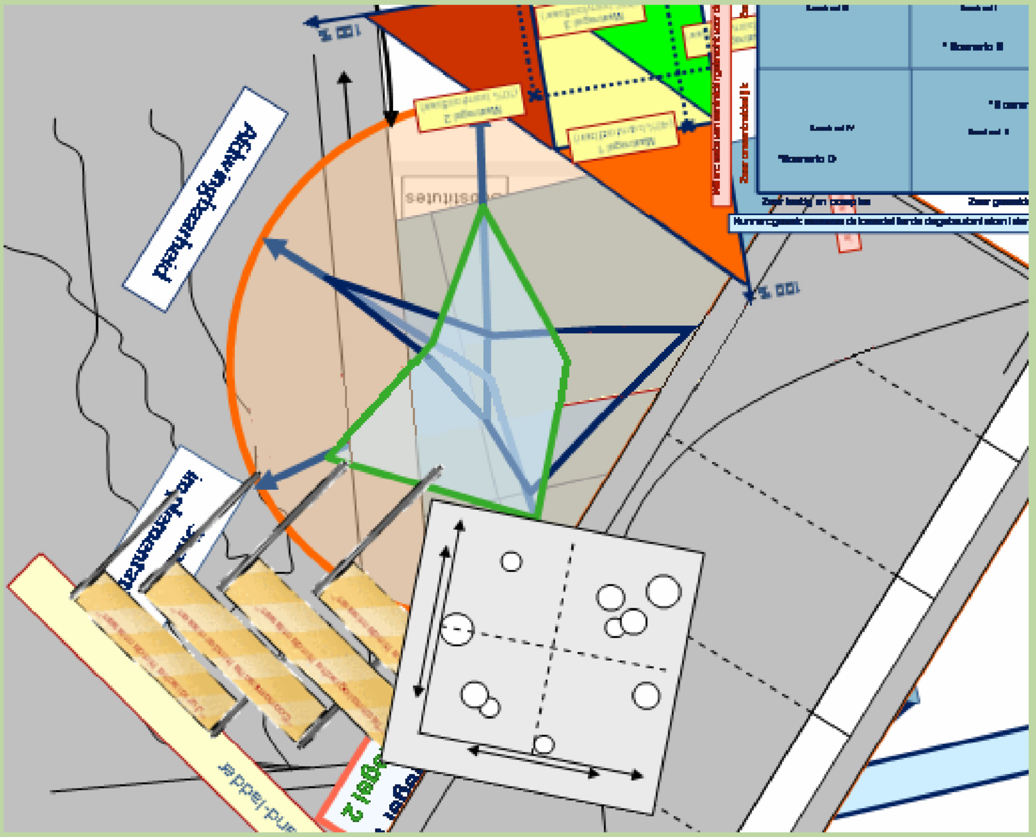
A VIEW ON RISKS



Risk Modelling Handbook

RISK MODELLING HANDBOOK

Selection of models and methods for conducting risk analyses

Authors:

Berenschot:
Ir. B.P.A. van Mil
Ir. A.E. Dijkzeul
Drs. R.M.A. van der Pennen

The authors would like to thank their partners, Delft University of Technology, for their share in this project.
From the department Policy Analysis:
Prof. mr. dr. E.F. ten Heuvelhof
Dr. M.J.G. van Eeten

From the department Safety Science Group:
Prof. dr. B.J.M. Ale
Prof. dr. A.R. Hale
Dr. ir. L.H.J. Goossens

Utrecht
February, 2006

CONTENTS

I. Analysis of vital interests and systems

II. Identification of threats

III. Evaluating and prioritising the impact

IV. Formulation, evaluation and implementation of measures

FOREWORD

Society is becoming increasingly dependent on vital infrastructure, such as the telecommunication and energy infrastructures, which is why the Ministry of Economic Affairs (*EZ*) has adopted a policy that ensures delivery security for both these infrastructures. One aspect of this policy is to conduct a risk analysis at a national aggregation level to discover what risks threaten delivery security and to evaluate what measures need to be taken.

There are countless methodologies, models and work forms for conducting such risk analyses. These are also described in the literature both in scientific papers and in reports that focus on practical applications. What is clear from the literature is that many types of models, with varying scopes, are available and that there is no standard method. After all, the desired approach depends on the goal of the particular analysis, the characteristics of the service or sector, the time available or the expertise available both within and outside the department. A roundtable discussion is one work form used to conduct risk analyses because it makes it possible to focus a considerable amount of expertise on a particular issue in a brief time period. However, this work form also involves the risk that results are influenced strongly by opinions, which are by definition subjective, and by the possible dominance of the experts participating.

This example demonstrates an important point: choosing a methodology, model or work form demands, at the very minimum, meticulous, explicit consideration. This fact, combined with the lack of a handy overview for policy staff, was the incentive for having this manual created by a team from Berenschot / TU Delft under the leadership of Berenschot's B.P.A. van Mil. This manual describes a variety of methodologies and work forms, thus assisting policy staff in selecting the appropriate work method. Previous experiences amassed by policy staff were drawn on exhaustively as this manual was being written.

This manual was compiled on behalf of the Ministry of Economic Affairs. However, I am convinced that it contains concepts and methodologies that could prove useful for other vital infrastructures. This conviction is based in part on reactions from colleague policy staff from various sectors who were consulted during this study. I hope that this book will be used effectively outside of the Ministry of Economic Affairs!

Ronald van der Luit, project leader

Ministry of Economic Affairs

INTRODUCTION

Objective of the manual

In today's society, all sorts of products and services depend on ICT and energy. It has been accurately said that ICT and energy are the engines that drive all of society's processes. As the department responsible for the provision of ICT and energy, the Ministry of Economic Affairs (*EZ*) is implementing a policy geared to ensuring delivery security within these two network sectors.

As part of this policy, Economic Affairs is conducting a risk analysis at the national level, for example in the framework of the 'Protection of Vital Infrastructures' (*BVI*) Project and the attacks on the twin towers in New York on 11 September 2001. The Protection of Vital Infrastructures Project is a result of Lower House member Wijn's motion[1] asking the government to draw up a plan of approach for protecting vital infrastructures, in particular ICT. This involves a large-scale process, launched in April of 2002 and coordinated by the Ministry of the Interior and Kingdom Relations, which involves close collaboration among departments, business and semi-government agencies. As part of the Protection of Vital Infrastructures Project, which involves all vital sectors in society, vulnerabilities and possible protection measures are inventoried. The objective of the analyses conducted in the framework of Protection of Vital Interests Project, but in the framework of all other risk analyses that the Ministry of Economic Affairs conducts as well, is to uncover all risks that threaten delivery security and to evaluate whether the government must take extra measures as a consequence of these risks.

This manual must be helpful in this process. By describing relevant methodologies that can provide insight into the risks and the possible effects of such risks, this manual will make it possible to conduct (even) better risk analyses. After all, applying these methodologies will make it possible to get a better idea of the nature and scope of any risks that may threaten delivery security in the telecommunication or energy sector and to gain a clearer idea of the measures that need to be taken based on setting the proper priorities. This contributes to (even) better policy that is well substantiated, explainable and based on sound argumentation.

Format

Section 2 of this manual explains the basis for a sound risk analysis. The insights are specified in the paragraph headings, which can be used as a sort of checklist.

Paragraph 2.1 explains that three different perspectives are involved in a risk analysis: the perspectives of the policy staff, the risk analyst and the process manager. Paragraph 2.2 then describes the points of attention a good policy staff maintain when conducting risk analyses. Paragraphs 2.3 and 2.4 describe the roles of the risk analyst and the process leader. Section 3 then outlines the different objectives that can serve as a basis for conducting a risk analysis. Different objectives require different methodologies. Paragraph 3.2 then describes a comprehensive methodology, which involves four steps:

Step I: Analysing the vital interests and systems

Step II: Identifying the risks

Step III: Evaluating and prioritising the effects

Step IV: Formulating and implementing the measures

Specific questions must be asked for each step. Specific models and methodologies are available for answering these questions; these are discussed in Section 4 (also classified by the four steps). Different models are applied when answering the questions posed during each of the steps. The ***summary page*** shows what model can be applied for what question.

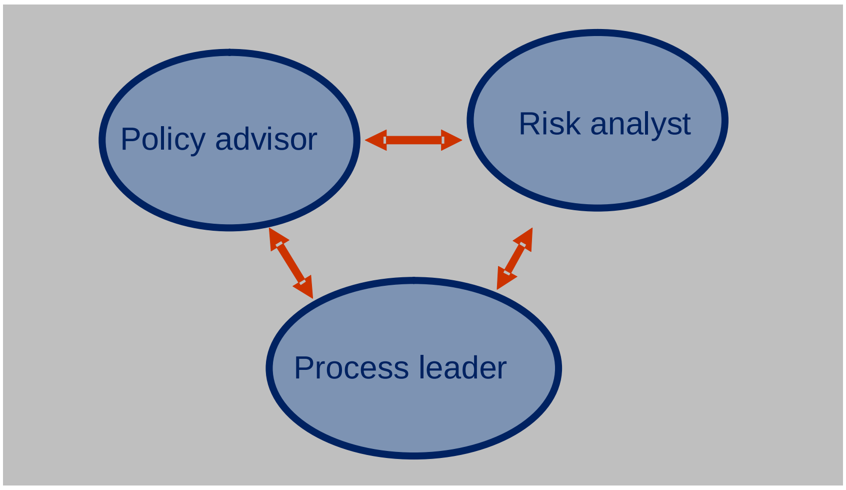
[1] 2663 no. 20, Motion of Lower House member Wijn

Section 5 provides an overview of the work forms that can be applied during the risk analysis process. These are, as it were, instruments with which the risk analysis method from Section 4 can be conducted.

THREE PERSPECTIVES FOR A SOUND RISK ANALYSIS

Three perspectives: policy advisor, risk analyst and process leader

A risk analysis can be performed from one of three perspectives or rationalities. For policy staff, all three perspectives are relevant when conducting a risk analysis.



First of all, there is the perspective of the policy advisor. The policy advisor continually asks himself whether the government has a role in taking measures regarding risks and, if so, what the government's role should be. Moreover, the policy advisor is also a political servant and must also consider political interests as he performs his duties. Serving his political 'customers' is thus important to the policy advisor. This means that he must sometimes be pragmatic; specific risks must be mapped out within a very short time.

Second, there is the perspective of the risk analyst. The risk analyst continually asks himself how he can get the most complete image of the risks possible. The risk analyst wants to collect all of the information for inclusion in his analysis. For the risk analyst, mapping out risks is an objective in itself.

Third, there is the perspective of the process leader. The process leader continually asks himself what parties must play a role in the risk analysis process, and what these roles should be. The process leader explicitly focuses on developing broad-based support.

A good policy advisor...

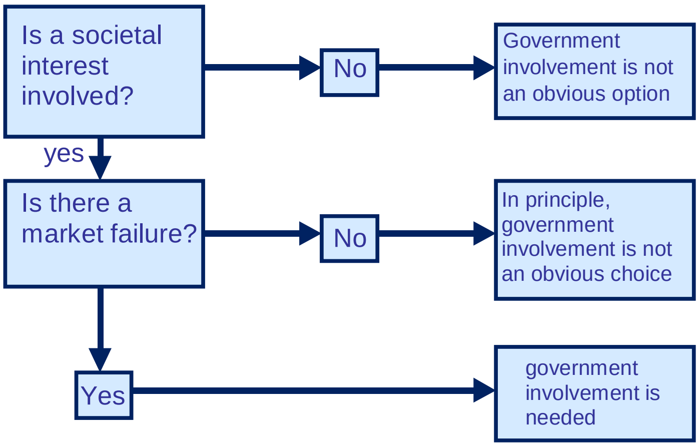
Important points of attention related to the perspective of a good policy advisor are discussed below.

...studies the social importance and gaps in the market and evaluates: is this a government task or not?

General economic policy is based on the notion that prosperity is best served by proper operation of the market, at least, where this is possible. However, some matters are not covered, or cannot be covered via the market, such as maintaining law and order and defence. On the other hand, many markets display special characteristics that stand in the way of proper operation. There are failures in these markets. The existence of market failures or gaps in the market may justify government intervention in market processes.

In principle, in a situation in which there are no market failures, there is no role for the government, unless the government can provide reasons for intervening. In the case of market failures, government involvement is required. In every case in which government involvement is being considered, a societal interest must be involved. The following diagram provides an evaluation framework for the issue of government involvement.

Evaluation framework: Government task or not?



Is a societal interest involved?

No

Government involvement is not an obvious option

yes

Is there a market failure?

No

In principle, government involvement is not an obvious choice

Yes

government involvement is needed

The first question is whether or not a societal interest is involved. Societal interests are interests whose promotion is deemed to be desirable for society as a whole. Examples are sustainable economic growth or better utilisation of ICT. Because, for example, (large-scale and lengthy) failure of ICT or electricity can lead to considerable disruption of societal and economic processes, these are considered societal interests. From that perspective, it is relevant to consider what would happen should KPN go bankrupt, for example, and its network should suddenly be left unattended. This has considerable societal and economic consequences because it would mean that other suppliers would no longer be able to provide their services as a result of their strong dependence on KPN's network for access and interconnection. In general, where societal interests are at risk, vital infrastructures are involved, and the government has an extra responsibility for these services. In the framework of the Protection of Vital Infrastructures Project, the term vital is defined as follows:

An infrastructure is considered vital if it fulfils at least one of the following criteria:

- Disruption or failure of a vital sector, product or service which would involve societal and/or economic consequences;
- Disruption or failure would directly or indirectly lead to many victims;
- Disruption is long-term, recovery would take considerable time and no viable alternatives are available during the recovery period

If a societal interest is not involved, then a government role is not a natural alternative. If a societal interest is involved, a second question is relevant.

The second question is whether there is a market failure. After all, even though societal interests are involved, that does not necessarily mean that the government must take on such interests. Frequently these interests are promoted without government involvement. Baking bread is a good example. The availability of good, healthy bread can be regarded as a societal interest, but because there is no market failure, government intervention not necessary. In this framework, the government could better serve in the role of Supervisory Agency.

A number of reasons for market failure are discussed below.

External effects. One can speak of external effects if an individual or organisation profits from or is disadvantaged by the economic activities of other individuals or organisations, and these parties are not themselves capable of mutually balancing the costs and benefits. In the security domain negative external effects are involved when market parties are not satisfactorily stimulated to reduce risks by taking the measures desired by society. For example, because their competitors are not taking such measures and thus this would negatively affect their competitive position. For example, because the risk for the end-user – the customer – is hardly visible: investing in reducing risks is not a profitable investment from a business perspective. For example, when the benefits of taking security measures are enjoyed by a party other than the one bearing the costs of taking these measures and these costs cannot be recovered via market transactions. In this case, the risks are not properly covered by the market. Moreover, this can change as a result of developments over time. For example, a few years ago Internet Service Providers (ISPs) were not scanning their mail servers for viruses.

After all, it was the consumers who enjoyed the benefits, while the costs fell completely to the ISP. Once ISPs themselves starting suffering from the effects of viruses, as manifested in exorbitant quantities of mail traffic generated by viruses, and started having to install extra server capacity, they were motivated to do something about the problem. The costs and benefits both accrued to the same party, namely the ISP. Moreover, the extent to which parties are able to accurately estimate the costs and benefits of measures also plays a role here.

Information symmetry. In an ideal market information is complete. This means that relevant information regarding suppliers and requestors and regarding the quality and price of the goods offered and those requested is available and clear. In practice, such information is never completely available, and the consumer incurs costs in terms of both time and money if he is to acquire good information. Thus there is information symmetry, specifically between the requesting party and the supplier. In addition, available information regarding the quality and price of the products can be unreliable.

Too little interaction between the actors in the system. For the production of some goods, minimum economies of scale are required. Unsatisfactory demand can become an obstacle for achieving the requisite minimum scale. If the market is not able to achieve these economies of scale itself, from a societal perspective too few of those goods are produced. That may be justification for government intervention, e.g. stimulation of pilot projects, exploration of ways to bundle demand and to organise and harmonise demand and to promote supply.

Too much interaction between actors in the system. This can result in abuse of market power: creation of cartels and price agreements, a few large parties who collectively keep new entrants out of the market. The type and extent of abuse of market power as a failure of the market depends on the perspective. From a static perspective, any form of market power is less than optimal. The prices of products are too high and the quality too low. From a dynamic perspective, specific forms of market power are desirable. Based on this latter perspective, companies need market power to earn excess profits that can then be used to generate resources for technological development, which is needed for long-term economic growth.

Lock-in effects. In some markets lock-in effects can arise; organisations wait for one another to take the first step. For example, development of hardware-specific software generally does not take place until hardware is being used by a large number of users. On the other hand, sales and use of that hardware does not pick up speed if no software is available.

Unpredictable risks and risks that cannot be insured. Risks that cannot be insured are risks that are so great or so unpredictable that they cannot be insured in the market or can only be insured at extremely high costs. If specific production that serves a societal interest cannot take place due to uninsurable risks or because risk premiums are exorbitant, this is also a type of market failure.

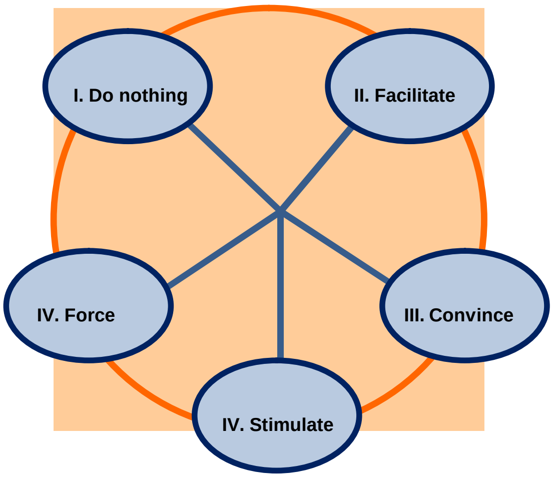
...Then select a suitable intervention level

The decision tree diagram at the end of Paragraph 2.2.1 is based on a dichotomy: there is or is not a question of societal interest and there is or is not a question of market failure. In practice, these are sliding scales and there is no simple yes or no answer.

