection Act (SFS 2003:778).

Risk analysis

A risk analysis is based on answering the three questions described earlier in the chapter: 'What could happen?' 'How likely is it?' and 'What are the consequences?' The answer to the first question has been partially answered in connection with risk identification. In the analysis phase it is a matter of refining the descriptions of the risk scenarios and assessing how probable it is that each of the scenarios identified will occur. After that, the consequences of the incidents are assessed, linked to the values that the analysis is built on. This step can also be advantageously coordinated on the municipal level with the work in accordance with the Civil Protection Act.

Probability assessment

There are several different ways of answering the question of how likely a specific risk scenario is. A common method is to use probabilities, or frequencies. But there are also other ways firmly linked to the risk analysis method used. A number of methods provide strong support for using probabilities and frequencies, while others use different scales for ranking how likely incidents are. The method for probability assessment chosen affects the use of the analysis results. Against the background of the individual analysis being used for planning and prioritising proposals for risk reduction measures, the methods for describing how likely an incident is to happen are divided into the following groups:

- a qualitative description of how likely the incident is;
- a qualitative description with the help of a ranking scale;
- a quantitative description with the help of a ranking scale and intervals; and
- a quantitative description with the help of frequencies.

A qualitative description of probability of the incident

The methods in the first group describe how likely a scenario is, which provides small opportunities for comparisons between different scenarios. Expressions like 'the incident is not likely' and 'the incident is very likely' that appear in the descriptions do not provide an opportunity to rank different scenarios with regard to how likely they are. For example, it is not possible to know which of two incidents are most likely based on the following descriptions: 'Incident A is likely' and 'incident B is possible'. The incidents cannot be ranked, since there is no established ranking between many words we used to describe something that is not certain. Moreover, the words have different meanings for people in different contexts. Since the analyses are intended to be a basis for decisions in a larger context, it cannot be expected that everyone has the same starting point for their assessments. This method of assessing the probability of different incidents is not optimal, considering the purpose of the risk and vulnerability analysis.

A qualitative description with the help of a ranking scale

A qualitative scale is used in the second group in order to rank different scenarios based on how likely they are in relation to each other. It is normal that this kind of scale contains five classes, for example 'very low probability', 'low probability', 'medium probability', 'high probability', and 'very high probability'. The difference compared with the first group is that the scale is used to assess all scenarios, which makes it so that different scenarios can be ranked based on how probable they are. The ranking, however, applies only to the scenarios that have been identified in the analysis in question. Scenarios from one analysis cannot be compared with scenarios from another analysis. In a comparison of a municipality's and a county council's risk and vulnerability analyses where both actors have used the same scale for assessment, the scenarios cannot be compared and ranked. The reason is that both actors most likely have different starting points for their assessments, which means that 'very probable', for example, means different things. This is also the reason why it would be difficult for another actor to use the information from an analysis that used this method to describe uncertainty.

A quantitative description with the help of a ranking scale and intervals

A scale with a limited number of classes, where each of the classes has a quantitative meaning, is used in the third group. Risk scenarios classed as 'low probability' are calculated as occurring, for example, 'between once every 100 years and once every 1000 years'. This method of expressing like-lihood has the same properties as Group 2 regarding the ranking of risk scenarios. Using quantitative estimates also provides other actors with much greater opportunities to relate the assessments to their own analyses. This type of scale also provides an opportunity to use the information as a rough basis for planning. A common division of a scale for indicating how often different scenarios are expected to occur is as follows: Yearly, every 10 years, every 50 years, every 100 years, and every 1000 years.

A quantitative description with the help of probabilities or frequencies

In the fourth group, likely risk scenarios are described with the help of probabilities or frequencies. The most common is the use of frequencies – that is, the expected number of incidents per year. Since the incidents of interest in a risk and vulnerability analysis do not occur particularly often, the estimated frequencies are often very small, for example 0.001 times per year or once per 1000 years. An actor using frequencies to assess how likely different risk scenarios are makes it possible for other actors to relate the information to their own analyses. Regardless of the method used, these estimations form assessments. It is in the nature of the project that the results can never be established with certainty as regards assessing the future. An analysis is not more 'safe' or 'true' because it contains numbers. It is important to always show what materials form the basis for different estimates in a risk and vulnerability analysis. Otherwise, other actors cannot determine how credible the assessments are and whether they were done in such a way that they fit into the context in question. The documentation can, for example, describe whether a specialist was used in the analysis, and what skills he or she has. A risk and vulnerability analysis is a basis for planning that should illuminate uncertainties, not hide them. A very useful way of expressing uncertainties in a frequency assessment is to describe it with the help of an interval. For example, it may say in the analysis that the most likely assessment of the frequency of a specific risk scenario is 0.001 times per year. The frequency can certainly be as low as 0.0005 and as high as 0.005 – that is, once every 200 to 2000 years.

Consequence assessment

Assessing what can happen and how likely it is constitutes an important basis for a risk assessment. Without information on what the consequences are judged to be if different scenarios occur, the analysis would be difficult to use as a basis for decision. In Chapter 4 the importance of describing which perspective is used in an analysis was discussed, which means among other things deciding how the consequences are to be described. The starting point for the consequence assessment should be the lives and health of the population, societal functionality, the basic values, and damage to property and environment. There is often reason to have several different descriptions of the consequences due to a specific scenario. For example, the consequences of the number of people who are expected to perish owing to a scenario may be described at the same time by indicating how much economic damage the scenario creates. As with the probability of a certain scenario, the different methods for describing the consequences are divided into four groups:

- a qualitative description of the consequences;
- a qualitative description with the help of a ranking scale;
- a quantitative description with the help of a ranking scale and intervals; and
- a quantitative description.