This also applies to the resulting government involvement. After all, if there is no market failure, government involvement is not really needed. Still, there may be reasons for government involvement, and for creating agreements between parties in the sector to facilitate and make certain things possible, for example. This may be necessary in order to achieve good policy.

When it comes to government involvement, a distinction can be made between five intervention levels that range from doing nothing to compulsory control:

Government intervention: five levels



One example is considering the intervention level when stimulating Internet users to take good security measures (using anti-virus software, etc.). Different alternatives are available. The first option is to *do nothing* because one can reason that this is the end-user's or service provider's responsibility. A second option is to *facilitate* service providers in consulting with one another and coming up with solutions. A third option is the *convince* end users and service providers - for example through communication - that this is really important, and thus requires attention. A fourth option is to *stimulate*, for example by having the government find service providers who do not take specific principles into account. A last option is to *force* action using strict laws and regulations, coupled with intensive maintenance.

Another example. In the framework of NACOTEL, telecom operators work with one another in the domains of safety and continuity, among others. NACOTEL can be considered a form of self-regulation, by which the government controls based on different roles. First of all, Economic Affairs has a *facilitating* role, e.g. it stimulates the development of a collective standard and stimulates the parties involved to share best practices. Secondly, Economic Affairs fills a *convincing* role, in part by providing information, for example, and by pointing out to parties the necessity of voluntary inspection by a third party. Thirdly, Economic Affairs *stimulates*, for example by making it mandatory for companies to report security incidents. It is interesting in that domain to award certification, analogous to the Police Certification, for example. Certification enables companies to enjoy advantages, e.g. a lower insurance premium or a specific preferred position that is coupled with fewer administrative burdens (fewer obligations regarding accounting to and reporting to the government). Fourth, Economic Affairs *forces*, e.g. by imposing mandatory inspections.

In each instance, policy staff must evaluate what intervention level is suitable. That depends in part on the scope and seriousness of the market failure, the desired intervention, the importance of the product or the service and the specific form the relationship with other parties in the sector takes.

...balance between robustness and flexibility

When formulating measures, the question of the level of robustness required for the measures is one that continually comes up. After all, if this is a temporary risk, an incidental risk or a feeling that a threat exists, when in fact it does not, this will impose constraints on the measures to be taken.

Thus, it may be completely legitimate from the perspective of the policy advisor to take symbolic measures at any time because such measures will increase the public's sense of security or, in other words, manage public confidence. Such actions make people and organisations feel safer. It may also be logical to choose measures that can be adjusted at any time or that involve fallback options. These are so-called “no-regret measures” - measures that are robust and sensible in (almost) all future scenarios. This can be desirable in the case of incidental risks.

A good policy advisor explicitly determines the level of robustness and flexibility required for the measures that must be taken.

...take the differences between a dynamic and a static market into account

When conducting a risk analysis and formulating and evaluating measures, it is important that the policy staff take the characteristics of the sector involved into account. One of the most important characteristics of a sector for risk analysis purposes is its level of dynamism.

The energy market and telecommunication market are examples of the two extremes here. The energy market is a relatively static market. As a product, energy has virtually no possibilities for development (with the exception of added features like freedom of choice and service). However, in the telecom sector, growth and innovation is largely due to digitising and standardising Internet technology. New products such as digital television, VoIP and RFID are appearing on the market and consumers are gradually replacing old technologies by new ones. There is nothing that resembles this kind of product development in the energy market.

When conducting a risk analysis or developing and evaluating measures, the aspect of dynamism must be taken into account. The life expectancy of a risk analysis in terms of developments or threats for the telecom sector is likely to be considerably shorter than a comparable one for the energy sector. After all, the introduction of new technologies can create new threats. On the other hand, the arrival of these technologies may reduce vulnerabilities as a result of redundancy. This also affects the life expectancy of risk analysis. Moreover, the difference in the level of dynamism in the different sectors also requires a different type of harmonisation of measures.

...links between management of public confidence and awareness

Policy staff not only has to deal with actual risks; they also have to deal with the perceived risk of citizens and companies. There are threats and risks that in actuality are small, but which citizens and companies can experience as significant. That raises difficult questions in terms of dealing with such threats. On the one hand, one can elect to ignore the experience and perceptions and only respond based on the actual risks (and thus allow unrest and disaffection among citizens and companies to well up and grow). On the other hand, one can elect to base government actions on the philosophy that one of government's specific objectives is to take different perceptions and possible feelings of insecurity on the part of its citizens into account.

A number of perspectives regarding action are relevant based on this second philosophy. After all, increasing citizens' sense of security requires managing public confidence. The government must also indicate when citizens have no cause to worry about an issue, when the risk is rather small or when one must accept the fact that a genuine risk exists. However, the consequence of this can be that the citizen is less cautious and that citizens stop taking precautionary measures that they took in the past. In turn, this increases the risk, which can be one reason for managing public confidence or making citizens aware of the risks.

Effective policy staff will strike a balance between management of public confidence on the one hand and management of awareness on the other.

...balances between new measures and best-practices

Risk analyses and new, supplemental measures are not always needed to eliminate existing risks. One statement made regularly is that the systematic application of existing measures or best practices (such as the timely use of software patches[2], the use of an up-to-date virus scanner and firewall and the use of the Code for Information Security by companies) would eliminate 80% of all risks. Supplemental measures may be required for the other 20%.

That means that good policy staff must meticulously weigh more frequent application of best practices on the one hand against the implementation of new measures on the other.

A GOOD RISK ANALYST....

A number of important points of attention that are involved from the perspective of a good risk analyst are described below:

...consciously choose either a scenario and/or an effect to be prevented as your starting point

There are two primary approaches for conducting a good risk analysis.

[2] Patches are modifications of existing software that eliminate errors or bugs in the software.

The first approach is to specify threat scenarios and initial events and then determine the consequences of these scenarios and events would have. Based on the analysis of the consequences, measures can then be formulated.

A second approach starts not by determining the threat scenarios and initial events that might cause a malfunction, but by formulating situations that must be prevented: worst cases or 'situations to be prevented and maximum effects'. Then one works backwards from the consequences. What circumstances, events or causes could create such a situation? Finally: what measures can be used to prevent these circumstances?

The second approach fits in with the line of thinking that argues that there are thousands of threat scenarios, and that it would never be possible to come up with a complete image of the threats, that trying to come up with all these scenarios is a time-consuming affair and that ultimately this does not result in the formulation of measures that actually prevent the worst case scenarios. Based on this philosophy, it is more effective to simply start with the worst cases – situations with consequences that absolutely must be prevented – and to work backwards from these situations. That does not mean that an approach via the scenarios and initial events would not be effective: it is a question of setting the right priorities for the different options at the right moment.

The following diagram systematically summarises the advantages and disadvantages of these two perspectives:

	'Scenarios and initial events' approach	'Situations and worst case consequences to be prevented' approach
Advantages	• Less obvious scenarios are also included in the analysis.	• Pragmatic approach because only those situations that demand action are studied.
Disadvantages	• Because there are an infinite number of possible scenarios there is the risk that a scenario that could have a significant effect is overlooked. • Scenarios are studied that do not have serious consequences. One can get lost in an unnecessarily large number of scenarios. • This approach can also be unnecessarily time-consuming.	• Based on this perspective, not all scenarios or initial events are studied.

A good risk analyst makes a conscious and explicit choice between these two approaches or combines the two approaches and can explain and justify that choice.

...consciously choose a qualitative and/or quantitative analysis

Many methodologies and conceptual models that are described in this manual allow the user to choose between conducting either a qualitative or quantitative version. Each version has both advantages and disadvantages:

	Qualitative analysis	Quantitative analysis
Advantages	• Requires less effort	• Requires more effort
Disadvantages	• Precision and accuracy levels may not be satisfactory	• Danger of creating a false sense of security

If risks are calculated to three places after the decimal point using quantitative methods, for example, one quickly has the sense that a high level of exactitude and accuracy has been achieved. However, that sense of accuracy can also be false, e.g. because it is based on all sorts of assumptions made during the analysis and on a clustering of subjective opinions. That requires nuances and recognition of the existing uncertainty.

Depending on the objective of the analysis and the involvement of experts, a good risk analyst meticulously weighs a qualitative versus a quantitative approach.

Sometimes, quantitative data are not available. In the case of people trying to escape from a tunnel, for instance, satisfactory data may be unavailable, but the behaviour of the people involved largely determines the consequences. In this case, the risk analyst has no choice.

... consciously choose classification and/or ranking

Once identified, risks can then be prioritised. Various techniques are available for doing this. Two recognisable techniques are classifying and ranking the risks.

When classifying risks, the risks are divided into categories, e.g. the category 'significant risk'.

When ranking risks, the risks are considered in relation to one another. The risk analyst arranges the risks in order of importance or likelihood. This is called simple ranking. Another version of ranking is paired ranking, which involves comparing a series of pairs of risks. In other words: each risk is compared to every other risk, specifying which of the two is greater.

Moreover, ranking can be performed in a qualitative or a quantitative manner. In the quantitative approach, the risk analyst also specifies how much greater the likelihood is that one risk will occur rather than another (instead of simply saying that one risk is more or less likely than another).

The advantages and disadvantages of classification and ranking are shown in the following table.

	Classification	Ranking
Advantages	• Simplicity (also in the case of large numbers of risks)	• Allows explicit and thus meticulous weighing
Disadvantages	• Because this system works with a limited number of categories, the analyst is sometimes compelled to place two risks in the same class, even though it can clearly be indicated that one of the two is more likely to occur than the other.	• Not suitable for larger quantities of risks • In the case of paired and/or quantitative ranking, computer support is an absolute plus (particularly due to the fact that participants are not always consistent in their evaluation of paired comparisons)

The four types of ranking differ from one another, particularly in terms of 'accuracy' and the amount of effort required to perform the ranking.

Ranking	Qualitative...	Quantitative...
Simple ...	Type 1: • Least accuracy, least amount of effort required.	Type 2: • Average accuracy, average amount of effort required.
Paired ...	Type 3: • Average accuracy, average amount of effort.	Type 4: • Largest degree of accuracy, most effort required.

The choice between type 2 and 3 depends in part on the number of risks being weighed. The efforts involved in paired ranking mount up quickly if the number of risks is large. For example, with 7 risks, 'only' 21 comparisons have to be made, while 20 risks requires 190 comparisons!

More information about applying the different types of ranking can be found in the description of these models in Paragraphs 4.3.4 and 4.3.5.

A good risk analyst must be aware of and carefully consider the available options. Ranking generally requires more extensive analysis; the analyst must determine whether the additional accuracy warrants the extra efforts.

...does not disguise a lack of certainty, but makes it transparent

In risk analyses, the goal is often to achieve uniform outcomes: for example, the likelihood that a specific situation will occur must be specified. The attempt to arrive at consensus and to achieve uniformity is the focal point. The danger is that in striving for consensus, the outcome can be a give and take between two randomly selected experts, which results in the estimated risk of occurrence being taken as a certainty, while in fact, it is not certain at all. Failure to distinguish that uncertainty can then have an undesirable effect on the analysis.

This is also referred to as the phenomenon of 'reproducibility'. If the same analysis is conducted a second time, how great is the chance of the outcome being the same or corresponding closely enough to the first outcome that the ultimate outcome of the risk analysis is the same in terms of possible measures?

A good risk analyst ensures that uncertainty during the analysis remains transparent, particularly if quantitative methods that could create a false sense of security are used.

...work cyclically and iteratively rather than chronologically

A strict, rigid step-by-step plan is often used when conducting risk analyses; the first step must be completed before the subsequent step can begin. Many risk analyses require that the possible scenarios that can arise be plotted (step 1), after which the effects of those scenarios are plotted (step 2), and finally possible measures are specified (step 3). Each of these steps might take half a year, but you are not allowed to think about step 3 (formulating measures) while you are still working on step 1.

What occurs in such a strictly chronological process is that a great deal of information is lost. After all, when studying the threat scenarios and vulnerabilities, solutions for eliminating those vulnerabilities will obviously come to mind. By organising these steps as separate units, one runs the risk that the only result of the vulnerability analysis is an indication of vulnerability and that all the information regarding measures that came up as the vulnerability was being analysed is lost. Once it is time to formulate measures, all of the suggestions made during the process have been lost because people have been replaced or simply because they were never written down. Then the measures in the last phase have to be pulled out of a top hat.

A good risk analysis project leader is aware of this phenomenon and attempts to work much more cyclically and iteratively rather then chronologically, and also attempts to collect interim results and to record things during the process so that ideas are not lost. Moreover, speaking about measures early in the process makes it more probable that both sides of the argument will be heard. For example, the parties involved can indicate that a suggested measure can better be replaced by another measure that is more cost-effective. It is better to conduct such discussions earlier in the game than at the last minute, when there is little time or space for such discussions.

... sometimes conduct a quick scan, but sometime look for depth

In many cases, a risk analysis process can be characterised as a funnel: first, an initial inventory is obtained via quick scans and the breadth and variety is mapped out. Then, the in-depth effects are worked out logically.

Depending on the objective of the analysis, one can choose a specific level of depth. Sometimes, for example, measures are so expensive that an in-depth study of the desirability of the measure is warranted.

A good risk analyst carefully evaluates the level of depth, while also devoting attention to the process after a quick scan, where attention is required.

A good 'risk analysis process leader'...

Important points of attention related to the perspective of a good process leader are discussed in this section:

...respects and anticipates 'coloured' input

The parties involved – such as companies or public managers of infrastructures and objects – have both a position and an interest in the risk analysis process. What they contribute to such a process can depend in part on the role they fulfil: 'Where you stand depends on where you sit'. To prevent the government from adopting new legislation or to avoid being assigned extra duties ('draw up a security plan that is periodically updated as required' or 'the obligation to be certified in a specific domain'), the parties involved will tend to participate based on that interest. This can lead parties to consciously or unconsciously downplay certain risks, while overemphasising others, e.g. because other parties are responsible for those risks, or to try to get extra government resources allocated to improving the safety or security of their particular product or service (which then strengthens their competitive position internationally). This sort of game can also come into play when formulating measures. Parties will be more likely to plead for measures whose costs are borne by others, but from which they themselves profit, than to promote measures for which they will have to bear the costs. For example, regional network managers can argue that investments in the quality of the high voltage network – which is under Tennet's management - are required in order to increase delivery security and that extra investments in the regional networks that they themselves manage will result in little improvement in terms of promoting continuity. Internet service providers emphasise what the end-user himself can do to protect himself, e.g. installing antivirus software. In other words: parties will have a tendency to support measures in another part of the industrial column or measures that must be taken by other parties. In that framework, further disentanglement of sectors like energy and telecom are relevant as well. This changes the industrial column from a (vertically) integrated monopoly to a market with different layers in which there is room for competition and in which a multitude of companies (public or not) are collectively responsible for the product or the service: from infrastructure managers to producers, from suppliers to intermediaries.

In addition, a good process leader realises that, to a large extent, the outcomes of a risk analysis result from the models applied, the parameters selected and the parties who implement the measures. After all, the input – what you put into the model - determines the output: what comes out of the model.

A good 'risk analysis process leader' respects the fact that the parties involved participate based on their specific interests and does not attempt to prevent this, but rather to utilise this fact productively. This can be done, for example, by asking the parties involved from the sector about measures to be taken by others in the sector rather than the party suggesting the measure.

...prevents group think and promotes hearing both sides of the argument

In a work form such as an expert meeting, the chance of 'group think' is considerable. The party who is first to say something about the nature or scope of a risk, for example, is deemed correct. The other parties involved do not have arguments at hand that enable them to enter the discussion, even though their own estimate of the nature or the scope of a risk may be completely different. A good 'risk analysis process leader ' prevents and attempts to anticipate the phenomenon of group think, e.g. by ensuring that assumptions are discussed, that counter-arguments are organised, that both sides of the question are heard and that critical questions are asked. Concretely, this can be accomplished by getting an option from an expert with opposing views, getting a second opinion, or by organising knowledge competition: asking two or more renowned experts or institutes to offer an option based on their vision.

This makes it possible to replace 'negotiated nonsense', which can be the consequence of group think, by 'negotiated knowledge': negotiated knowledge that becomes available by confronting the arguments. And where parties do not agree with one another, this must not fall into oblivion, but must be recorded: agree to disagree. This is necessary in order to be able to properly deal with the subsequent steps of the analysis.

For that matter, before such a group process one can try to ensure that both sides of the argument are heard, e.g. by inviting the parties involved off the record, by ensuring representation from the different links in the

industrial column or the government column (policy, execution, supervision/inspection) or by ensuring that several experts from a specific domain always participate so that genuine discussion takes place rather than an oration by a single expert. In this way, the subjective opinion of an individual can be objectified through consultation with others.

…create a good process design with 6 elements in advance

A good 'risk analysis process leader' pays attention to the process of creating a risk analysis. In any case, the 'risk analysis process leader' must ask the following six questions:

What is the objective of the risk analysis?

a. What is the objective in terms of the content of the analysis? For example, to determine the likelihood that a specific risk will occur, conduct an extensive risk analysis from beginning to end, perform a quick scan or (e.g.) plot existing measures and then evaluate them?

b. What is the objective in terms of process? For example, to provide an answer to a question from the Lower House, to provide an analysis in the framework of the Protection of Vital Infrastructures Project, to stimulate action in the sector, etc.

What phases can be distinguished in the process of that risk analysis?

What parties must be involved in the process?

a. In what phases?

b. From what role?

c. With what tasks, authorities and responsibilities?

What methods and work forms can be used?

What tools are needed to achieve the desired result (time, money, energy)?

What rules apply in the process? For example:

a. Rules for decision-making: who decides?

b. Rules for dealing with (confidential) information: how are parties informed and how is communication handled?

c. Rules regarding joining and leaving the process: who may participate in discussions or decision-making, and can parties voluntarily withdraw from the process?

d. Rules for conflict resolution: how are differences of opinion dealt with?

e. Other rules

Involving parties

As is evident from these questions, other parties must be involved as well. For example, parties who are able to contribute their knowledge (scientists) to the content of the analysis, parties who have a special interest in terms of the outcomes of the risk analysis (those who cause the risk and those who must bear the consequences of the risk), parties who will be called to account if the risk actually manifests (e.g. governments), parties who will profit from specific measures (such as accounting firms, security companies, quality certification agencies and insurance companies). Parties who are able to implement the measure or block such implementation.

Roles of parties: participate in decision-making, participate in discussions, and receive information

For each of the parties involved, the role that party can and is allowed to play in the risk analysis must be specified. Three main roles are distinguished: shared decision-making, mutual consultation and information exchange. Below a number of keywords are listed for each role.

Shared decision-making:

- Make decisions
- Approve or reject
- Contribute binding proposals
- Evaluate proposals
- Translate insights into a decision
- Veto a decision
- Etc.

Mutual consultation:

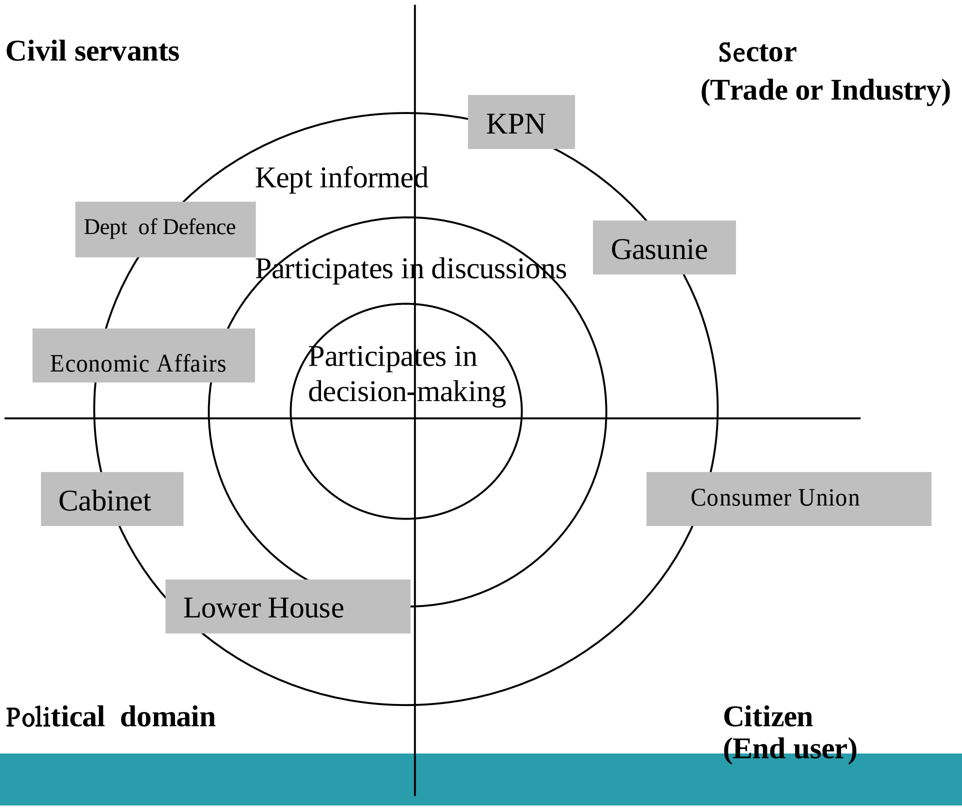
- Contribute a non-binding proposal
- Make suggestions in harmonisation with others
- Contribute knowledge and expertise
- Be consulted
- Etc.

Information exchange:

- Be informed

Different roles in the different phases

The role of a specific involved party may vary depending on the phase in which the risk analysis takes place. Thus, it may make sense to initially designate a party as one that is kept informed, but then at a later phase (e.g. when input for the risk analysis has to be collected) allow that party to participate in discussions.



Moreover, it may be sensible to involve parties who will be charged with implementing measures once the risk analysis is completed in weighting the possible measures in a timely manner and to have them 'share in decision-making' in that capacity. This may help ensure the cooperation of these parties at a later stage.

A good 'risk analysis process leader' will ideally specify what role each party plays in each phase of the process. The figure above can be useful in this context. The figure distinguishes four types of involved parties: civil servants, political figures, the sector and end users.

Notes regarding the figure: A good 'risk analysis process leader' specifies what parties are involved in what roles for each phase. As an illustration, several parties are mentioned in the figure. The role fulfilled by each party is specified: information exchange, mutual consultation or shared decision-making.

... simultaneously manages based on contents, progress and broad-based support

Contents, progress and broad-based support are all important, but in practice these are at odds with each other. Analyses that involve good content cannot always count on sufficient broad-based support. Attempts to win broad-based support can lead to a clumsy negotiation process in which people are so afraid of offending other parties that they actually inhibit the desired progress. Conducting a speedy process can have consequences for the depth at which the contents can be analysed. Sometimes, a quick scan is the most that can be achieved given the ambitious time schedule. Sometimes, too much emphasis on progress can lead to the need to make assumptions regarding matters that should have been worked out in detail and specified, or in the inability to gather information that is less readily available due to a lack of time.[3]

A good 'risk analysis process leader' tries to ensure that the outcomes of a risk analysis are robust, realised within the desired time span and can count on the maximum feasible level of broad-based support.

...see the process as the prelude to broad-based support and implementation

In most situations, the recommendation is not to wait until the last minute to inform the parties involved of the results of a risk analysis, but to include them in the process in a timely manner and allow them to influence the outcomes of that process (naturally without jeopardising the special responsibility the government has for coming up with measures). After all, giving parties influence over the outcome of such a process enables them to commit to the outcome at an earlier stage.

Moreover, by consciously involving specific parties in the risk analysis process, not only can broad-based support be developed for measures that may have to be taken, but the awareness of the parties regarding risks is also increased. Such awareness can already be a result in itself, e.g. because a party follows up within his own organisation. Thus, the involvement of these parties is extremely relevant.

However, involving parties is no cakewalk. Choices must be made. After all, many parties maintain special relationships with one another. For example, consider the delivery and regional network companies that are organisationally separate from one another, but are still part of one enterprise.

A good 'risk analysis process leader' utilises the process as the prelude to implementation.

[3] De Bruijn, Ten Heuvelhof, In 't Veld, Process Management; about process design and decision-making, Schoonhoven, 1999

MANUAL: NOT A STRAIGHTJACKET, BUT AN AID

THE HOW QUESTION AND THE WHAT QUESTION

This manual offers an interesting and extensive overview of methodologies and work forms.

But this manual must also enable you to determine on a case-by-case basis what (mix of) risk analysis methods and work forms can be most appropriately applied in what situation. After all, how can policy staff choose the right methodologies and work forms from the variety described in this manual?

Methodologies and work forms come in many types and sizes. They each emphasise different factors and each is (more) appropriate in different situations. Sometimes they are appropriate for the initial phase of the risk analysis process, sometimes for the final phase. Some methodologies and work forms are more appropriate for a quick scan-type approach, while others lend themselves better to more in-depth analysis. Some work forms are appropriate for brainstorming, others for decision-making. Some methodologies are appropriate for a quantitative approach, others are not. Some methodologies lend themselves well to group processes and interaction, while other methodologies are particularly appropriate for the 'expert-behind-the-desk' approach.

The combination of methodologies and work forms to be chosen is important here. After all, sometimes different models are complementary, helping to flesh each other out. But sometimes methods overlap and do not lend themselves to use in combination with certain other methods. This is specified for the individual models.

The 'How-question' involves the approach and work forms to be chosen from among those included in this manual. Is the sector involved or not? Are interviews conducted or plenary brainstorms? And so forth. The answer to this question depends on the objective of the analysis. This is further discussed in Paragraph 3.2.

The 'What question' involves the risk analysis methods to be chosen from among those presented and clarified in this manual. What methodology must be used to identify threats or to arrange them in order of importance? What methodologies help to expose the level of resistance existing systems offer? What methodologies must be used to gain insight into the cost/benefit ratio of possible measures to be taken? And so forth. This is further discussed in Paragraph 3.3.

'HOW QUESTION': DIFFERENT PROCESS-ORIENTED OBJECTIVES, DIFFERENT APPROACHES AND WORK FORMS

Different process-oriented objectives...

It is important that the Ministry of Economic Affairs have insight into the risks that threaten the proper functioning of telecommunication and energy provision in the Netherlands. This insight is needed so that decisions can be made based on careful considerations and priorities can be set for the measures that may have to be taken. The complexity of the facilities involved, the rapid technological and market developments, the dependencies between various systems and the changing threats all combine to make it more difficult to gain insight into risks and to make decision-making regarding measures more complicated. This situation compels the ministry to update and improve its knowledge of methods and analytical techniques, so that the decision-making process for risks can be supported as optimally as possible given the circumstances.

The use of the methodologies from this book can be prompted by any number of objectives, which must sometimes be realised in combination with one another. A number of these are discussed below, though the list makes no pretence of being complete:

- Formulating packages of measures in the framework of the Protection of Vital Infrastructures Project.
- Developing broad-based support for measures to be taken.
- Creating awareness and stimulating action in the sector.

- Setting up relationship management because lengthy relationships with interested parties from the sector are involved.
- Responding to questions from the Lower House as accurately and as quickly as possible.
- Conducting tests if new information comes to light or new insights arise in the course of the process.

These objectives may conflict with one another. For example, a quick, but incisive answer for the Lower House may be at odds with developing broad-based support for measures that must be taken. That also means that meticulous evaluations must be made.

Different approaches and work forms

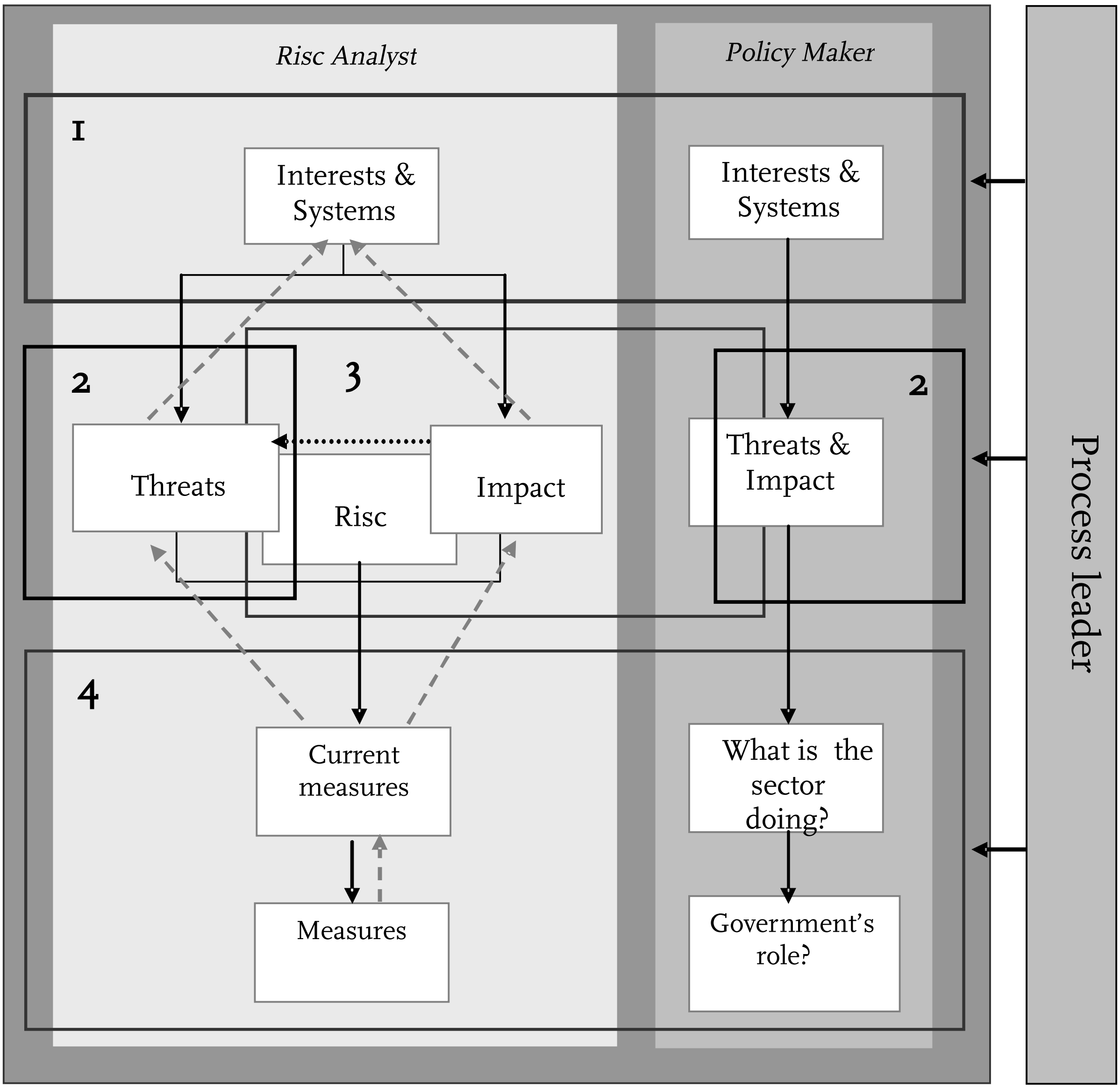
In the case of different objectives for the risk analysis - as described above - different methodologies and work forms are also appropriate. Based on the objective mentioned in the previous paragraph, three relevant types of objectives can be distinguished. The possible consequences resulting from the use of methodologies and work forms are specified below for these types of objectives.

- Type 1: If the objective is to formulate packages of measures in the framework of the Protection of Vital Infrastructures Projects, the obvious solution is to conduct an extensive, in-depth analysis because there is sufficient throughput time to do this. It is also obvious to investigate how different products and services depend on one another, because it is in precisely this domain that Protection of Vital Interests offers added value. Methods such as a 'dependencies model' are appropriate here. There is also room to incorporate a process in which the knowledge and expertise of the sector is involved. That, in turn, requires work forms that facilitate such interaction, such as expert meetings. This type also lends itself specifically to the risk analyst's perspective.
- Type 2: If the objective is to develop broad-based support for measures to be taken, to create awareness, to stimulate action in the sector and to set up relationship management, it is clear that the sector should be involved at an early stage of the process and that work forms that make this feasible should be adopted. This type particularly lends itself to the process leader's perspective.
- Type 3: If the objective is to respond to questions from the Lower House as quickly and incisively as possible, desk research is the obvious choice, possibly in combination with the help of experts called in from inside and (perhaps) outside of the government. This type lends itself to the policy staff's perspective.

'What question': different objectives, different methodologies

The 'What question' involves the risk analysis methods to be chosen from among those presented and clarified in this manual.

Here, a distinction is first made between the types of comprehensive method that can be employed by the risk analyst and the policy staff. The comprehensive method is shown in the following figure. The figure shows that four steps to be taken by the risk analyst and policy staff share certain similarities, but also reflect certain differences. In describing the comprehensive method from these two perspectives, four different phases are clarified and questions are formulated that can be asked during these phases. The models and methodologies that can provide support are explained for each of these questions.



Moreover, the figure gives the impression that existing measures are only mapped out during the final phase of the risk analysis. However, when estimating risks, naturally existing measures are implicitly taken into account. This has been positioned in step 4 because in many cases the models with which existing measures are mapped out are the same models that are used to analyse supplemental measures. Moreover, a systematic and extensive analysis of all existing measures is needed during the final phase because without insight into these measures, it becomes much more difficult to formulate supplemental measures.

The model suggests a specific sequence when working through the different steps and, in turn, when applying methodologies and models. However, this sequence is not strictly necessary. The risk analyst, policy staff or process leader can also work cyclically or iteratively, simultaneously using models and methods from different phases. For example, the figure shows that steps 2 and 3 can be performed simultaneously and overlap to a certain extent. The models and methodologies applicable to these two steps can thus be applied simultaneously and are also interchangeable. That is to say, a number of the models and methodologies from Phase 2 can also be applied Phase 3 and vice versa, though the form may have to modified to a certain extent.

Different models and phases are frequently combined in a risk analysis. For example, consider the perspective by which interest, threat and resistance are analysed simultaneously; such a model is used by the General Information and Security Service (*AIVD*) and the National Coordinator for Combating Terrorism as well as by several ministries in the framework of the Protection of Vital Infrastructures Project.

Comprehensive method for the risk analyst

The Comprehensive Method for the risk analyst is based on the different phases that can be distinguished in the risk analysis process. The literature dealing with risk analyses uses different standards for the phases in a risk analysis process. Concepts such as threats, vulnerabilities, resistance and impact thus take on different meanings. The Comprehensive Method proposed here gives a clear image of the sequence of the different steps that can be distinguished for a risk analysis, but must be considered as one of the possible approaches.

In the Comprehensive Method, four phases are distinguished for the risk analyst:

1. Analysis of vital interests and systems: models and methodologies with which vital interests and systems can be mapped out. Moreover, attention is devoted to the products and services these interests involve and the processes and nodes that are relevant for producing these products and services.
2. Identifying threats: models and methodologies with which threats can be identified. Here attention is devoted to the dependencies of other vital products and systems.
3. Evaluating and prioritising impact: models and methodologies with which risks and consequences can be evaluated and prioritised. Furthermore, different likelihood-effect analyses and analyses of vulnerability and resistance are involved.
4. Formulating, evaluating and implementing measures: models and methodologies with which existing measures can be mapped out, new measures can be formulated and evaluated and their implementation can be monitored. Furthermore, attention is also paid to broad-based support and the costs and benefits of the various measures.

For all phases, the choice of a specific model or a specific work form depends on factors such as the time available, the requisite input of knowledge and expertise from experts and the available tools in terms of manpower (FTEs) or money.

Different questions play a role in each of the four phases of the risk analysis. When answering these questions, different models and methodologies can provide support. Below, questions are formulated that may be useful during the four phases of the risk analysis; the corresponding models and methodologies are also mentioned.