Level	Consequences	Description
1	Extremely limited	Small direct effects on health, extremely limited disruptions to societal functionality, transient mistrust towards individual social institutions, extremely limited damage to property and environment
2	Limited	Moderate direct effects on health, limited disruptions to societal functionality, transient mistrust towards several social institutions, limited damage to property and environment
3	Serious	Significant direct or moderate indirect effects on health, serious disruptions in societal functionality, continued mistrust towards several social institutions or changed behaviour, serious damage to property and environment
4	Extremely serious	Extremely large direct or significant indirect effects on health, extremely serious disruptions to societal functionality, continued distrust towards several social institutions and changed behaviour, extremely serious damage to property and environment
5	Catastrophic	Catastrophic direct or extremely large indirect effects on health, extreme disruptions in societal functionality, solid mistrust towards social institutions and general instability, catastrophic damage to property and environment

Consequences with the help of a qualitative ranking scale.

Qualitative description of consequences

The first group uses qualitative descriptions of consequences without evaluating whether one scenario is more serious than another, for example 'The consequences of the scenario would be very serious'. These types of descriptions are difficult to use as a basis for planning, since it may be difficult to compare different alternative measures. Qualitative description with the help of a ranking scale Describing consequences with the help of a qualitative ranking scale means establishing a scale that can be used to show how serious the different risk scenarios are in relation to each other. There could, for example, be a scale with five steps where the consequences of a scenario may be classed as 'catastrophic', 'very serious', 'serious', 'limited', and 'very limited'. The table below shows an example of this kind of scale, which also contains a more detailed description of the different levels.

The scale provides other actors the opportunity to show how the ranking between risk scenarios was done based on the consequences the scenarios could result in.

Quantitative description with the help of a ranking scale and intervals

Consequences can also be expressed so that it is easier for others to relate the assessment to their own analyses. This is done through detailed descriptions of what is needed so that the consequences of a scenario are described with the different classes, for example through giving the different classes a quantitative meaning. An example of quantitative description with the help of a ranking scale regarding lives and health. It has five steps: (1) 'No deaths', (2) '1-5 deaths', (3) '6 to 20 deaths', (4) '21 to 100 deaths', and (5) 'over 100 deaths'.

A quantitative description

The last group contains ways to describe the consequences quantitatively, for example as 'number of injured' or 'economic damage (MSEK)'. This way of expressing consequences can also contribute to the actor conducting the analysis being able to express uncertainty through estimating with the help of an interval. A broad interval indicates

Risk analysis					
Scenario	Frequency (per year)	Consequences			
Scenario 1	0,1	10 dead			
Scenario 2	0,01	50 dead			
Scenario 3	0,005	200 dead			

Illustration of the results from a quantitative risk analysis.

the estimate is very uncertain; for example 'the number of deaths owing to the scenario is estimated to be between 10 and 100 people'.

Regardless of which type of consequence description is used, the information that forms the basis for the assessment should be reported, just as applies to expressing the probability of something occurring. This makes it easier for other actors to use the information in their analyses. Regardless of which method is used to describe how probable different risk scenarios are, and what their consequences would be, the results can be presented in a table (see next page). The risk scenario is described in the first column; in the second is the probability that the risk scenario occurs, and in the last column are the estimated consequences if the scenario occurs. Each row corresponds to one risk scenario.

Risk assessment

Risk evaluation or risk assessment means that an analysis is used to asses whether a risk level is acceptable or not. Moreover, different opportunities to reduce the risk (if they exist) can be included. The evaluation is a suitable basis for planning and implementing risk-reducing measures, which is one purpose of risk and vulnerability analyses. Since there is no established level for what constitutes an acceptable or tolerable risk, risk evaluation in a risk and vulnerability analysis often deals with evaluating a number of alternatives for how the risk can be reduced. The evaluation itself is based on weighing advantages of proposed measures against their drawbacks and coming to a conclusion on whether the measure should be implemented or not. The evaluation should be based on the effects the measures proposed are estimated to have on the level of risk – that is, how much they reduce the risk, and the costs they entail. If there are other advantages and disadvantages, these should also be emphasized in the evaluation.

A problem in this context is that it could be difficult to show the risk-reducing effect of the measures, which is crucial for the analysis being used as a basis for decisions. Without a description of what effects a given measure is expected to have, it is difficult to determine whether the measure is suitable. One way of showing the connection between proposed measures and the effect is to start from the results of the risk analysis. They provide a picture of the situation before the measure has been implemented. The effect is subsequently described through showing how the measures will affect the risk. Concretely, this means showing how a measure of interest affects the answers to the three questions: (1) 'What could happen?' (2)'How likely is it?' and (3)'What are the consequences?' One way of doing this is showing which risk scenarios will be influenced by the measure in question, and at the same time describing how likely it is that the scenarios will occur, and what the consequences will be. With the help of this information, it will be easier to compare the costs of the measures with their effect on the risk. It will also be easier to compare different measures with each other. A risk evaluation is performed twice in a risk and vulnerability analysis. The first time is an issue of taking a position on which of the various risk scenarios that have been identified, and which the organisation chose to go further with, in order to evaluate crisis management capacity. The second time is when crisis management capacity is analysed, and there is a basis for performing the final risk evaluation. This is an issue of determining whether the risk level is acceptable or not, as well as whether any measure to reduce the risk level is to be implemented.

Examples of risk matrices.



Risk matrix

A 'risk matrix' is a common tool used in risk evaluations. It consists of two merged scales, and is used for assessing how likely it is that a specific risk scenario will occur, and what the consequences would be. The scales are often designed as a quantitative or qualitative ranking scale. The risk matrices may look different, depending on the perspective the analysis is based on. Two examples of risk matrices are illustrated in the figures on the next page. The vertical axis denotes how likely it is that a specific scenario will occur, and the horizontal axis illustrates how serious the consequences are judged to be. In the matrix on the left, a qualitative ranking scale has been used for both axes. This means that it is only possible to see whether a specific risk scenario is judged to occur more often than another, and whether the consequences are judged to be severe. On the other hand, it is not possible to see how much worse or how less likely one risk scenario is than another. It is, however, possible to do this with the matrix on the right in the figure. A ranking scale is certainly used, but the various steps also have a quantitative content that makes it possible to estimate how much worse a certain risk scenario is than another, as well as how much less likely one scenario is than another. For example, a scenario assigned to Category 4 on the probability scale (counted from the bottom) is around 10 times more likely than one assigned to Category 2.