1. *Analysis of vital interests and systems*

This phase involves analysing the vital interests, products & services, processes & nodes and their context. Questions that may be useful and the corresponding models are listed in the following table.

Questions regarding vital interests and systems	***models***
What are the vital products and services?	2.2.1
What situation do we want to avoid?	2.3.1
What does the sector and the relevant environment look like?	1, 3, 5, 6
What are the relevant processes and systems for producing these products and services?	2, 6
What are the relevant (geographic, physical or virtual) nodes for producing these products and services?	1, 4
What parties are responsible for these processes, systems and nodes?	1,6
What layers can be distinguished in the industrial column?	1
What external developments may lead to vulnerabilities?	2, 5
What are the underlying dependencies between the vital products and services?	4, 6

2. *Identifying threats*

This phase involves analysing the threats and dependencies. Questions that may prove useful and the corresponding models are listed in the following table.

Questions regarding identifying threats	***models***
What (types of) threats may arise?	7, 14, 15, 18,19,20
What are the (types of) vulnerabilities in the current situation?	7, 9, 15, 16
What level of resistance to these threats do the existing systems offer?	17, 30
How can (the nature of and likelihood of) deliberate human action be mapped out?	8, 12, 13, 15
In what management area do the threats appear?	14
How can these threats be evaluated and prioritised in relation to one another?	10, 11

3. *Evaluating and prioritising the impact*

This phase involves analysing the likelihood that the risk will actually occur, the consequences should it occur and the vulnerabilities and level of resistance. Questions that may prove useful and the corresponding models are listed in the following table.

Questions regarding evaluation of and prioritising the impact	***models***
How can the impact be mapped out?	18, 19, 21, 24, 25
What (types of) effects can occur?	16, 22, 26
What are the most relevant likelihood-effect combinations?	23
In what management area do the effects appear?	27
What does the recovery time mean for the scope of the damage?	25

4. *Formulating, evaluating and implementing measures*

This phase involves analysing the existing and requisite measures and the fields of influence in which realisation must occur. Questions that may prove useful and the corresponding models are listed in the following table.

Questions regarding formulating, evaluating and implementing measures	***models***
What types of measures can be distinguished?	28
What existing measures have already been taken?	29
What supplemental measures are required?	38
In what fields of influence must measures be implemented?	31, 33, 34
How extensive are the costs and benefits of different measures?	35, 37
What parties do those measures affect?	28, 29
For what measures can you count on broad-based support and for what measures can you not count on such support?	30, 32, 33, 37
How well can the measures be enforced?	39, 40

How can the measures be compared?	36, 38
What approach can be used to monitor the implementation of the measures?	41
How robust are the measures in time?	20
To what extent does a measure fit in with the features of the market?	2.2.4, 25

Comprehensive Method for policy staff

The Comprehensive Method for the policy staff has many point of similarity with the methodology for the risk analyst. Initially, the policy staff also investigate vital interests, systems and inventories and in the second and third phase also analyse the threats, risks and impact. In the fourth phase, just as for the risk analyst, the focal point is formulating, evaluating and implementing measures. However, the underlying questions that play a role for policy staff during this phase are of a higher (political-administrative) level of abstraction than those for the risk analyst. In this phase, the policy staff first asks to what extent the sector itself is already taking measures to manage specific risks, whether these are adequate and acceptable and what the (supplemental) role of the government should be.

The following four phases can be distinguished in the Comprehensive Method for policy staff:

1. Analysing the vital interests and systems: models and methodologies with which vital interests and systems can be mapped out.
2. Identifying the threats: models and methodologies with which threats can be identified.
3. Evaluating and prioritising the impact: models and methodologies with which risks and consequence can be evaluated and prioritised.
4. What is the sector's task and what is the responsibility and task of the government in light of the importance to society and in light of market failure. This phase involves using models and methods for mapping out what risks have already been mitigated by the sector and how. Furthermore, attention is devoted to different levels of intervention and different role patterns.

Because the applicable questions and models for phases one, two and three have already been mentioned, the following table only lists the questions and corresponding models for the fourth phase of this risk analysis.

Questions regarding risks covered or to be covered by the sector and the role of the government	***models***
Is a societal or public interest involved?	2.2.1
Is there a market failure?	2.2.1, 37
Is a role for the government desirable or not?	2.2.1, 30, 37
What role must the government take? How extensive must this role be?	2.2.2
What interventions can the government take? What management and control method can the government use?	2.2.2, 28, 29
What risks is the sector already covering? How does the sector do this? Are these measures effective?	27, 28, 29
What incentives does the market have for taking measures?	2.2.2, 37
What other reasons are there for a government role (e.g. setting a good example)?	30, 3.2.2

METHODOLOGIES AND CONCEPTUAL MODELS

Introduction

This section deals with a broad range of methodologies and conceptual models. The format for this section is based on the four types of methods and models as these are distinguished in the different consecutive phases of a risk analysis. First of all, the models and methodologies with which vital interests and systems can be mapped out are described. This is followed by an inventory of models and methodologies with which threats can be identified. The following paragraph contains models and methodologies with which risks and effects can be evaluated and prioritised; the section then ends with a description of models and methodologies with which existing and supplemental measures can be mapped out.

In each paragraph, a distinction is drawn between classifications and checklists on the one hand and conceptual models on the other. If classifications and checklists are involved, categories are proposed with which events, chances, consequences or measures can be mapped out. If conceptual models are involved, a description of the essence of the model is offered, as well as the steps that can be distinguished in applying the model (and the preparation and any subsequent steps), a checklist of conditions for applying the model and finally the sources that point the reader to literature where additional (background) information can be found.

1 Layer models

Essence

A realistic description of a vital sector can be drawn up based on the realisation that the sector consists of various sub-markets or layers. Collectively, these sub-markets constitute the industrial column. The Bits & Pieces Model shown in the figure is an example of such a layer model. It clearly depicts the vertical dependencies of a service or sector, in this case the ICT sector. By sub-dividing the sector into sub-sectors when describing a specific sector, a layer model provides insight into the market and simplifies and thus helps focus the analysis in a later phase. If the same exercise is performed for other products, services or sectors, the horizontal dependencies (dependencies between infrastructures from different sectors) can also be charted. For example, there is a connection between electricity production and the availability of oil; after all, the price of electricity is linked to the price of oil.

Preparation, steps and follow-up

The following steps can be distinguished when using the layer model.

Step 1. Define the Scope

Many infrastructure-dependent sectors (such as the ICT sector shown in the figure) consist of a complex, intertwined mesh of networks and services, in which different layers can be distinguished. First of all, the sector, sub-sector or service for which a layer model is to be developed must be specified. For example, is this the telecommunication market, the service telephony or the Internet? Once a clear scope is defined, the different layers may be charted.

Step 2. Describe the layers

For the electricity sector, a distinction is generally made between production, transport, distribution and delivery. For gas and oil, storage is added as a layer. For telecommunication, the layers are classified as infrastructure, transport, teleservices and added value services.

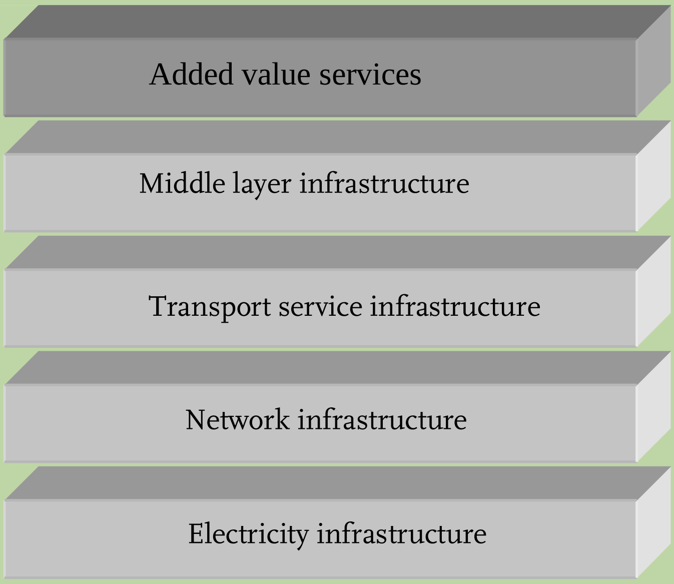
The *Bits & Pieces Model* – used as an example in the figure - describes the different layers for the ICT sector as follows:

1. First of all, the model assumes that electrical power must be considered as an underlying foundation for all ICT services.
2. Above this is the network infrastructure. This consists of information transmission provision facilities such as glass fibre, cable and radio and TV transmitters.
3. The following layer consists of transport services such as telephony, Internet and television distribution. These services are supported by different suppliers and use different underlying infrastructures.
4. Above the transport services is the infrastructure middle layer. This layer contains the added value services that facilitate the lowest layer.
5. The top layer consists of the added value services. Examples include domain name services, voice mail, SMS and Internet servers.

Furthermore, there is another version of the layer model - the OSI Model (Open System Interaction) - that is frequently used in the ICT sector to map out network traffic.

Step 3. Position the actors and show the geographic dimension

After the different layers are selected, the actors can be filled in. For example, if there are four electricity producers in the Dutch market, four circles can be drawn on the production layer representing these four producers. If these producers are also suppliers, the diagram must clearly depict this.


Added value services
Middle layer infrastructure
Transport service infrastructure
Network infrastructure
Electricity infrastructure

This makes the institutional relationships in the sector clear, the layers at which parties are active (and what sort of anti-competitive behaviour that can stimulate against other parties), and where monopolies or oligopolies exist. The geographic distribution per layer can also be depicted. After all, some actors are also suppliers, the diagram must clearly depict this.

This makes the institutional relationships in the sector clear, the layers at which parties are active (and what sort of anti-competitive behaviour that can stimulate against other parties), and where monopolies or oligopolies exist. The geographic distribution per layer can also be depicted. After all, some actors are only active in a specific region, for example, regional network managers in the electricity network.

In addition, it is frequently quite useful to create a dimension model (described in the next section) after the layer model has been created. The dimension model enables the analyst to describe the layer (or activity) using three dimensions.

A layer model can be constructed in an infinite number of ways: this depends on how many layers are distinguished in the industrial column. In principle, no group process or expert meeting is required for this: desk research is sufficient, perhaps combined with a number of interviews. Naturally, the picture constructed using desk research constructed can then be tested in the sector.

Checklist of conditions

When using models, it is important not only to consider the separate layers, but also the links between these layers. These links are also referred to as the interfaces. After all, important risks may lurk in these interfaces, particularly because they can fall into a responsibility vacuum.

If desirable, the description of the model can be detailed per layer at a later stage by further sub-dividing a layer into sub-layers. This can be done by designating sub-activities. The more detailed the layers, the more precision the analysis can deliver.

Sources

’‘Dunn, M., Wigert, I. CIIP Handbook 2004, Critical Information Infrastructure Protection, An Inventory and Analysis of Protection Policies in Fourteen Countries’.

Council for Traffic and Communications, *Tussen droom en draad*, 2003 (see www.raadvenw.nl). This was a preliminary study, published in 2004, conducted by Berenschot for the recommendation ‘*Hoezo marktverwerking*’.

External Input Model

Essence

The external input model shows an overview of all streams and external influences that affect a system (object or node) and can thus constitute a risk for the functioning of the system..

Preparation, steps and follow-up

As an example, the figure shows a generating plant system. The external input model uses the principles of the SADT method (Structured Analysis and Design Technique). This is a method by which the transformation of inputs to outputs in a specific system is mapped out. Here a distinction is made between the activity (in this case ‘electricity production’), the mechanisms (employees, machines), the inputs (raw materials, ICT services, energy) and controls (protocols or regulations). The controls regulate the system, the mechanisms support the activity and the inputs are converted into outputs.

The system depends on all incoming arrows (controls, mechanisms and inputs), which makes the corresponding risks understandable. For example, disruption of an input constitutes a risk, but errors in the existing regulations and protocols that are intended to control the activities in the system can also pose a risk and must be prevented.

Checklist of conditions

Using this model requires a certain amount of expertise. Involvement in the sector when applying this model is also a condition in order to ensure that the requisite knowledge is incorporated.

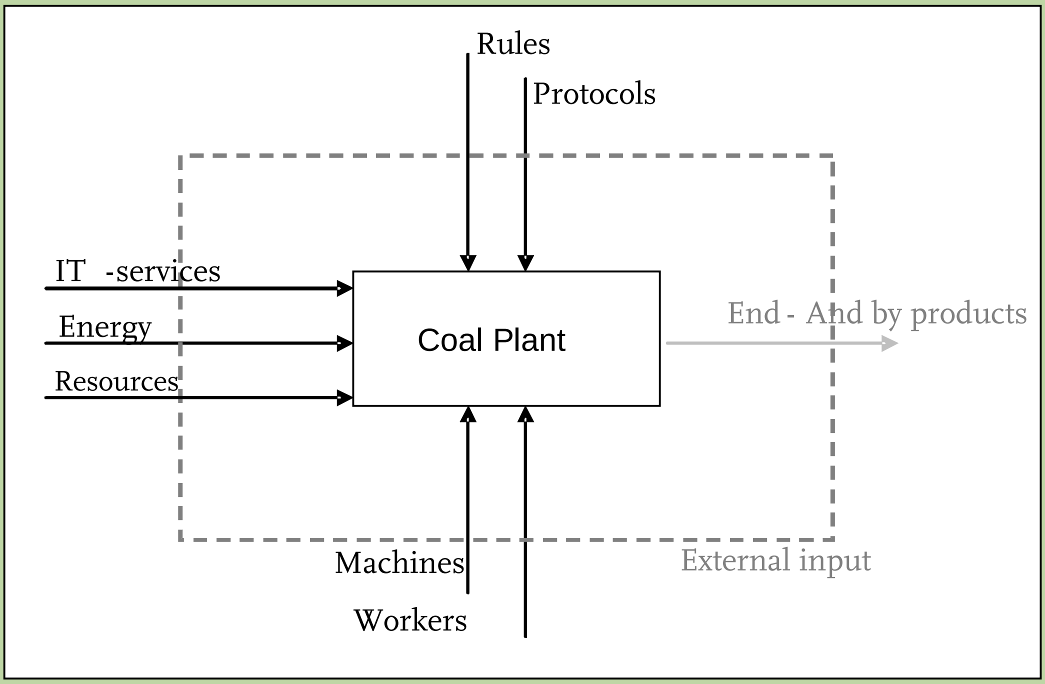
When using the external input model, it is important that all streams are mapped out. Risks are not necessarily limited to the primary inputs, controls or mechanisms. Less obvious streams can also involve considerable risks. Taking this aspect into account, it can be useful to conduct the system analysis on site. In other words: at the node. An excursion, during which the team of analysts visits the object to be investigated, is useful as a work form. Only then is good insight actually obtained into all the inputs, outputs, controls and mechanisms for the relevant system. Moreover, certain aspects of the operation of a node at site A may differ from the operation of the (ostensibly identical) system at site B. The vulnerabilities of one of these systems may also differ from those of the other.

One disadvantage associated with the use of the external input model is that only streams that flow into the system are depicted. Thus, no attention is paid to the streams between different sub-activities that occur within a system. A combination of the external input model and the layer model can offer added value in this regard.

Bronnen

Berenschot en COT, Second-opinion op de quick-scan, 13 januari 2003

Berenschot en COT, Voorstel tot herontwerp van de vervolgstappen, 13 januari 2003


Rules
Protocols
IT -services
Energy
Resources
Coal Plant
End - And by products
Machines
Workers
External input

3 Dimension Model

Essence

Over the last few decades, many (vital) infrastructure-dependent sectors have been liberalised. In the area of risk management, the government used to be responsible for the public utility sector. Because of institutional changes, these responsibilities have been allocated elsewhere, private parties have been assigned new tasks and Regulatory Authorities have been set up to supervise this system.

The dimension model makes it possible to map out the sector systematically using three dimensions. These dimensions (organisation, market and control) collectively provide a complete, accurate image of the structure of the market, and the parties operating in that market or who bear responsibility for that market.

Preparation, steps and follow-up

Het The dimension model can be particularly helpful when mapping out the structure of the sector, the roles of the parties involved and their responsibilities.

Prior to applying this dimension model, a layer model can be created, plotting the layers that can be distinguished in the industrial column. For example, for electricity the layers would be production, transport, distribution and delivery. Then the dimension model can be used to describe each layer in the three dimensions to be distinguished.

The following steps are involved when working out the dimension model:

Step 1: Describe the organisation dimension

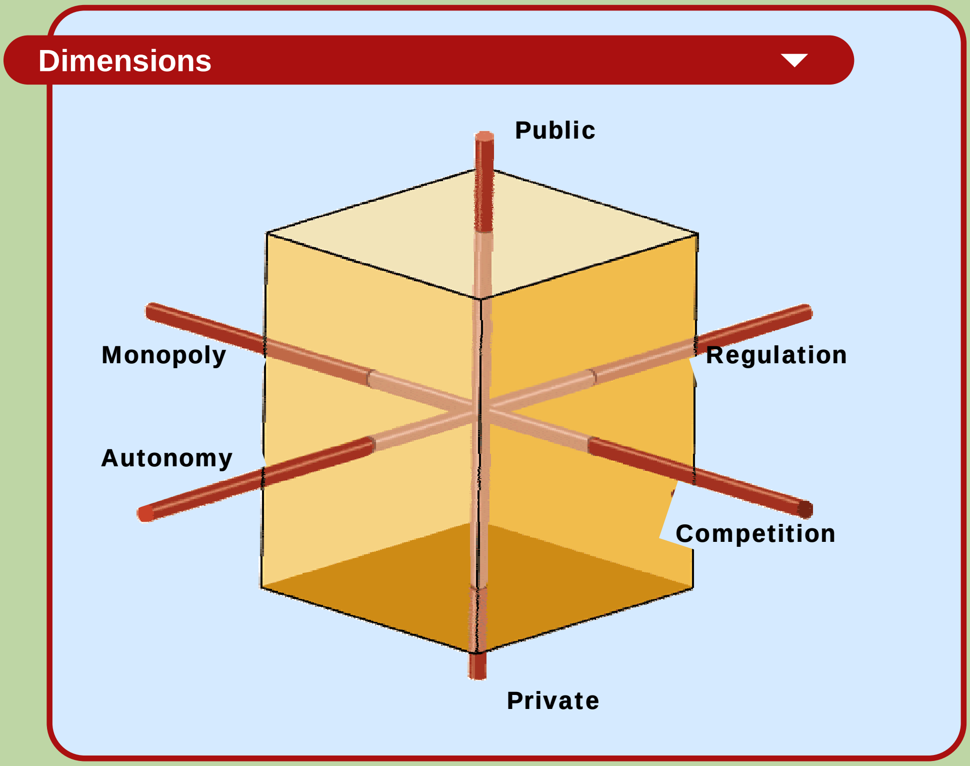
Are the tasks performed by a public or private agency (with the related policy ambitions for the privatisation operation)? In addition to the ownership relationships, other factors also determine the level at which one can speak of ‘private’ or ‘public’. A list of different sub-dimensions that can be mentioned in this context is presented below (see also the Council for Traffic and Communication as well as Bovens and Scheltema):

Ownership relationships. This is far the most important sub-dimension, considered by many to be the only one. From public to private, the following steps can be distinguished: government agency, state-owned company, government that holds a majority interest, government that is a primary shareholder, government that has (a limited number of) shares and finally: the individual enterprise in which the government has no shares at all.

(Legal) structure of the organisation’s operational management. Must the organisation maintain public or private (legal) structures in terms of its internal operational management? In the case of a legal structure, for instance: is the structure a public legal person or a private entity (such as a foundation, association or N.V.).

Power relationships. Does the government (the minister of the responsible department) have authority over the activities that the organisation performs, or does the government have no authority at all over these activities? In this context, we are speaking of ministerial responsibility and the level of independence, among other things. From public to private, the following steps can be distinguished: complete authority, public liberalisation, privatisation and outsourcing.

Financing relationships. Are the activities of the organisation financed using public funds or private resources? Here as well, various gradations can be distinguished.



Step 2: Describe the market dimension

Is the market a monopoly market or is competition involved? And if so, is there a level playing field (with the related policy ambitions that have to do with freeing up the markets, which are expressed in the form of a liberalisation operation)?

This dimension deals with the question of the extent to which competition is involved. The market regulation can fall anywhere on the scale from complete lack of a market on the one hand (monopoly) to the ideal free market (many suppliers, many customers) on the other. In any event, it is relevant to make a distinction between the types of competition that exist (see also Van Twist and Veeneman; see also the Council for Traffic and Communication): Competition on the infrastructure: this is the case if the market is not a natural monopoly and multiple suppliers can offer their services via the same infrastructure. An example is the delivery of electricity by different suppliers who deliver their services over the same network.

Competition for the infrastructure: in this case, there is only one supplier who has the right to offer services on the infrastructure. That right is obtained in competition with other potential suppliers. The concessions for UMTS are an example of this situation.

Competition between infrastructures: in this scenario there is competition between suppliers that deliver (approximately) the same service, but via different infrastructures. The services delivered on the two competitive markets are to a certain extent (imperfect) substitutes for one another. One example of this situation is competition between Internet via ADSL and via the cable.

Competition with the infrastructure: here a service is delivered that competes with the service delivered via an infrastructure. An example is the availability of an (emergency) aggregate for electricity. An example from another sector is bottled water from the source that can be seen as a substitute for water from the tap.

- Competition by comparing performance. This involves services from suppliers who have a monopolistic position compared to suppliers that deliver comparable services elsewhere. This is generally a stimulus utilised when purchasers do not have freedom of choice: obviously the discipline of the market does not work in this situation. One example of this is the regional network managers of electricity networks, who can be compared to one another, but do not compete with one another.

Moreover, different combinations of competition can occur rather than one pure form. A combination of 'for' and 'on' the infrastructure occurs in the case of radio frequencies: to obtain a concession you must compete for the infrastructure; then you must compete with other stations on the infrastructure for listeners. Moreover, there is of competition between infrastructures, e.g. television and the Internet.

p 3: Describe the control dimension

here autonomy or regulation (with the corresponding policy ambitions that are expressed in the deregulation operation)? Here as well, there are different interim steps or gradations. The level of regulation increases to the extent that the following are true (see also the Cabinet Memorandum regarding privatisation and liberalisation in network sectors):

In addition to generic competition regulations (Competitive Trading Act), there are also sector-specific competition regulations (e.g. the Electricity Act or the Telecommunication Act)

In addition to the Dutch Competition Authority (*NMa*) there are also sector-specific Regulatory Authorities (e.g. OPTA)

For example, special (restrictive) rules apply for already established parties which give new entrants the opportunity to enter the market. These rules are also referred to as asymmetrical rules. Such rules apply apply in the telecom sector, where parties such as KPN can be designated parties with 'significant market power'. Parties with significant market power are subject to specific regulations.

Societal organisations and intermediary organisations also exert influence. The Consumers Union is one example. These organisations stimulate the creation of additional laws and regulations and more transparency and bring pressure to bear for other different regulations.

Checklist of conditions

is important to first distinguish the layers (see the layer models described above).
e value of this model increases when, in working out the dimensions, one not only specifies whether there is autonomy or regulation, but also specifies the extent to which resistance can be expected to any proposed risk-related measures.
Moreover, this model primarily serves as an initial quick scan for plotting the sector. At a later stage of the risk analysis, it may also be helpful when determining effective measures. Furthermore, the field of influence must also be taken into account: what parties are active here, what (market) incentives drive them, etc?

Sources:

uncil for Traffic and Communication, *Tussen droom en deed*, 2003 (see www.raadvenw.nl). This was a preliminary study, published in 2004, conducted by Berenschot for the recommendation '*Hoezo marktwerking*'.

vens, M.A.P. and M. Scheltema, '*Rechsstatelijke redeneerpatronen*', in: Scientific Council for Government Policy, *Over publieke en private verantwoordelijkheden, Voorstudies en achtergronden*, The Hague, 1999.

st, M. van, and W. Veeneman (editor), *Marktwerking op weg: over concurrentiebevordering in infrastructuregebonden sectoren*, Utrecht 1999.

Cabinet Memorandum *Privatisering en liberalisering in netwerksectoren, 2000*.

4 Dependencies Model

Essence

The Dependencies Model charts the mutual dependencies (interdependencies) between different products and services and distinguishes four different types of interdependencies. A product or service can be delivered, intertwined, more or less independent or dependent, based on the extent to which the product or service contributes to other products or services on the one hand and the extent to which it is dependent on other products or services on the other. By positioning sectors or services in this model, one can see how products or services are linked to one another.

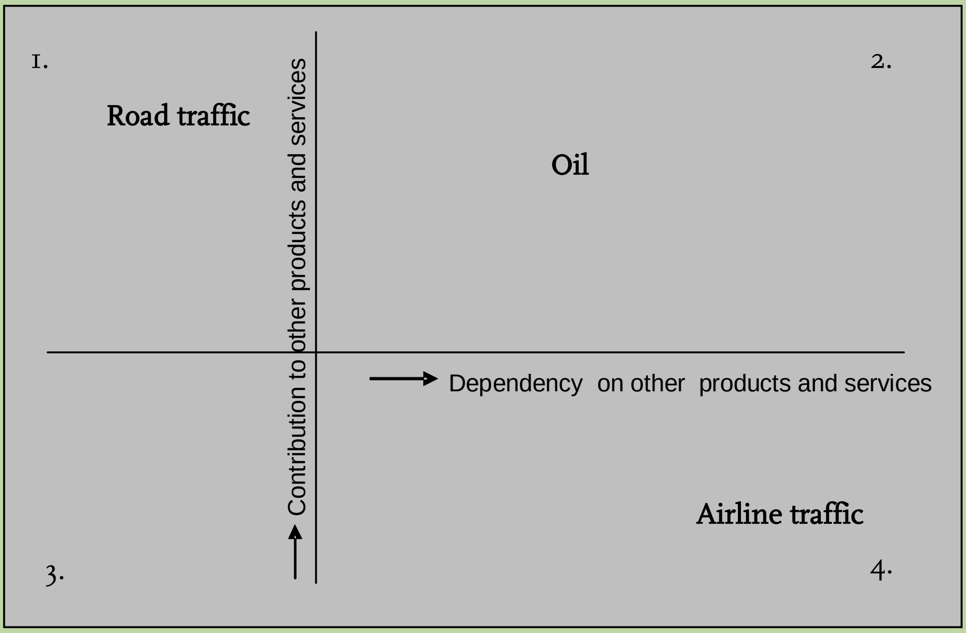
Preparation, steps and follow-up

The initial step in working out the Dependencies Model is to define the scope for the system being studied. Are all possible products and services considered, only vital products and services or only infrastructure-dependent products or services, for example?

The next step is to determine the level of dependency. Does a specific product (e.g. electricity) provide important input for other products and services or is the product dependent in many ways on the input of other products and services? In the first case, a risk in the sector being studied automatically involves a risk for producing products and services for which it provides input. In the other case, the sector being studied is subject to risks due to its dependency on other products and services over which the sector has no direct influence.

By investigating the extent to which the sector contributes to other products and services and the extent to which the sector is dependent on other products or services, the quadrant to which the sector belongs can be specified. The table below shows the quadrants and the corresponding characteristics.

	Type of dependency
Quadrant 1	*Delivering products and services* These products and services contribute significantly to other products or services, but are themselves not very dependent on other products or services (generating)
Quadrant 2	*Intertwined products and services* These products and services contribute rather significantly to other products and are themselves quite dependent on other products or services (critical)
Quadrant 3	*More or less independent products and services* These products and services contribute relatively little to other products or services and are themselves not very dependent on other products or services (independent)
Quadrant 4	*Dependent products and services* These products and services contribute relatively little to other products and services, but are themselves quite dependent on other products and services (dependent)


1.
Road traffic
Contribution to other products and services
2.
Oil
Dependency on other products and services
Airline traffic
3.
4.

After determining the quadrant to which the product or service belongs, the dependencies can be graphed by placing them in the appropriate quadrant in the matrix.

As a follow-up to this analysis, the relations and dependencies for all products and services that are dependent on other products or services can be described in detail.

This model can be applied in an interactive setting, such as in a workshop or expert meeting. In that case, it is important to ensure that the experts participating, who are probably experts in a particular subdomain, speak about their personal areas of expertise and not about those of others. After all, if this is not done, experts in a specific domain can be overruled by people who do not have specific expertise in that domain.

Checklist of conditions

Opinions regarding the level of dependency and the contribution of products or services to other products or services can differ. Moreover, this model requires knowledge of the different products and services. Involvement in the sector is required to produce meaningful results with this model.

The model involves a relatively high level of abstraction. In order to produce usable analyses, the dependencies found must be worked out in more concrete detail later in the process.

Sources

TNO, *Bescherming vitale infrastructuur: Quickscan naar vitale producten en diensten*, TNO: FEL 03-C002

5 PEST-SWOT Model

Essence

The PEST-SWOT analysis as shown above is a model with which the strengths and weaknesses, opportunities and threats in the environment of the product or service can be described using four different perspectives: political-administrative, economic, social-cultural and technological. The four perspectives – that are so characteristic of PEST analysis - can be regarded as a short checklist of perspectives.

In addition, the SWOT analysis can also be used to evaluate a previously implemented measure or package of measures.

Preparation, steps and follow-up

Step 1. The first step in working out the PEST-SWOT model is to determine the time horizon. For example: Is it important to specify possible developments in the environment of the product or service being studied for the coming year or for the coming ten years?

Step 2. Formulate the PEST developments. Then all possible developments for the four different perspectives are formulated. Examples of political-administrative developments are liberalisation, disentanglement and self-regulation. One might also consider changes in political stability or in regulations that affect a product or service. Examples of social-cultural factors include demographic developments and social mobility. Examples of economic developments include unemployment, inflation and the availability of energy sources. Technological developments could include new telecommunication techniques such as VoIP or local energy generation using combined heat and power equipment (CHP).

Step 3. SWOT. In a subsequent step, for each perspective from the PEST analysis, one investigates whether the developments offer an opportunity or pose a threat or perhaps do both simultaneously. Then the strengths and weaknesses of the service being studied must be identified. Then, a determination can be made of whether a specific threat can be reduced by the system's strengths. Where threats are involved and the product or service has weaknesses in that area, the measures that can minimise the weaknesses and can minimise or avert these threats must be studied. This is shown in the following figure.

	Strengths	Weaknesses
Opportunities	Develop measures that use strengths to take advantage of opportunities.	Develop measures that utilise opportunities by overcoming weaknesses.
Threats	Develop measures that use strengths to avert threats.	Develop measures that minimise weakness to avert threats.

Internal factors	Political-administrative		Economic		Social-cultural		Technological	
	O	T	O	T	O	T	O	T
Strengths 1. xxx 2. achieved in 2000 3. zzz	+ + + +							
Weaknesses 4. aaa 5. bbb 6. ccc	- - + + +		+ + + - -		+ + - +		+ + + -	

Step4. In In a final step, the measures found can be evaluated ex-ante using a SWOT analysis. What are the strengths and weaknesses of the measure? For example, in terms of weaknesses, the side effects that might arise can be considered. What opportunities and threats apply to these measures?

This step already takes measures into account. Thus, use of this model is not limited to the environmental analysis phase, but the model can also be helpful when trying to come up with measures. A brainstorming session can be a good method for filling in this model. After all, it is particularly important to gain insight into the number and variety of developments.

Checklist of conditions

The results of the PEST SWOT analysis cannot be considered static. After all, environmental factors change. What may initially be an opportunity, can quickly become a significant threat. This must be taken into account when interpreting the results. The usability of the model increases when the analysis is repeated periodically. Another important condition for ensuring useful results from the model is information on what type of follow-up will be performed using the results of the completed SWOT analysis.

In applying this model, it is important that *all* strengths, weakness, opportunities and threats and developments in the environment be included in the analysis, both the realistic ones and the unlikely ones. Ensuring that a range of different skills and perspectives is represented in the team of analysts is thus one condition for success; a brainstorming session with experts is an appropriate work form when using this model.

Sources

Johnson. G en K. Scholes (1999) *Exploring corporate strategy*, Prentice Hall: London (p. 104/105)

Five Forces Model

Essence

Porter's Five Forces Model depicts the organisation of a specific sector in the form of a diagram. It provides insight into the dependencies that apply to the sector and the substitutes for the service (or product) in question and, as well as showing what actors are involved in producing the service. Moreover, the model is also appropriate for mapping out the environment of an alleged or virtual monopoly and then working out what bankruptcy of that monopoly party would mean. Analyses of companies like KPN, UPC and large energy companies that also manage part of the electricity network are all good examples of this.

In fact, the model is a combination of the previously described external input model and a dependency analysis. The model is particularly appropriate for conducting an environmental analysis of a sector as a whole. In contrast to other models, the Five Forces Model also clarifies what products or services provide a substitute for the products and services from the sector in question. Finally, this model reveals the dependencies and any domino effects: the relationships with suppliers and customers provide an indication of where such effects could occur.

Preparation, steps and follow-up

The following aspects are mapped out in the order in which they are handled below:

Step 1. Plot the existing market and competitors. Who are the current players in the market? What is their market share and to what extent is there rivalry or competition between them?

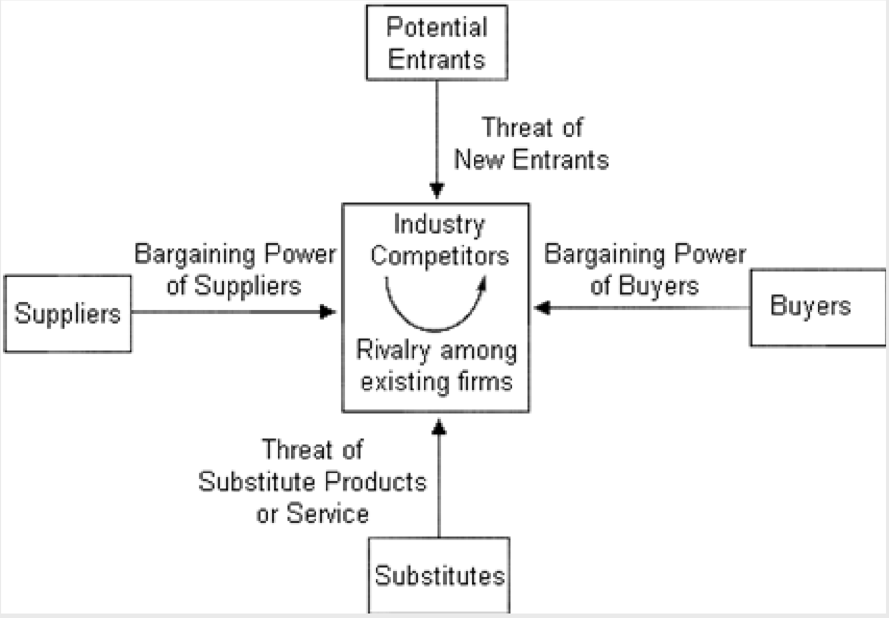
Step 2. Plot any new entrants. Are there new entrants? What opportunities exist for these new entrants? Is there a level playing field?

Step 3. Plot the customers. Who purchases the product or service? To what extent is there freedom of choice for these customers? To what extent is the offer varied? Moreover: energy is a product for which there are few possibilities for diversification other than price. The quality of the service provision and diversification in different the form of new types of contracts are examples of this.

Step 4. Plot any substitutes. Are there any substitutes for the product or service? To what extent do these substitutes eliminate part of the possible threats and vulnerabilities for the product or service? Answering this question provides an indication of the current level of resistance and robustness of the product or service. This is considerable in the case of telecommunication, for example: if the mobile telecommunication service is disrupted, customers can fall back on fixed telecommunication lines to a large extent.

Step 5. Plot the suppliers. Who are the suppliers? To what extent does the product or service depend on these suppliers?