Sometimes different colours are used in a risk matrix to describe whether a risk is or is not acceptable. Red is normally used to denote an area that is unacceptable, and green an area where the risk is acceptable. It is also possible to use colour scales without connecting them to whether



Vulnerability assessment.

the risk is acceptable or not. The risk matrix evaluates only one risk scenario at a time, and what is actually of interest to an actor is the total risk – that is, the contribution from all of the risk scenarios. This can be problematic, since it is relatively easy to control the results in a risk matrix by increasing or decreasing the level of detail describing the risk scenarios. Despite this shortcoming, the risk matrix is a common tool that adapts itself well to providing a rough overview of all the risk scenarios identified.

Capacity assessment

Capacity assessment is a form of vulnerability analysis and is regulated and described in more detail in municipal and county council risk and vulnerability analysis regulations (MSB 2010:6) as well as in state authority risk and vulnerability analysis regulations (MSB 2010:7). They will thus not be described further in this guide.

Vulnerability analysis

The vulnerability analysis aims at analysing, in detail, how serious and extensive a specific incident affects society or the organisation itself. Various vulnerabilities are identified with the help of the analysis. An important difference between a vulnerability analysis and a risk analysis is that the former is carried out with regard to a specific risk scenario identified in the risk analysis. A further difference is that the vulnerability analysis analyses one or more scenarios with the intention of identifying various vulnerabilities in more detail than in the initial risk analysis.

The consequences that society or the organisation itself – despite its capacity – failed to anticipate, resist, manage, and recover from indicate how vulnerable the organisation is to a specific incident. The emphasis in a vulnerability analysis should therefore be on analysing which consequences a certain incident entails and how the organisation manages, resists, and recovers from it. The chapter on tools and methods



(Chapter 5) shows a number of methods that can be used to analyse vulnerabilities and capacity, for example a dependence analysis that is in the form of a vulnerability analysis.

Working with scenarios

In analysing capacity and vulnerability, it is normal to work on relatively detailed descriptions of various types of risk scenarios. This has many advantages. One of them is that a scenario in general is easy to take in and understand, even for those who normally do not work with risk and vulnerability analyses. Another advantage is that scenarios, to a great extent, make it possible to assemble several specialist competences for joint analyses and assessments. For a scenario to be useful, it could be described and formulated as shown below:

- The scenario is based on a threat or source of risk, and can be described as one or more incidents that are directly or indirectly connected to each other. It is thus the introduction to the scenario and should preferably be identified in the preliminary risk analysis.
- The cause consists of the underlying circumstances that lead to the scenario and – if they exist – any special circumstances that trigger the situation.
- The context is the situation in which the scenario takes place. It can, for example, be the circumstances, geographic location, or weather-related conditions that are of significance for describing the scenario.

Identification and analysis

In a municipal organisation, every administration and company must identify the risks and vulnerabilities that could affect activities and the geographic area. They can also assess any damages and consequences. Based on this, an evaluation of what consequences any incident could have, as well as the probability that it will occur, is then conducted. The focus lies more on the consequences than the probability. The basis is then used to create a collective picture of risks, vulnerabilities, and relations of dependence in the entire municipality.

Exemple

• Direct consequences are the immediate effect the scenario has on people's lives and health, societal functionality, and the basic values within the time period the scenario is to illustrate.

Based on a scenario, the crisis management capacity of different actors can be analysed starting from incident development. Normally it is more interesting to try to draw conclusions for a larger set of risk scenarios. It is therefore important to try to vary the conditions for the scenario in order to thus 'cover' a greater number of risk scenarios, for example varying weather conditions, technical infrastructure functions, the contributions from other actors, and so on, in this way examining whether the crisis management capacity applies to a large number of scenarios.

MSB regulations regulate how municipalities, county councils, and state authorities must report their risk and vulnerability analyses. It is an advantage if there is a clear connection to the action programmes, plans, investigations, and other measures needed to put the risk and vulnerability analyses into a risk management context. This makes switching over to handling risks possible, as the risk management process is described in chapter 2. Concerning measures proposed in the results and conclusions, there are a few important aspects to keep in mind. Above all, measures that require investments and decisions in various forms. To determine whether the measures are suitable or

Exemple

Results and conclusions

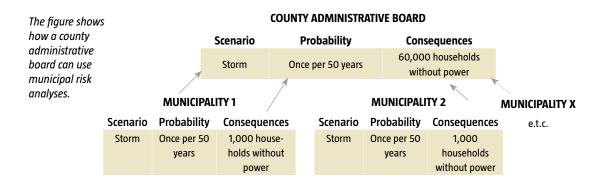
Starting from identified risks, a county council performs risk and vulnerability analyses, both for the respective administrations and regionally, as well as overall for the entire county council. In the latter case the analysis is based on prioritized scenarios. On the basis of the overall risk and vulnerability analysis, a crisis management plan and a crisis communications plan are established for the county council. Starting from the measurement proposals produced during the analyses, the measures necessary for improving or ensuring the county council's management capacity are prioritized. The risk and vulnerability work is a process in the daily work of the administrations and the activities.

not, any effects must be shown in relation to the costs. This consequently deals with showing a cost-benefit perspective on the measure proposals.

Presenting the measure proposals identified in the analysis makes it easier for those who are to make decisions based on the analysis. They get a clear description of what costs the measures entail and what effects (in terms of risk reduction) the measures are estimated to achieve. With the help of this information, it is possible to judge whether the costs are warranted.