Answering these questions produces a model that offers insight into the level of resistance to threats the service of the product offers, the dependencies on other services (suppliers) and the level of competition (and in this context the attention that may be paid to security aspects). These elements are also described in the dimension model and the dependencies model, though in a different way and in another context. A combination of the Five Forces Model with (one of) these models is thus an obvious choice.


Potential Entrants
Threat of New Entrants
Bargaining Power of Suppliers
Suppliers
Industry Competitors
Rivalry among existing firms
Bargaining Power of Buyers
Buyers
Threat of Substitute Products or Service
Substitutes

Checklist of conditions

When interpreting the results of this model, the level of dynamism in the sector or service must be taken into account. Both the telecommunication and energy sectors are in a transition phase on the way to a more liberalised market. Thus, where initially there may have been only a few new entrants, at a later stage there may be considerable competition.

This model requires sufficient knowledge of the sector or service.

This model does not provide a complete environmental analysis. It only involves an analysis of the market. Aspects such as political, economic, technical and social influences are not taken into account. Moreover, the model has a reactive character; it specifically involves the existing situation and external factors.

Sources

Porter, M.E. (1998) *Competitive strategy: Techniques for Analyzing Industries and Competitors*, The free press: New York

Classes of events and causes

In the literature, risks analyses are supported not only by models, but are also frequently supported by classes and types of events, the corresponding causes of the event or scales for expressing the likelihood that something may occur. The following paragraphs offer an inventory of classes and scales that can be helpful in systematically inventorying and categorising events as well as the causes and duration of the disruption.

First of all, different cause categories can be distinguished for threats:

- Organisational causes
- Technical causes
- Unconscious human actions
- Conscious human actions
- Natural disasters
- Failure or malfunction in another vital product or service

Secondly, different types of events can be distinguished:

- Events involving people
- Events involving objects
- Events involving sectors
- Events involving image

Classes for types of human actions

Essence

Classifying the types of human actions and the related types of human failures can be useful for gaining better insight into the nature of threats.

In terms of human actions, a distinction can be made between knowledge-based, skill-based and rule-based actions. The table below describes the distinctions between these three types.

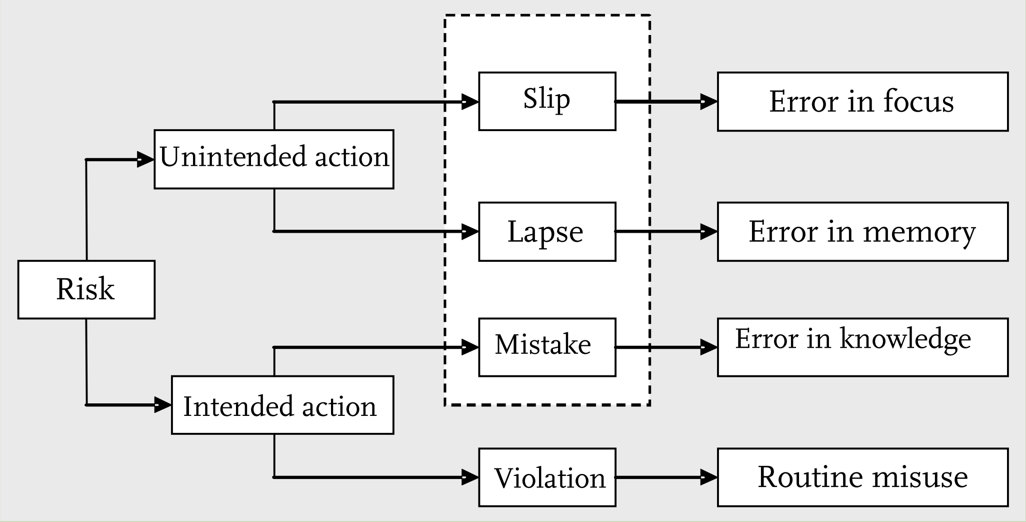
Knowledge-based	The task is performed consciously. A task is performed for the first time or in a new environment. It is not a routine task, thus the action requires considerable effort and progresses slowly.
Skill-based	Performing a routine task. Not a particularly conscious execution of the tasks. Tasks are performed quickly without requiring much effort.
Rule-based	The rules to be followed when performing the tasks are available, but are not frequently used.

In a professional environment (hospitals, universities), a number of knowledge-based actions are performed. On the work floor in a factory where activities are performed based on instructions and protocols, most activities will be rule-based actions. In that case, the following psychological causes for unsafe action can be distinguished:

Slip	Right intention, wrong action. Because people are operating out of habit, exceptional causes are overlooked.
Lapse	Right intention, but the operator has a memory lapse
Mistake	These errors specifically involve a lack of skill. This can be described as taking the wrong action with the wrong intention
Violation	Failure to comply with rules or procedures

Checklist of conditions

The psychological cause of unsafe action is fairly obvious for each class of human action. Thus it can be expected and assumed that in an organisation whose activities are primarily rule-based, more lapses and routine errors will occur than in a professional organisation where the complexity of the work requires employees to improvise more frequently.



Sources

Managing the Risks of Organisational Accidents, J. Reason, 1997, and Human Error, J, Reason, 1990. P 207.

New Technology and Human Error, J. Rasmussen, e.a. 1987

Checklist of initial events and domino effects

The following table can be used to identify and classify initial events; it distinguishes between three types of initial events: technical and organisational failures, natural disasters and (un)conscious human actions. The fourth column deals with failure or malfunction of a vital product or a vital service.

The overview does not provide a complete overview of initial events, but can be helpful as a checklist. Depending on the objective of the risk analysis, analysts can expand or reduce the model.

The list of vital products or services is based on the concept 'vital'. Obviously this definition can differ per risk analysis or per analyst. The term 'vital' is defined in Paragraph 2.2.1.

The following overview shows the four types of initial events; the last category involves the failure or malfunction of vital products or services.

Organisational and technical causes	**(Un)conscious human act**	**Natural disasters**	**Failure or malfunction of a vital product or service**
Organisational: Logistics errors Installation errors Production errors Operator errors User errors Construction errors Poor/deficient quality control Deficient employee training and supervision Personnel turnover *Technical:* Software malfunction Short circuit Leaks Damage to cables and pipes Material deficiencies Failure of the measurement, regulating security equipment Hardware disruptions	Break-in Theft Hold-up Extortion Kidnapping Forgery Fraud Kidnapping Vandalism Plundering (Industrial) espionage Catastrophic terrorism Deliberate damage/sabotage Demonstrations Riots Strikes Personnel illness as the result of a pandemic Government regulations (Arbo, Regulatory Authorities, etc) Carelessness Negligence Fire Explosion Implosion	Rain Hail Snow Ice Frost Heat Drought Lightning Storm Flooding High water Earthquake Landslide Shift/Earth tremors Lengthy drought Serious cold Lengthy cold Heavy rains Serious storm	Electricity Natural gas Oil Fixed communication Mobile communication Radiocommunicatie & -navigation Satellite Broadcaster Internet access Postal and courier services Drinking water facilities Food provisions facilities Health care Payment services (private) Financial transfer by the government Water quality Water quantity Maintaining public order Maintaining public safety Administration of justice Maintaining law and order Diplomacy Providing information

In the case of the last category, i.e. failure of a service, a distinction can be made with regard to the duration of the failure or malfunction. One very basic classification is based on three categories:

- Short term
- Medium term
- Long term

A more detailed analysis can provide subtler distinctions, for example as shown in the following table and as used in the framework of the Protection of Vital Infrastructures Projects:

Disruption characteristics	In minutes	One to a few hours	Half to whole day	1-2 days	3-7 days	1-4 weeks	1-12 months	One to a few years	Continual
Service A									
Service B									
Service C									
Etc.									

Simple ranking: qualitative and/or quantitative

Essence

A simple ranking can be applied in situations in which it is difficult to foresee how likely it is that an event will occur. For example, kidnapping of a company employee by an angry, disappointed ex-employee who has been fired. How great is the likelihood that this will occur? One in a hundred; one in a thousand?

Moreover, applying simple ranking can be useful in cases in which the likelihood categories are not distinctive enough. The events or scenarios that fall into a likelihood category (e.g. the category 'extremely small likelihood') differ dramatically: one occurrence is much more likely than another. For example, many forms of terrorism (conscious human action) have an extremely small chance of actually occurring and fall into the least chance category, while different types of terrorist actions can be specified that are much more likely (e.g. 100 times more likely to occur) than other terrorist actions.

Preparation, steps and follow-up

In short, simple ranking is based on the following principles. A list of potential of events and/or scenarios is drawn up, and then the parties involved (e.g. experts such as representatives of the AIVD or people from the sector) are requested to rank these events and/or scenarios in sequence: what events/ scenarios do you consider more likely to occur than the others? In other words: the events/scenarios are ranked in the order of their likelihood to occur. That creates a ranking or prioritisation of the likelihood that the events/scenarios might occur. Because the events are arranged in a sequence and because not every occurrence is explicitly compared to every other occurrence, this is referred to as a 'simple' ranking.

A simple ranking can be either qualitative or quantitative:

	Qualitative	Quantitative
Simple	Version 1: Simple, qualitative	Version 2: Simple, quantitative

For a simple **qualitative** ranking, the following two steps must be taken first.

Step 1: Make a list of potential events/scenarios that can occur.

Step 2: Place the events/scenarios in the sequence of their likelihood to occur. Take the second occurrence from the list of potential events and place this before (greater likelihood) or after (less likelihood) the first occurrence from the list of potential events. Then position the third occurrence from the list of potential events at the very top (greatest chance), in the middle, or at the end (least chance). Then place all the other events from the list in this sequence one by one.

This can be done as follows (P stands for 'probability' or 'likelihood):

P (operator error) > P (computer virus) > P (kidnapping of an employee) > etc.

This completes the simple qualitative ranking. For a simple **quantitative** ranking, steps 3 and 4 must also be performed.

Step 3: Specify in each case how much more likely one occurrence is compared to an occurrence that is less likely. This can be done as follows (where P stands for ‘probability’ or ‘likelihood’):

P(operator error) is twice as great as

P(computer virus) is 100 times as great as

P(kidnapping of an employee).

Step 4: Then calculate the relative chances. Assign the occurrence with the least likelihood a relative likelihood of 1. That makes the calculation easier as well as making it possible to compare the relative likelihood of different events. Place the results in a table similar to the one shown in the following example:

Occurrence scenario	Relative chance
Operator error	200
Computer virus	100
Kidnapping of an employee	1

Checklist of conditions

Try to limit the list of potential events; otherwise the analysis becomes extremely time-consuming.

The method can be used in a group meeting, but in that case two suggestions are very important. First of all: when the method is used in groups, it is strongly recommended that the list of potential events/scenarios be limited. Secondly: if possible, utilise an electronic boardroom system for support. This allows all participants to easily prioritise the items and makes quick aggregation of the entries made by the individual participants possible, so that there is more time left for discussion.

11 Paired ranking: qualitative and/or quantitative

Essence

Just like with simple ranking, paired ranking can be used in situations in which it is difficult to specify the likelihood that an occurrence that might occur will actually occur, without comparing it to other events. Furthermore, it is useful to apply this method when the likelihood categories are not sufficiently distinctive.

Preparation, steps and follow-up

In short, the method is based on the following principles. A table is drawn up with a series of events and/or scenarios on both the horizontal and vertical axes. The same events/scenarios are placed in the same sequence on both axes. Then the parties involved are requested to compare these pairs of events/scenarios: which of the two events/scenarios do you consider more likely to occur? All events/scenarios are compared to all other events/scenarios. Ultimately, this results in a ranking or prioritisation of events/scenarios that can arise. Because each occurrence from the list of potential events is explicitly compared to every other occurrence, this is referred to as a 'paired' ranking.

Just as with simple ranking, a paired ranking can be either qualitative or quantitative.

	Qualitative	Quantitative
Paired (multiple)	Version 1: Paired ranking, qualitative	Version 2: Paired ranking, quantitative

For a paired **qualitative** ranking, the first **two steps** described below must be performed.

Step 1: Make a list of potential events/scenarios that can arise.

Step 2: Construct a table with the same events/scenarios in the same sequence on both axes.

Step 3: Then compare each occurrence to every other occurrence, and indicate whether the likelihood of occurrence on the left-hand axis (vertical axis) is greater, identical to or less than the likelihood of the occurrence on the right-hand axis (the horizontal axis). As an illustration, an example of a paired, qualitative ranking table is shown below. Three examples are filled in: the chance of an operator error is greater than the chance of a software malfunction, the chance of a kidnapping is less than the chance of a software malfunction and the chance of a nuclear attack is identical to that for a kidnapping. The areas with a grey background do not have to be filled in. After all, this is the 'mirror image' of the rankings in the areas without a grey background.

		Software malfunction	Operator error	...	Kidnapping	Nuclear attack	...	Drought	Storm	...	Electricity	Fixed communication	...
nisational/te cal causes	Software malfunction	=											
	Operator error	>	=										
	...	...	...	=									
conscious an act	Kidnapping	<	...	...	=								
	Nuclear attack	...	...	...	=	=							
	...	...	...	...	...	...	=						
ral disasters	Drought	...	...	...	...	...	...	=					
	Storm	...	...	...	...	...	...	...	=				
	...	...	...	...	...	...	...	...	...	=			
re or unction of a product or ce	Electricity	...	...	...	...	...	...	...	...	...	=		
	Fixed communication	...	...	...	...	...	...	...	...	...	...	=	
	...	...	...	...	...	...	...	...	...	...	...	...	=

In the quantitative version, the party involved not only indicates whether the chance is greater than, identical to or less than the other event, but also how much likely or less likely it is. Rather than using the symbols > (greater than), = (equal to) and < (less than), numbers are entered in the table. Another table is shown below as an illustration. Two examples are filled in: the chance of an operator error is three times as great as the chance of a software disruption. The chance of a kidnapping is 0.1 times as great as the chance of a software disruption. In other words: the chance of a software disruption is 10 times greater than the chance of a kidnapping.

Step 4: Then calculate the relative sequence of likelihood. This can be difficult because the parties involved do not by definition rate items consistently. They may consider occurrence A more likely than occurrence B, which, in turn, is more likely than occurrence C, but at the same time they indicate that C is more likely than A.
Assign the occurrence with the least chance a relative chance of 1. That makes it easier to calculate the ratio for the relative likelihood of pairs of events. Then place the results in a table like to one shown below:

Occurrence scenario	Relative chance
Operator error	30
Software disruption	10
Kidnapping of an employee	1

If the parties involved have not been consistent, the results will not be nice round numbers as shown in the preceding table. Computer support for calculating the scores is indispensable when using paired ranking.

Checklist of conditions

Try to keep the list of potential events limited, because each additional occurrence in a paired analysis exponentially increases the number of comparisons. With two events, only one comparison is required, but 100 events requires 4950. The table below shows how much comparisons are required for a given number of events

Number of events	Number comparisons to be made
2	1
3	3
4	6
5	10
6	15
7	21
--	…
100	4950
N	(N-1)*(N/2)

This method cannot be used without an adequate calculation program. If you are using this method in a group meeting, you can use an electronic boardroom in which such a calculation module has been installed

Deed-Perpetrator Matrix (DDM) for conscious human act

Essence

The Deed-perpetrator matrix shows the modus operandi for different types of perpetrators. The vertical axis shows the acts (as well as modus operandi) and the horizontal axis shows the types of perpetrators (perpetrator profile). This matrix provides insight into the level at which perpetrators and acts are realistic and can be expected.

Preparation, steps and follow-up

Step 1. In the first step, the types of perpetrators are distinguished and a list of potential modus operandi - work methods or acts – is compiled.

Step 2. Then an analysis of the combination of deed and perpetrator is conducted. After all, in the figure that arises the most logical ones can be indicated, as has been done in the sample figure below using a different background colour. The figure is obviously not complete and the most logical events can also differ per type of sector, product or service.

Step 3. In a third step, a selection of the most relevant events can be made. Which of the areas with grey background should be given priority, for example because the anticipated damage in the case of occurrence is great? Based on that selection, measures can then be specified..

Checklist of conditions

The AIVD has the knowledge to make a realistic estimate. Thus, it makes sense to involve this service for this type of analyses.

It can take quite some time to fill in a Deed-Perpetrator matrix. When doing this, it is important to realise that filling in the matrix is not itself the objective, but that it is just a step in the prioritisation of such events.