Collocation and aggregation of risk and vulnerability analyses

The Swedish crisis management system is built on a holistic perspective – that is, the information produced for a specific risk and vulnerability analysis must be usable by other actors. The individual actor and the individual analysis are only pieces of the larger puzzle. The actors must contributed to society's collective ability to identify, analyse, and evaluate risks and vulnerabilities in such a way that the total effect is greater than if each and every one conducted their own analyses in isolation. For the system to function, the information from risk and vulnerability analyses must be communicable between the actors, and the content must be easily usable for those receiving the information. Various actors - the county administrative boards, for example should not simply conduct their analyses by compiling the information acquired from the municipalities and the county council. Rather, this deals with the county administrative board simply being able to use the analyses from the municipalities and the county council in producing the regional analysis. The county administrative boards have a different perspective in their analysis than the municipalities and the county council, and therefore a part of the information in the incoming analyses must be adapted before it becomes a part of the collocated analysis. A simple example can illustrate this. A county administrative board could, for example, be interested in the risk of serious storms in the county and decides that the consequences of storms must be described in terms of the effect on societal functionality (an evaluation). One way of doing this is describing the number of households that lose electricity due to a storm (concretising the evaluations). Conducting the assessment can be relatively time-consuming, since it probably means that the county administrative board must obtain information on the power grid and how the customers are placed in all the municipalities of the county. A simpler way would be to use the municipal analyses. Through them, it is possible, for example, to get information on the municipalities' assessment of what consequences arise when a storm occurs. The figure on the next page shows how a county administrative board assesses the consequences of a storm, based on the basic data from the municipalities in the county. In this case, all the municipalities have shown the 'storm' scenario and expressed the consequences as the number of houses estimated to be without power if the scenario occurs. If the county administrative board judges the information to be reasonable, it can choose to base its analysis on this information. In the figure below, the county administrative board estimates the consequences at 60,000 households without power, which could be the sum of the consequence assessments from the municipal analyses. It is not always so easy to perform an analysis like the one in the figure below. It may, for example, be that the municipalities have not analysed the 'storm' scenario, or haven't assessed the consequences in terms of how many households would be without power. The point is still that the county administrative board's overall judgement is made easier with a



common scenario and an assessment of the probability and consequence. It is then possible to see whether the information needs to be supplemented from any municipality. Without this way of showing results, the county administrative board's opportunity for making an overall judgement is significantly more difficult. Thorough documentation is important for other actors to be able to use the same information in their own analyses. It could be an issue of things that have to do with the risk analysis itself, but also of thing that are linked to conditions, delimitations, evaluations, and so on. Proper documentation, with descriptions of the risk scenarios and assessments of probability, are a clear foundation for decisions. It also provides good opportunities to create a comprehensive picture of risks and vulnerabilities at different levels and in various sectors of society.



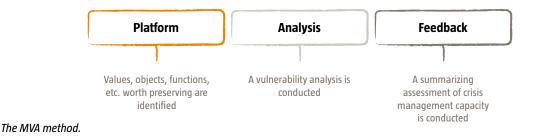
CHAPTER 5 Methods and tools

A method for risk and vulnerability analysis can be described as an approach to analysing risks and vulnerabilities in an activity, a geographic area, or in a system. Certain methods include both risk analysis and vulnerability analysis, while others are more suited to specific systems or a specific hardship. This chapter presents several methods that can be used to conduct risk and vulnerability analyses. Different methods can be combined advantageously and adapted to individual needs.

Risk and vulnerability analyses can be quantitative and qualitative. In a quantitative analysis, there should be adequate access to numerical data for calculating the probability of a risk incident. If this type of basis is not available, a qualitative analysis may perhaps be better suited. The broader analysis methods are often qualitative and require less effort in general. In certain cases, several methods must be used and combined to obtain a satisfactory analysis. There is therefore often reason to make use of both qualitative and quantitative data and information.

Seminar-based scenario methods

Scenario methods study one or more risk scenarios that could occur in the future. The results of the risk analysis provide a good description of different risk scenarios. The seminar-based scenario methods start from group discussions around a defined risk scenario that is frequently used for risk and vulnerability analyses. Some of the commonly occurring methods are MVA, IBERO, and ROSA. There are great similarities between the methods, but what differentiates them is that they focus differently on different areas in the analysis. The following text presents several seminarbased scenario methods that can be used in the work of the municipalities, county councils, and authorities on risk and vulnerability analyses.



MVA – multidimensional activity analysis

The MVA method was developed by a research group at Lund University, along with the Emergency Preparedness Authority and a number of municipalities. The purpose of the method is to analyse the vulnerabilities and capabilities of organisations and activities from a broad perspective, to develop measure proposals, and to create conditions for good exchange of knowledge and for personal networks. The method has a social perspective, which means that the assessment of consequences is based on their influence on society. Generally, it describes how the work on a risk and vulnerability analysis is to be designed, but it also emphasizes that the working process is an important part of the result.

There is IT support (software) for the method, but the method can also be used without it.

The MVA method is scenario-based and starts with a group of people gathering to discuss different risk scenarios that could occur in the activities of the actors. The work is divided into three different seminars: platform, analysis, and feedback.

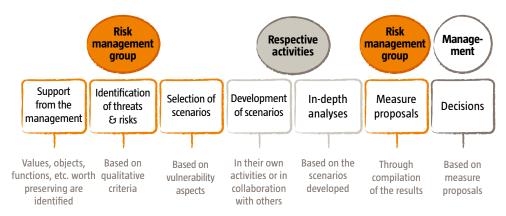
During the first seminar – platform – the working group inventories values, functions, and objects that are regarded as worth preserving. In the analysis, the actors start from a matrix and attach great importance to identifying the different parts of the activity, for example technical supply systems. Undesirable incidents, consequences, sources of risk, and risk objects are then inventoried, and a probability and consequence assessment of the identifies risks is conducted. When identification and inventory are finished, the group has worked up a broad analysis that will later lead into a number of risk scenarios. In the next phase – analysis – a vulnerability analysis of the scenarios chosen is conducted. This is a detailed vulnerability analysis where the group maps the actor's capacity to manage the risk scenario chosen and assesses the consequences. The scenario analysis is based on different periods of time. The first period starts with describing the scenario. The group then works on questions concerning measures, responsibilities, and capabilities. Finally, undesirable developments are indicated before the group goes on to the next period.

Feedback is the final step. The results of the analyses are then used to discuss how the capacity for managing the different risk scenarios can be improved. A consequence analysis and capacity assessment are conducted, which leads to measure proposals. The work of several organisations or administrations can be collected into a common risk and vulnerability analysis.

ROSA – Risk and vulnerability analysis

The ROSA method is the result of collaboration between the Emergency Preparedness Authority, the Kronoberg County Administrative Board, and Växjö Municipality. The method puts great importance on the risk management process support among the management, and the structure and mandate of the risk management group, among other things. A risk management group is a specially constructed group that works with the risk management process. It is composed of representatives from different parts of the organisation. The method also stresses that other work within the area should be included, that a continuous crisis management process is created, and that the work must be an integrated part of the actor's normal activities. The purpose of the method is above all to assess the actor's ability to manage an undesirable incident, as well as to provide a stimulus for work on crisis management issues.

ROSA is a vulnerability-oriented method. It starts from the hypothesis that it is not possible to identify in advance all the thousands of threats and risks that actors are vulnerable to. Active analysis work, however, must be able to cover a large part of the threats and risks that could be



The ROSA method.

expected to arise. ROSA starts from scenarios that support the group in assessing the actor's ability to manage hardships. The method was developed to suit municipalities, county councils, and other authorities as well as actors in the business world.

The first step in the ROSA method is garnering support for the work from management. The analysis work is then begun with identification of risks and threats. Scenarios in the activities concerned are then developed from the broad analysis. The assessments are based on the group's knowledge and are therefore qualitative. Every representative in the group writes down a number of risk scenarios that can be identified and then a simple probability and consequence assessment, on a scale of 1 to 5, is conducted. The descriptions become the basis for the next step, in-depth analysis.

The risk management group decides which scenarios need to be analysed further. Those that are rejected should be designed so that they function as 'type incidents', meaning that in some way they are representative of a large number of similar incidents that could happen to the actor. The activities affected by a given risk scenario are tasked with conducting a more in-depth analysis of the scenario.

The result of the in-depth analyses are compiled and presented by the risk management group. The next step is to include all the scenarios that were analysed and create an overview of the actor's risk profile. An assessment is then made of what weak points exist in the form of insufficient functions and resources. To visually illustrated different capabilities, signal colours are used for the three levels of assessment: very good, good, and poor. Finally, the results are presented to the management group, who makes a decision on which measures should be taken.

The method is relatively widespread, chiefly among smaller municipalities. One advantage of the method is that it is simple and adapted to the sometimes complex ways that municipalities, county councils, and authorities sometimes work. Nor does it require any in-depth knowledge of risk analyses from the participants.

IBERO – instrument for preparedness evaluation of area responsibility

The IBERO method was developed by the Stockholm County Administrative Board with support from the Emergency Preparedness Authority and in collaboration with the Swedish Defence Research Agency (FOI) and Lund University. IBERO has more the character of a tool than a method, but contains the various parts that are important in analysis work. The tool is adapted for individual actors, municipalities, county councils, county administrative boards, and authorities in their work on risk and vulnerability analyses.

The tool is scenario-based and supports the actors with area responsibilities in their work on analysing the ability to withstand and manage undesirable incidents, as well as review the consequences of the incidents. The tool is also IT-based and can store a large amount of information from various actors. It also supports communication between actors. The analysis tool contains four functions that are shown in the figure on the next page.

The work is carried out by a group that discusses and formulates various risk scenarios. There is the opportunity to analyse several different incidents that happen to one and the same actor – what's called synthesis. The advantage of synthesis is that it is possible to compare activities. Capabilities are tested in several situations, with a starting point of different incidents in the analyses. This means that the results of the analysis from an individual actor can be used for analyses at higher levels of operation, or for a summary of several actors' analyses. The approach visualizes the main

Preparedness evaluation for individual actor	Preparedness evaluation for several actors	Inventory of risks and resources	Reporting functions
 Assess capacity, consequences, causes, and spill over incidents Draw conclusions on capacity, consequences, causes, and spill over incidents for individual incidents Evaluate own general ability to manage extraordinary incidents and propose measures to strengthen manage- ment capacity 	 Draw conclusions on particular events for several actors Draw conclusions on society's general ability to manage extraordinary incidents and prioritise among measures in order to strengthen management capacity 	• Inventory within the geographic area	• Make out individually tailored working reports with different intersections in order to utilize the information in IBERO effectively

The IBERO method.

consequences of the various incidents, as well as capacity in the various parts of the crisis management process and for different incidents. The side effects of the incidents on other sectors of society are also clarified.

When the risk scenario analysis is ready, the capacity of the activity for managing the incident is assessed. The starting point of the assessment is the ten different tasks in the crisis management process that are described in the tool. A consequence assessment is then conducted, as is an assessment of any spill over incidents. The assessments should be carried out by expert advisers and can take place through interviews, document studies, or workshops.

There is a reporting portion and a smaller risk inventory portion in the tool. The report module allows the actor to make out a report as needed, while the inventory module is used to compile risks and resources within the geographic area – things like hazardous goods, dangerous activities, and resources.

Traditional risk analysis methods

Everything used to analyse technical systems, which are also called system-based methods, are included from the traditional risk analysis methods. In this chapter, the definition of system is used, which can be compared with the activity or function the actor intends to analyse. In certain cases the methods could be too detailed or too technically focused to be usable in complex systems such as activities in the municipalities, county councils, and other authorities. On the other hand, they can be a good complement to work on risk and vulnerability analyses. The difference between scenario-based methods and traditional risk analyses is that the latter focuses more on describing the system and its functions before the analysis is conducted. The analysis methods taken up in this section are Broad Analysis, Fault Tree Analysis, and the 'What-if' method.

Broad analysis

Broad analysis is a qualitative method used to map risks in a system and identify risk scenarios. The analysis is also called preliminary risk analysis, since it is often used in the initial phase and as a basis for prioritising in the continued analysis work. It does not provide a complete picture of the system's risks, and it does not describe any vulnerabilities or the ability to handle them. The goal of the broad analysis is to obtain an easily understandable picture of all the potential risks within the actor's activity. The method is represented in almost every analysis method as a first step in the work.