	Scenario	Criminal Activity	Mild Crimina Activity	Serious Crin Activity	Unbalanced Person	Ex-employee	Violent Activity	Activist	Intelligence Service	Terrorist	Script kiddie	Hacker	Hacktivist	Journalist
Internal eavesdropping	**1**													
Installing eavesdropping equipment	1.1			■					■					
ICT sniffing	1.2					■							■	■
External eavesdropping	**2**													
Using microphones or wiretaps	2.1			■					■					
ICT sniffing	2.2								■		■		■	■
Broad-scale eavesdropping (echelon)	2.3								■					
Breaking an encryption code	2.4								■					
Intercepting Starling (Tempest)	2.5								■					
Shooting	**3**													
from a distance	3.1			■						■				
from closeby	3.2			■	■		■			■				
Exploding projectile	3.2			■						■				
Occupation	**4**							■						
Blockade	**5**							■						
Bomb on a person, suicide bomber	**6**				■					■				
Bomb threat with hazardous powder	**7**			■			■							
Bomb threat or letter	**8**													
False bomb threat	8.1				■	■		■						
False threat of a letter	8.2				■	■		■						
Leaving a packing containing a bomb	**9**			■						■				
Bombs	**10**													
Car bomb	10.1			■						■				
Boat bomb	10.2									■				
Airplane bomb (model airplane)	10.3									■				
Airplane bomb (Cessna / helicopter)	10.4									■				
Airplane bomb (commercial aircraft)	10.5									■				
Firebomb	**11**			■			■			■				
Arson	**12**			■			■			■				
Carjacking	**13**			■			■			■				
Blackmail	**14**													
Blackmail involving threat	14.1			■					■					
Blackmail involving hacking	14.2		■	■		■								
Collateral damage	**15**			■						■				
Compromittation	**16**								■					
Corruption	**17**			■		■								
Theft	**18**													
Opportunistic theft	18.1	■			■	■								
Opportunistic theft involving break-in	18.2	■												
Premeditated theft	18.3		■	■		■			■				■	
Premeditated theft involving break-in	18.4		■	■					■					
Kidnapping	**19**													
Kidnapping	19.1			■	■					■				
Abduction	19.2			■						■				
Hacking	**20**													
Unconcentrated	20.1										■			
Concentrated	20.2					■	■		■	■		■	■	■
Wardriving	20.3										■			■
Wardialling	20.4										■	■		■
Housejacking	**21**			■										
Infiltration	**22**			■					■	■				
Imprisonment	**23**		■	■				■						
Manipulation	**24**													
Social engineering	24.1		■	■					■	■		■	■	■
Damage to business resources	**25**													
Destroying business resources	25.1	■					■	■						
Defacing the web site	25.2										■		■	
Attacking the web site	25.3		■	■							■	■	■	
Moles in the building	**26**				■	■	■							
Damage to personnel	**27**													
Violence aimed at personnel	27.1				■									
Serious threat to personnel	27.2				■		■							
NBC contamination	**28**													
Contamination of NBC resources	28.1			■	■					■				
Sending NBC Letter	**29**									■				
Robbery	**30**			■						■				
Communication sabotage (telephone system. Alrams)	**31**			■				■	■	■				
Process sabotage	**32**													
Disrupting production processes	32.1			■		■				■				
Denial of Service (DoS)	32.2								■	■		■	■	
Distributed denial of service (DDOS)	32.3								■	■	■	■	■	
Hijacking processes and systems	32.4									■				
HPM weapons	32.5								■					
Viruses (computer)	**33**													
Viruses/ worms	33.1			■							■	■		
Trojan Horses	33.2								■	■			■	

Can-Will Matrix

Essence

The Can-Will Matrix clarifies how easy it is for perpetrators with malicious intent to successfully pull off possible events and the appeal for pulling off each type of event. The events can be positioned in a quadrant, distinguishing between events whose execution is complex but attractive (quadrant III), complex and quite unattractive (quadrant IV), easy but unattractive (quadrant II) and easy and quite attractive (quadrant I).

Preparation, steps and follow-up

The following steps can be distinguished in applying the Can-Will Matrix:

Step 1: Select a perpetrator profile. The Deed-perpetrator matrix described earlier in the manual can be used for this.

Step 2: Select events. Just as for the perpetrator profiles, the Deed-perpetrator matrix can be used to the events to be studied. The checklist of initial events can also be consulted.

Step 3: Specify the can-will coordinates for each occurrence for that perpetrator profile. The 'can' category involves – among other things - the ease with which a perpetrator could successfully effect the deed. For example, you would want to take into account the requisite preparation time and risk of being caught. Another relevant variable is the number of perpetrators required to successfully effect the deed. The more people required, the more difficult it would be to accomplish. In that sense, the span of control is relevant. For example, an organisation of terrorist cells that are limited in size might reduce the chance of being caught. The 'will' column specifically involves analysing the specific perpetrator's objective. For example, cause the maximum damage, disrupt society or create fear.

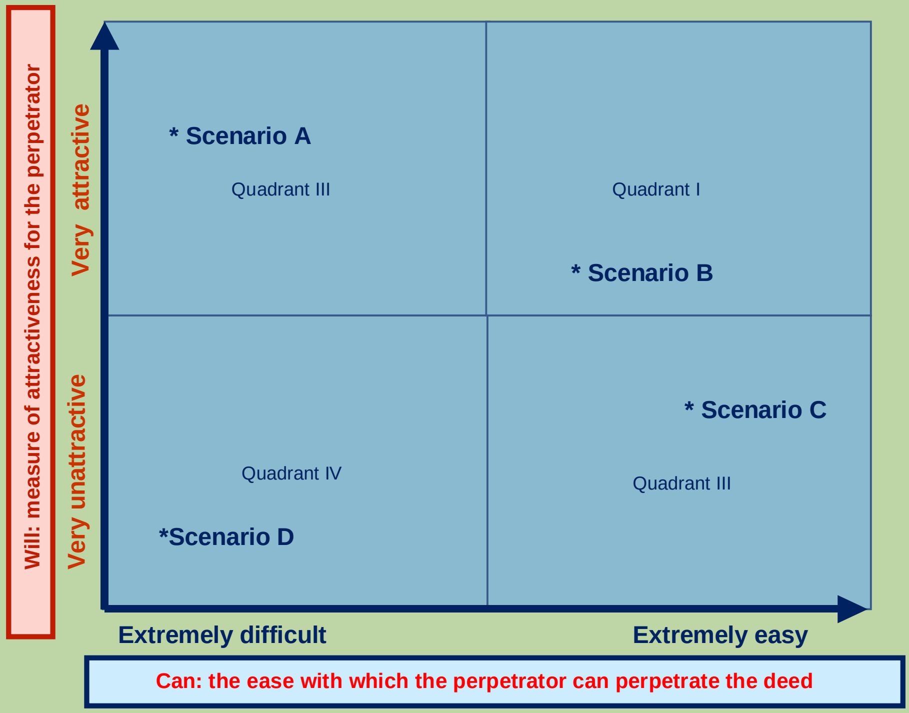
Step 4: Conduct an analysis for other perpetrator profiles as well. In this step it is important to investigate what events are relevant when another perpetrator is considered. A terrorist's modus operandi would likely differ from that of a petty (opportunistic) criminal. Then you must again specify how the occurrence can be placed in the matrix for that perpetrator profile.

Step 5: Prioritise the realistic events. The final step is to prioritise the events from the different quadrants of the matrix based on how likely they are to occur. The events from quadrant IV (very difficult and complex and very unattractive) are less likely to occur than events from quadrant I (very simple and very attractive).

Checklist of conditions

The results obtained when applying this model must be interpreted with care. After all, it is not necessarily true that events that are simple to execute and attractive are almost certain to occur and that no attention needs to be devoted to preventing those events that are difficult and unattractive. After all, there will probably be more measures in place to prevent events in quadrant I from occurring than for those in quadrant IV.

This model requires sufficient expertise in the service or sector involved. Availability of the required knowledge can only be guaranteed by involving the sector when conducting this type of analysis. After all, only representatives of the sector can provide proper insight into the simplicity or complexity of pulling off a specific event in their own sector, or involving their product or service. Involvement of the AIVD is crucial because of its knowledge and expertise in this domain. An appropriate work form for this model is an expert meeting or workshop in which a team of analysts participates that at a minimum includes representative of Ministries, knowledge institutions and sector members. Because opinions regarding what is "appealing" can differ, it is important that the work form have a brainstorm or debating aspect.



The model is intended primarily for internal use. Distributing the results of this model can increase the vulnerability of the product or service.

KWINT Layers-management model

Essence

The layer management model involves a combination of a layer model and a classification into management areas in order to inventory risks. Such a model offers a clear overview of risks for the 'industrial column' per layer in combination with the level at which the risks must be addressed..

Preparation, steps and follow-up

Step 1. Choosing the layers. The classification into layers to be maintained depends on the sector or service being analysed. The example in the figure describes the layers for the Internet.

Step 2. Select relevant management areas. For management areas, a distinction can be made between the level of one organisation, the national level or the international level. That is the perspective chosen for the table used as an example here.

Step 3. Plot the risks. When the vulnerabilities and risks for a specific service or sector are charted and categorised by the corresponding management area per layer, this provides insight into the distribution (or clustering) of risks over sub-sectors and management areas. This then gives a good indication of where risks occur and thus where they must be addressed. Infringement on the privacy of one employee's Internet information is a matter for the organisation involved, while the activities of computer criminals operating on a broader scale is a national (and in some cases even an international) matter. This model makes it possible to see whether there is a concentration of risks in one specific layer or a single management area.

In a subsequent step, measures can be identified and analysed.

Checklist of conditions

The objective of this model must not be to position risks in each cell in the table. Some cells may be empty. The objective is to gain insight into where the risks actually arise.

Use of this model requires sufficient insight into the sector, product or service to be investigated and the related responsibilities. In addition to knowledge of the different responsibilities and management areas on the part of the policy staff, involvement of the sector is also a condition for generating meaningful results with this model. Thus, an expert meeting or workshop is an appropriate work form for using this model.

Sources

TNO-FEL, Stratix Consulting Group, *Samen werken voor veilig internetverkeer*, Final report of the research project entitled '*Kwetsbaarheid van het internet (KWINT)*' conducted on behalf of the Ministry of Traffic and Communications, January 2001

Management Layer	Management domain and organisation	More management domains: national	Even more management domains International
Information Layer	Hackers, computer criminals Privacy and financially confidentiality interests poorly safeguarded	(IT) activists, computer criminals loss of confidence among consumer companies	macro virus attacks distributed denial of service loss of confidence among consumer companies
Generic Applications	hijacking domain names	DoS attack or hacking of DNS, TTP and other generic applications SpoFs at conversion points for Internet services to/from mobile services Hacking/fraud/ DoS attacks on important services via generic applications Loss of confidence among Trusted Third Parties and comparable services	Loss of confidence among Trusted Third Parties and comparable services
Network Layer	Poor firewalls Lack of a security policy Failure of important routers due to DoS attacks and hacks	failure of AMS-IX means a failure of large part of the Internet services in the Netherlands Failure of part of the Duthc backbone	failure of international nodes
Transmission Layer	Scarce equipment glass fiber, lack of manpower delay due to problems with digging rights, licenses Scarce ISP connections	cable breakage caused by digging / events of nature	failure of the backbone infrastructure (e.g. undersea cables) not all cross-connects are redundantly configured, creating SpoF SpoFs in management and control system
Facilities	Power disruptions	Power disruptions scarcity of electricity mains at the Cyber main port	failure of the electrical power network
Convergence & Interrelationship		unintended chain dependencies in complex networks for which the total overview is inadequate	Scarcity in networks can lead to a cascade of failures Recognised gaps in commercial off-the-shelf (COTS) resources

Path analysis

Essence

In the path analysis, the analyst imagines himself to have malicious intent and attempts to approach the object in question from that perspective (and to gain access to it, for example). A party with malicious intent will seek the path of least resistance that achieves the objective he has in mind. The model is particularly applicable for systematically detecting weak points in objects'' security. A path analysis can also contribute to formulating measures for the detected weaknesses.

Preparation, steps and follow-up

The following steps can be used when conducting a path analysis:

Step 1: Make a list of the types of perpetrators who may want to cause damage or could wreak havoc on a specific object (building or node). A terrorist, burglar, angry ex-employee, confused person, activist/demonstrator, etc..

Step 2: Select a type of malicious intent and look for the path of least resistance. The analyst puts himself in the perpetrator's shoes and tries to imagine how such a person (e.g. a terrorist) would operate. The point of departure is that the terrorist will consistently use the path of the least resistance that will achieve his goal. The terrorist looks for the weakest point in the monitoring system: path 1.

Step 3: Then construct path 2, path 3, etc.. In step 2, path 1 is identified: the path that the terrorist will take in the current situation. Then the analyst must suppose that measures have been taken to make path 1 less attractive, and to search for the most attractive for the terrorist in this new scenario: path 2. This process is repeated for path 3. And so forth. This analysis continues until the paths for the analyst become quite unrealistic. For example, so unrealistic that a terrorist would select another target.

Step 4: Conduct the same analysis for the other types of 'perpetrators', such as a burglar or an angry ex-employee.

Step 5: Then conduct the analysis for other objects as well.

Checklist of conditions

Conducting a good path analysis requires good preparation. After all, depending on the type of analysis - a path analysis can require extensive knowledge of an object, and may thus require considerable preparation. For example, if the analyst must put himself in the shoes of an angry ex-employee, he must also have the same insight into potential weak points as that ex-employee would have. Such knowledge is considerably more extensive than that of a malicious activist, for example, who has never been in the object itself, an analysis which would thus require less preparation time.

It is preferable to conduct the path analysis at the object itself. Only then can good insight be obtained into the nature of the object and the actual weak spots. For example, a path analysis of an important gas storage facility in Den Helder should not be conducted from a department building in The Hague, but at the site itself. To produce valuable results, it is also important to use an out-of-the-box approach. A brainstorming approach, in which the actions of the analyst as potential perpetrator are not characterised as right or wrong, is thus important.

Conducting a path analysis is a complex exercise. In a meaningful path analysis not only are different paths worked out; the analysis is also repeated for different perpetrator profiles. This makes the analysis both laborious and time-intensive. The analyst must ensure that he has adequate time and space to properly conduct such an analysis.

Fault tree analysis

Essence

A Fault Tree Analysis can be used to describe the logical development of undesirable events in a systematic manner. The mode of thinking used for a fault tree analysis is the exact opposite of the chronological process that takes place when an accident occurs.

Preparation, steps and follow-up

The first step in conducting this analysis is to specify the undesirable occurrence. This occurrence is called the main event in the fault tree analysis. Then the immediate causes are identified that can trigger the main event. To be able to identify the underlying causes, these causes are then analysed one for one. The desired level of detail depends on the objective of the analysis.

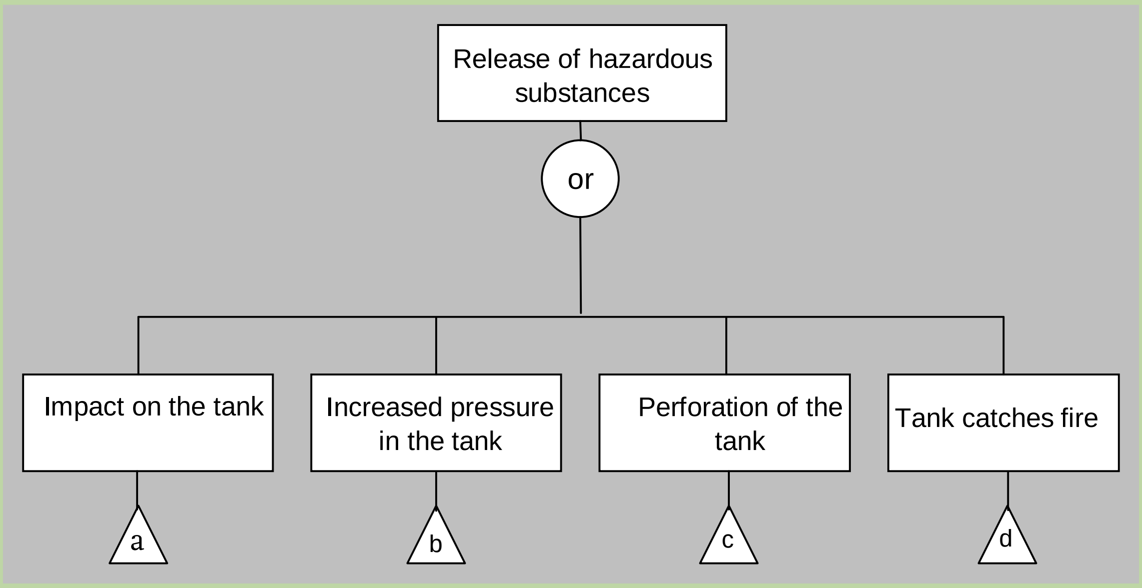
The figure depicts a fault tree analysis for releasing LPG from a tank truck. In this figure the triangles represent the events. The events are linked using so-called 'connectors'. These connectors between the events are 'or ports' (or gates) or 'and ports' (and gates). Triangles represent any possible underlying (more detailed) causal factors. The main event in this fault tree analysis is releasing LPG. Four possible underlying causes are identified, each of which can lead to this occurrence: impact on the tank, the tank catches fire, pressure inside the tank increases or the tank is perforated. In turn, for each of these underlying events, underlying causes can be identified.

Checklist of conditions

An effect or scenario that must be prevented is assumed. The likelihood of that effect is not necessarily taken into account. In order for this type of analysis to produce meaningful results, it is important that you take chances.

Moreover, this model requires sufficient expertise of the service or sector in which the occurrence can occur. The requisite expertise can only be ensured if sector members are involved in the analysis.

The fault tree analysis model should preferably be applied at the object itself. Only then can sufficient insight be obtained into the possible causes of a specific occurrence at that location.



Sources

Helsloot, I & N. Rosmuller (1994) *Jaarboek onderzoek 2000*

Historical analysis (data gathering)

Essence

Based on historical events, what has occurred, exactly what damage was caused and what measures were taken at the time can be systematically mapped out. Filling in this model provides an indication of the chance that specific events may occur and the damage that can be expected if they do, for example in light of the measures taken at that time.

Preparation, steps and follow-up

A historical analysis can take one of two forms. In some cases, the sector or Supervisory Agency may have proper records, for instance, in which case the analysis simply consists of retrieving and interpreting the information. In the other cases, the records may not be as complete or accurate, in which case it is considerably more difficult to find the relevant data and a broad search strategy must thus be employed.

In the first step, the analyst determines what information must be collected. Using this information, a table can be created, similar to the example here, which shows the four factors date, occurrence, measure and damage. In the second step, the data are collected. Different work methods can be envisioned for collection of the data, such as an Internet search, excursion or collection of information delivered in the framework of reporting obligations.

Checklist of conditions

This model succeeds or fails based on the meticulous of the record-keeping regarding events and the comprehensiveness of the information included in the model. What is frequently missing is the organisation’s commitment to keep track of this type of information. Organisations must thus be stimulated (or forced) to keep good records when such risks occur and to make such information public (to the policy staff or the Supervisory Agency).

Date	Occurrence	Measure	Damage
25 January 2000	Fire	Fire department arrives at the scene in a timely manner after proper functioning of the alarm system.	Slight smoke damage to the building.
16 March 2003	Letter containing a potentially dangerous powder	Mail scanning system detects the letter in a timely manner.	Employees from the mail room are examined at the hospital as a precaution; there is no indication of permanent injury.
31 October 2005	Virus in system	IT service intervenes and removes the virus.	System completely down; back-up function functioned properly, so that only those documents that were open in the different software programs at the time the system went down are lost.