A broad analysis is preferably carried out by a working group that has knowledge of both the method and the system to be analysed. The qualitative character of the analysis means that identifying risks and causes, as well as assessing consequences, is based on the experiences and creative thinking of the working group, and any possible check-lists. Before the work begins, it is a good idea to obtain as much information as possible about the system, but also information, statistics, and experiences from similar systems. The analysis work itself starts with brainstorming that can be supplemented with a systematic approach, for example check-lists.

When the risks are identified, each of them are analysed through a description of the course of the incident. Factors

BROAD ANALYSIS OUTLINE								
Identified risk/	Possible causes	Consequences	Comments	Risk evaluation	Conse- quence			Recom- mended
scenario				Probability	н	м	Е	measures
Collision train/car	 Crossing barrier out of order Train driver did not stop on red 	 Personal injuries Material damage Traffic jam 		3	4	1	2	Flyover junctions
Derailing of liquefied petroleum car	 Substandard maintenance Sabotage Train driver speeding 	 Explosion BLEVE Personal injuries Material damage Traffic jam 		1	5	2	5	Fördjupad riskanalys krävs
Derailing of car with carbon dioxide	 Substandard maintenance Sabotage Train driver speeding 	Toxic gas release		2	5	3	4	More in- depth risk analysis required

Broad analysis.

such as possible causes, consequences, and probability are noted. The consequence assessment is based on the categories people, environment, and property. A five-step scale is often used in the assessment, but the actors can establish their own classes for their activities according to what seems suitable. The probability assessment is carried out in the same way. The risks are then ranked based on the results of the probability and consequence assessment. The results of the assessment are best reported in a matrix.

The last step in the analysis is proposing measures. Cost proposals for the various measures can also be reported. The results report should be easily comprehensible, with the help of diagrams or a broad analysis outline. The scenario, possible causes, consequences, existing protection, measures taken, and risk evaluation are presented in the report, as well as recommended measures.

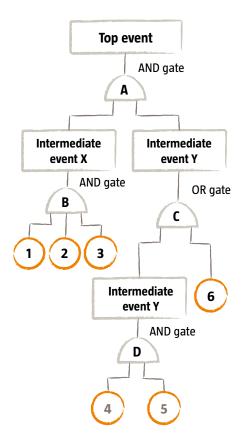
'What if' analysis

The 'what if' analysis, or 'what happens if' analysis, was developed during the 1960s in the oil and chemicals industry. The method is chiefly used in the processing industry, but can be used in other areas, for example handling environmentally hazardous goods, or flammable or explosive goods. The most common area of use is risk assessment in connection with changes in processes or activities.

The purpose of the 'what if' analysis is to identify potential undesirable incidents in a system, and to investigate underlying causes as well as possible consequences. The analysis of the deviations that can arise in planned functions leads to improvement proposals and a basis for measures.

Initially, a structured brainstorming is carried out around which undesirable incidents could possibly occur in the system. The participants start from the question "What happens if ...?" The questions are usually formulated starting from previous experiences, but the participants also have help from blueprints and flowcharts. The method is relatively simple, but requires good imagination and knowledge of the system so that the right questions can be asked. When the undesirable incidents are identified, the causes of why they could happen are analysed. In addition, a consequence assessment is conducted. Sometimes a probability assessment of the undesirable incidents and their consequences is also conducted. Finally, measures for decreasing the probability of undesirable incidents occurring, or for reducing their consequences, are proposed. The results are best presented in a diagram or in an outline that provides an easily understandable picture of the results.

The analysis is relatively quick to carry out and is thus quite inexpensive. Nor is it as structured or detailed as other analysis methods. No greater theoretical or analytical background is thus required to carry it out. The most suitable structure for the analysis group is several people with knowledge of the method, and several with good knowledge of the system.



Fault tree analysis.

Fault tree analysis

The fault tree analysis is chiefly used in technical systems and for investigations into cause. It has a relatively broad area of use and is one of the methods most used for risk analysis. The method has its origins in the space industry and was developed during the 1960s. It aims at identifying the reasons why undesirable incidents occur. The starting point is an undesirable incident, called a top event. Through a logical approach, the incident is gradually broken down to the desired level of detail so that the error that caused it is discovered. It is also possible to see the connections between different erroneous actions and erroneous functions that led to the top event. The method is both qualitative and quantitative in character. A fault tree analysis consists of three elements: fault tree construction, identifying which combinations of events caused the top event, and an evaluation. In constructing the fault tree, the top event and the erroneous

actions and functions that could lie behind the cause of the top event are described. This takes place through logic gates that have different contents. The gates show, among other things, whether the top event was caused by only one incident, or several incidents in combination. The erroneous actions and erroneous functions identified are then broken down so that it is possible to discern which incidents cause them. In the next step, the incidents that started the chain reaction – called basic events – are identified. Specific combinations of incidents are then mapped.

The evaluation of the fault tree takes place in the form of an assessment of the probability or frequency of the top event being calculated. This can occur both qualitatively and quantitatively. The quantitative assessment is conducted with the help of calculation rules linked to the logic gates.

It is best if there are skills in both the method and the system in the group. For the analysis to be the best one possible, a properly informative basis is required.

Other traditional methods

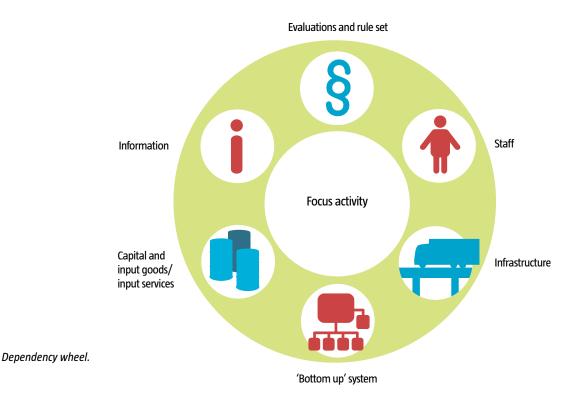
Apart from the traditional methods above there are several others such as Event Tree Analysis, HAZOP – Hazard and Operability Analysis, MORT – Management and Oversight Risk Tree, and SMORT – Safety Management and Organisation Review Technique.

Other methods, models, and tools

Beyond the established and traditional methods already presented, there are a few other methods, models, and tools worth mentioning in the context, such as Dependency Analysis, Capacity Assessment, RIB, and IDA.

Dependency analysis

Dependency analysis is a method that the Emergency Preparedness Authority developed from a commission to analyse critical dependency relationships in society. The method aims, in other words, for an actor to be able to identify and analyse existing dependencies on other actors. This is not a risk and vulnerability analysis, but the method can be



advantageously used to analyse the actors' relationships of dependency. It is suited for municipalities, county councils, other authorities, businesses, and individual activities. The knowledge brought forth in a dependency analysis provides a good foundation for such things as discussing how society or the actors' activities can be safer, as well as improving plans and making them more in-depth prior to crises.

The dependency analysis is divided into three steps: selection and description, identification and evaluation of external dependencies, and aggregate analysis. In the first step the activities to be analysed – the societal functions – are selected. What the activities must deliver is then described, as is to what extent and to whom.

In the next step, external dependencies are identified. The actors can either do it themselves via an external resource, or with the help of a 'dependency wheel', which was developed as an aid to the work (www.beroendehjulet. se). The tool is provided by MSB free of charge.

When the selection and description are complete, the external dependencies of each activity are identified and evaluated.

First, the needs of the activity are described, starting with the question: What does the activity need to function? That is, what is required for the activity to Values and rules achieve what was illustrated in the previous description? Needs entailing a dependency on an activity or resource outside of the organisation itself are called external dependencies and are evaluated in the next phase. The starting point for the evaluation is the activity's capacity of managing a disruption in another activity that it depends on. As a basis the consequences, shock absorbers, and stamina are first assessed, starting with the following questions:

- *Consequences*: What happens to our own activity if and activity it depends on isn't functioning?
- *Shock absorber*: Are there alternative ways of meeting the needs without the activities we depend on?
- *Stamina:* How long will the activity manage without the activity it depends on?

Based on the description of consequences, 'shock absorbers' and stamina, the strength of the dependency is evaluated according to the following scale:

- *Critical dependence:* The activity has no shock absorbers and extremely limited stamina.
- *Clear dependence:* The activity has some shock absorbers and a certain amount of stamina.

Example of a dependency matrix.

	Sewage	District heating	Electricity supply	Emergency medical care	Municipal elder care	Labour power
Sewage	-	0	0	5	5	3
District heating	0	-	0	5	5	1
Electricity supply	5	3	-	3	5	3
Emergency medical care	0	0	0	-	3	1
Municipal elder care	0	0	0	3	-	1
Labour power	3	3	3	5	5	-

• *Weak or uncertain dependence:* The activity can have weaknesses under very specific circumstances, but can in the majority of cases handle the disruption well.

No activity is completely independent from another and no activity is entirely without influence on others. On the other hand, there is a relative difference in the degree of dependency between various activities.

In the third and final step of the analysis, the information around every activity is collected into an aggregate analysis that provides a comprehensive picture of how the activities studied influence each other, directly and indirectly. The first step in the aggregate analysis is structuring the collected material on the dependencies of the activities. This can be done with the help of a matrix where all the dependencies and their strengths are indicated. All the activities analysed are on both axes of the matrix. The strength of the dependency, as it was estimated in earlier steps, is indicated at the intersection between two activities. The matrix shows all the direct dependencies for each activity.

Tools connected to risk management

IDA – indicator, data, analysis

IDA is a web-based statistical database developed by the Swedish Rescue Services Agency and which is now provided free of charge by MSB. It contains statistics on the information that MSB collects and analyses. The statistics cover the entire country, and all the counties and municipalities. The database is comprised chiefly of available data within the field of disasters.

The database is divided into three parts: indicator, data, and analysis. The indicator portion contains data from national databases and provides information on situation reports and comparisons between municipalities, counties, and the nation. One of the indicators is taken from SKL, the Swedish Association of Local Authorities and Regions' report Transparent Comparisons for Security and Safety, which is presented annually.

The data portion provides users with the opportunity to create their own tables and diagrams based on MSB statis-

tics. There are also links to other disaster databases with statistics on such things as natural disasters, municipal crisis management, and everyday safety. The analysis portion contains summaries, cost-benefit analyses, and evaluations of methods and working methods used by various actors.

RIB – integrated decision support for protection against disasters

RIB is primarily a toolbox and source of information for actors in operational decision making who manage hazardous substances in various ways as part of their work. The tool has its starting point in activities affected by the Civil Protection Act – emergency services, the police, the Coast Guard, and customs, for example. It is also usable from a broader perspective, within the field of risk management.

RIB is a link-up of several databases that provide information on how a disaster can be managed, how preventive work can be planned, what risks a disaster that has occurred entails, what resources are available, and where they are located. RIB contains things like information on over 5,000 hazardous substances and information on resources within emergency services, businesses, and authorities in the form of material, vehicles, and experts who can be made use of. The resources can be searched by municipality, region, or across the whole of Sweden.

Apart from the main programme, there are a number of calculation tools for operational decision making that touch on hazardous substances and which are addressed to emergency services, municipalities, and county administrative boards. There is also a management system that can be used during an operational effort. In the management system, it is possible to record incidents and decisions, strengths, basic tactical attitudes, trends, and decisions in broad outline. It is possible to create a graphic picture of the ongoing effort. Apart from this there are documents, training packages, and databases as support for work in the field. As part of the program there is also RISKERA, a GIS took for visualising the risk profiles of municipalities, chiefly during large-scale disasters. RIB is provided free of charge by the Swedish Civil Contingencies Agency to actors currently active in the field.

References and further reading

Vägledning för kommunalahandlingsprogram (MSB, Publ.nr MSB245 - april 2011)

Faller en – faller då alla? En slutredovisning av KBM:s arbete med samhälls-kritiska beroenden (MSB 0001-09)

Hur styrs skyddet? (MSB 0133-09)

Olyckor och kriser 2009/2010 (MSB 0170-10)

Styrel, inriktningsdokument (MSB, dnr 2009-3054)

Beroendeanalys – så gör du! (KBM) Kontinuitetsplanering – en vägledning (KBM)

Samhällsviktig verksamhet, Definition av samhällsviktig verksamhet ur ett krisberedskapsperspektiv (MSB Faktablad)

Samhällskriser och katastrofer, juridisk handbok (SKL 2007)

Risk- och sårbarhetsanalyser, SEX GODA EXEMPEL (SKL 2010)

Proposition 2010/11:1 Budgetproposition

Skrivelse 2009/10:124 Samhällets krisberedskap – stärkt samverkan för ökad säkerhet

Proposition 2007/08:92 Proposition 2005/06:133, Samverkan vid kris för ett säkrare samhälle

Appendix - Terms and concepts

Below is a presentation of the terms and concepts used in the guide. The same concept can often have different meanings, depending on the context in which it is used. Since they cannot easily be defined, the concepts used should chiefly be used as part of this guide. In other contexts, these concepts have been used with other meanings.

Responsibility principle

The responsibility principle means that the person responsible for an activity under normal circumstances has the same responsibility during a crisis. The responsibility includes taking the measures required to create both resilience and crisis management capacity. The principle also means each actor is responsible for cooperating with others, often across sector boundaries.

Capacity

This means crisis management capacity and the ability in societal functions to withstand serious disruptions.

Crisis management capacity means that within the area of activity or responsibility there must be an ability, during serious disruptions, to lead one's own activity; to make decisions within one's own area of activity or responsibility; to disseminate quick, correct, and reliable information; and if needed to be able to cooperate with other actors. There must be an ability to initiate measures as early as possible to manage or participate in managing the consequences of incidents that occur, and carry out the measures required to remedy, protect against, and alleviate the effects of what has occurred.

The ability, in societal functions, to withstand serious disruptions means that there must be an ability to withstand serious disruptions so that the activity can be conducted at such a level that society can continue to function, while ensuring basic services, security, and medical care at the same time.

Crisis

An incident that affects numerous people and large portions of society, and threatens basic values and functions. A crisis is a condition that cannot be managed with normal resources and organisation. A crisis is unexpected, outside normal, everyday existence. Resolving the crisis requires coordinated measures from several actors.

Crisis preparedness

Crisis preparedness means the ability to prevent, withstand, and manage crisis situations through training, practice, and other measures, as well as through the organisations and structures created before, during, and after a crisis.

Threat

Includes the capacity and intent of an actor to carry out harmful actions. A threat can also consist of an incident or a phenomenon that in and of itself causes danger for something or someone without there being actors with the capacity and intent to cause damage in that context.

Critical dependency

Dependency that is crucial for societal functions to be able to function. Such dependencies are characterised by a loss or disruption in productive activities leading relatively immediately to impairments that may result in a serious crisis occurring. The activity affected is characterised by a lack of stamina, redundancy, and the possibility of replacing the resource lost or functioning without it.

Risk A consideration of the probability that an incident will occur and the (negative) consequences that this could lead to.

Socially necessary activity

Socially necessary activity means an activity that meets one or both of the following conditions: A lack or serious disruption in the activity that alone or alongside similar incidents in other activities leads in the short term to a serious crisis occurring in society. The activity is necessary or quite essential for a crisis already occurring in society to be manageable so that the harmful effects are as small as possible

Vulnerability

Indicates how much or how seriously society or portions of society are affected by an incident. The consequences that an actor or society – despite a given capacity – did not manage to anticipate, manage, withstand, and recover from indicates the level of vulnerability. Area of activity and responsibility This means the authority's own area of activity, as well as the area of society within which the authority has a particular responsibility.

Extraordinary incident

Extraordinary incident means an incident that deviates from the normal, which entails a serious disruption or imminent risk of a serious disruption in vital societal functions and which requires speedy efforts by a municipality or county council.

Serious incident

Serious incident is a concept chiefly used within the field of health and medical care, the Swedish National Board of Health and Welfare, defines the concept as an incident that is so comprehensive or serious that resources must be organised, directed, and used in a particular way.

Continuity planning

A method for ensuring an organisation's capacity to deliver through planning for continued activity under impaired abilities. That is, to be able to deliver services and products that are the most important for the organisation and its target audiences despite interruptions.

Picture listing

Illustrations: Advant Produktionsbyrå AB and Per Hardestam.

Photos:

- p. 6 Niklas Larsson/Scanpix
- p. 10 Kalle Lind/Scanpix
- p. 23 Mats Kockum/Scanpix
- p. 36 Karl Melander/Scanpix
- p. 60 Gaetan Bally/Scanpix

Anticipation and prevention are essential for proper emergency preparedness and good safety work. Authorities should therefore continually analyse what risks and vulnerabilities exist in their area of responsibility. Risk and vulnerability analyses form an important part of authorities' risk management.

The purpose of this guide is to support government authorities, county administrative boards, municipalities, and county councils in their work on risk and vulnerability analyses, and to provide suggestions on how the analytical process can be managed. An easy-to-understand picture of the methods and tools to be had for the work is also presented.

The guide also describes an approach to looking at risks impartially and to adapt the work on risk and vulnerability analyses to the needs and circumstances of the organisation itself. This guide is addressed primarily to those who are working with risk and vulnerability analyses, but can also be useful in a training context, and for those otherwise interested in the subject.

Swedish Civil Contingencies Agency (MSB) SE- 651 81 Karlstad Phone (0)771-240 240 www.msb.se/en Order No. MSB366 - March 2012 ISBN 978-91-7383-208-3