18

Persistence method

Essence

The persistence method is based on the presumption that a prediction for a future moment in the time can be made based on a trend in events distinguished from previous years and historical figures.

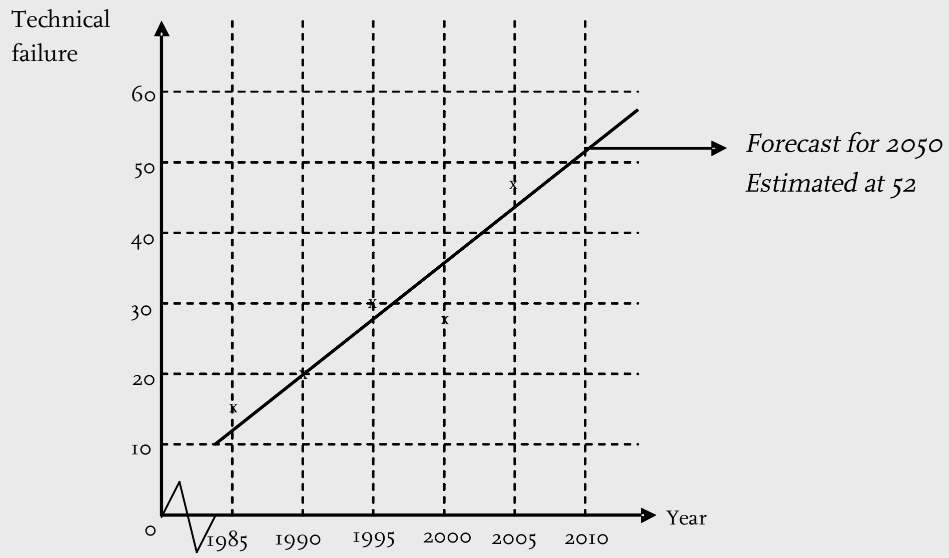
Preparation, steps and follow-up

This model is based on two variables and is simple to use. The time – expressed in hours, days or years, for example - is generally placed on the horizontal axis of the model. The frequency at which the risk occurs is plotted on the vertical axis. The next step consists of meticulously filling in the data in the model, so that one can see how many events have occurred per time unit. An “average line” is then drawn through the points included in the model; in most cases, there are also a few exceptions. Drawing this trend line makes it possible to make an estimate of the frequency with which the risk will occur in the (near) future.

If large, increasing numbers are involved, such a forecast can be extremely important in terms of being able to take the right measures. Certainly this applies if the trend conforms to a logarithmic function.

Checklist of conditions

The model provides a trend based on and extrapolated from historical data. The level of certainty is thus limited and is only indicative. This must be taken into account when interpreting the results.


Technical failure
60
50
40
30
20
10
0
1985
1990
1995
2000
2005
2010
Year
Forecast for 2050
Estimated at 52

Trend Impact Assesment (TIA)

Essence

Many methods for risk analyses presuppose a certain level of continuity and predictability. Risks to be anticipated should (must) be based on what has occurred in the past.

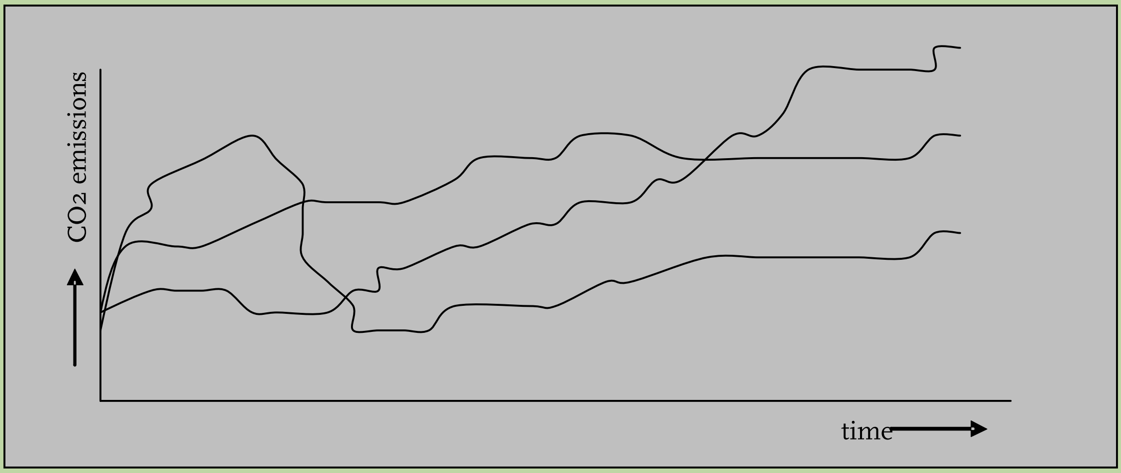
Trend Impact Assessment (TIA) assumes that future events (such as policy changes but also technological breakthroughs) can cause changes in the trends. Thus, a TIA attempts to estimate what factors or sudden events could initiate such changes, how probable it is that such changes might occur and how this would influence the variable being studied in the risk analysis. A TIA forces the analyst to think about what important events might occur in the future, based on which assumptions can be worked out more explicitly and a more detailed image of the future can be obtained.

Preparation, steps and follow-up

Step 1. The first step in a Trend Impact Assessment is to specify the trend to be investigated. This can be a variable such as the CO2 emissions in the figure, but it could also be the price of oil.

Step 2. A second step is to determine the timeframe the analysis is to cover. In some situations, it makes senses to plot the possible trend developments for the coming fifty years; in other cases a timeframe of a few months or a year is sufficient. This depends in part on the frequency with which possible events will occur.

Step 3. Then an initial trend is sketched of (in this case) the CO2 emissions should occurrence A (e.g. refining the regulations) occur at a particular moment. The impact this occurrence is expected to have on the development of CO2 emissions over time is shown in a curve on the graph. In the following steps, this exercise is repeated for occurrence B (and possibly C, etc.), until the impact of all possible events in the Trend Impact Assessment have been worked out. Methods for identifying possible events include exploring the literature, a brainstorming session or the Delphi Method.



Checklist of conditions

In When applying this model it is important to include *all* possible events in the analysis, both the realistic ones and the unlikely ones. This means that variety in the team of analysts is one condition for success. An expert meeting that includes a brainstorming session is a suitable work form for this.

The model requires a sufficient level of expertise. Involvement of experts from the sector as well as from research institutes and knowledge institutions is thus a condition for arriving at meaningful predictions.

The predictions from such an analysis are only useful for a short time. New developments occur and new insights regarding the anticipated impact of events must be continually collected. To increase the value of the predictions, the Trend Impact Assessment must be repeated periodically based on new insights (depending on the timeframe selected).

Scenario analysis

Essence

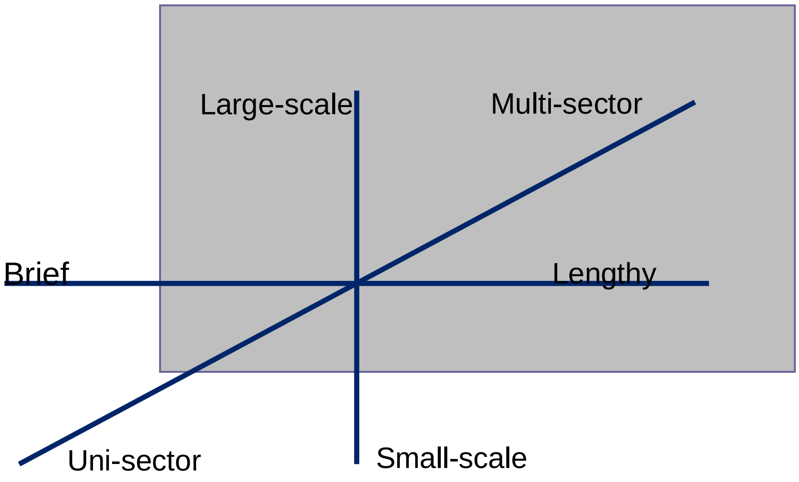
Scenario analysis can be helpful in plotting the relevant risks that can occur in a specific sector or with regard to a specific product or service in the future. Using scenarios, statements can be made regarding the robustness of the (precautionary) measures (being) taken in a specific sector or for a specific service and whether or not additional measures are needed

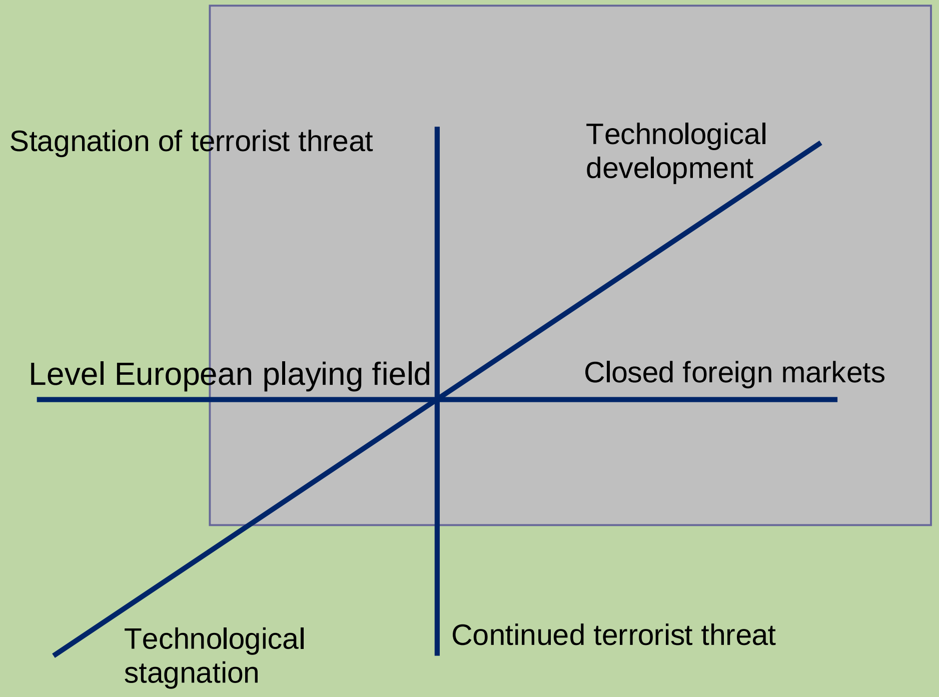
Preparation, steps and follow-up

A scenario analysis can be conducted using two approaches. In the first approach trends or future images are plotted using selected axes. Based on Shell's experiences in the seventies, Von Reibnitz (1988) and Schwartz (1993) developed a step plan for designing scenarios using this approach:

1. Specify the core question
2. Specify the factors or crucial forces in the sector or service environment
3. Specify the driving forces or mega trends behind these factors (e.g. international economic development)
4. Arrange factors and forces on the basis of interest and lack of certainty (only include factors whose development is uncertain and that can have a significant influence on the sector or service to be analysed.)
5. Design the scenario logic (the factors and driving forces that still remain after step 4 forms the axes of the possible future scenarios.)
6. Detail the scenarios
7. Evaluate the core question by going through the scenarios and drawing conclusions regarding possible measures.
8. Monitor developments: are the conclusions still relevant after the passage of time?

In a second approach, the risk dimensions are used to draw up the scenarios. The dimensions of these risks can be: large-scale versus small-scale, multi-sector versus single sector and lengthy (disruption) versus brief (disruption). This produces a three-dimensional model that serves as a point of attention when formulating scenarios. When creating a good scenario, these three axes are explicitly and consciously considered. In the framework of the Protection of Vital Infrastructures Projects, for example, the combination multi-sector and lengthy is interesting, in part because this type of analysis has clearly not yet been conducted in other policy processes.




Stagnation of terrorist threat
Technological development
Level European playing field
Closed foreign markets
Technological stagnation
Continued terrorist threat

Applying the scenario analysis preferably demands a broad, out-of-the-box approach. This way an environment is created that produces the most complete image of possible future events and scenarios possible. An appropriate work form when applying this model is a workshop or simulation that includes analysts from knowledge institutions, companies and government agencies.

Checklist of conditions

When developing scenarios, there is the danger that the analyst will focus too on extreme situations while ignoring or downplaying more obvious (but no less important) risks.

Moreover, when applying this model it is also important to think about scenarios within scenarios. For example: How do people react during a power disruption (e.g. no electricity during a flood)? Will it be possible to utilise all the electricity company's repairmen for repair activities or will some of them be busy trying to save their own submerged or damaged home? Will a nurse in such a situation be available for work in the public domain or will she first want to tend to those in her private environment?

Sources

D. de Weger (et al), Leidraad scenario-analyses voor ongevallen in tunnels, COB Bouwdienst Rijkswaterstaat, mei 2004

Schwartz, B, Forecasting and scenarios, in Handbook of system analysis, eds. H.J. Miser and E.S. Quade, Wiley, Chichester

Classifications for type and scale of the effects

There are numerous classifications that can be used to map out the types and scale of effects.

A good example is the five categories shown in the table below. The table also includes a classification of the scale of the effect: low, middle and high. The values proposed here are indicative. The risk analyst can also use other values depending on the object of the analysis. For example, if risks are studied that can lead to a maximum of 20 deaths, then the intervals 'less than five deaths' (= low), 'between 5 and 10 deaths' (=middle) and 'more than 10 deaths' (=high) can be used, for example. That leads to a greater level of precision than the intervals used in the following table for that point. Another type of classification that has proved popular is the classification based on six categories used specifically to maintain:

- Physical integrity
- Social living climate (quality of life)
- Financial-economic
- Nature
- Environment
- Government-administrative image

If damage to people is involved, in conformance with Perrow a distinction can still be made between types of victims. Four types are distinguished in the following table, which uses the example of an airline crash:

First type of victim	Operators of the system (pilots or factory employees)
Second type of victim	Involved in the system, but cannot exert any influence on it (airline passengers)
Third type of victim	Not involved in the system (residents of the Bijlmermeer at the time of the airplane crash)
Fourth type of victim	Second generation victims (from the effects of radiation)

Category	Criterion	Low	Middle	High
Persons	Number of dead of severely injured	Fewer than 100 dead or severely injured victims	Between 100 and 1000 dead or severely injured victims	More than 1000 dead or severely injured victims
Animals	Percentage of dead / seriously injured for the groups: pets, small farm animals, large farm animals. Note: this is not the economic (or material) value but the immaterial value of these products	Less than 20% of the livestock	Between 20% and 60% of the livestock	More than 60% of the livestock
Environment	Surface affected area	Less than 1000 km²	Between 1000 and 10,000 km²	More than 10,000 km² (more than a third of the surface are of the Netherlands)
Material damage	Damage expressed in euros	Less than 1 billion euros	Between 1 and 10 billion euros	More than 10 billion euros
Immaterial damage	The number of people who experience a malfunction in the daily state of affairs	Consequences for less than 20% of the population	Consequences for between 20% and 50% of the population	Consequences for more than 50% of the population

A body such as the AIVD conducts a likelihood/effect-type analyses in the framework of the Protection of Vital Infrastructures Projects based on the following quantification of the likelihood on the one hand and the effect on the other:

Chance	Factor
Not realistic	0
Not probable	1
One in a million	2
Once in 50,000 years	4
Once in 5000 years	8
Once in 500 years	16
Once in 50 years	32
Once in 5 years	64
Once in 6 months	128
Once a month	256

Thus, 10 categories of likelihood are defined. When the order of scope is involved 8 categories of effects are used, with the effects expressed in monetary terms:

Effect	Factor
Less than /equal to 2000 Euros	1
Between 2000 and 10,000 Euros	2
Between 10,000 and 100,000 Euros or a few victims with mild injuries	4
Between 100,000 and 5 million Euros or many mildly injured, dead or severely injured victims	8
Between 5 million and 100 million Euro or up to 10 dead or severely injured victims	16
Between 100 million and 1 billion Euros or up to 100 dead or severely injured victims	32
Between 1 and 5 billion Euros or between 100 and 1000 dead or severely injured victims	64
More than 5 billion Euro or more than 1000 dead or severely injured victims	128

Because the categories for likelihood and effect increase logarithmically, the scores that can be linked to them also increase logarithmically. That is why a quadratic increase was chosen. A simple example is offered. A person wants to decide whether extra measures need to be taken to prevent bicycle theft, for example by buying a ‘U’ lock. The effect of a stolen bicycle small and - if a normal bicycle is involved that costs less than 2000 Euros - the score is 1. However the chance that the bicycle might be stolen (or destroyed) is considerable, since the bicycle is stored at Amsterdam Central Station every day and sometimes over the weekend: at least 5 times a year. That results in a score of 64. Multiplying 1 times 64 results in a risk of 64 units.

In the classic manner, the seriousness of a risk is weighed by multiplying the likelihood that the risk will occur by the amount of the damage. This creates likelihood-effect models, described below. But according to Klinke & Renn (2002) risks are evaluated by many more criteria than simply the likelihood that the risk will occur and the extent of the damage. The following table shows these criteria, including likelihood and effect. Telecommunication is used as an example.

Indicators	Description
Extent of the damage (‘effect’)	This involves the negative effects of not having telecommunication services and networks available, such as the number of dead or seriously injured victims, the material damage expressed in euros, the number of people faced with the malfunction in their daily activities, etc.. Here a distinction is made between the direct damage and the indirect damage as the result of chain dependencies.
Likelihood of occurrence (‘likelihood’)	Estimate of the relative frequency of discontinuity in telecommunication services and networks
Potential for mobilising forces	Describes the (anticipated) societal reaction by people or organisations who face these risks. This can be citizens, companies, interest groups or politicians.
Externalities	Indicate whether and to what extent external effects are involved for the risks in question
Understandability	To what extent can causal links between (potential) causes and consequences be identified and quantified? This involves an overall indicator for different components that interpret the (lack of) certainty surrounding this
Ubiquity	Defines the (re-)distribution of potential damage
Reversibility	Describes the possibility to restore the environment to the state it was in before the damage occurred
Recovery time	Defines the time that lapses between the initial occurrence, such as failure of a telecommunication service, and the moment the environment is restored to the state it was in before the damage occurred
Delaying effect	Failure characteristic; defines the time that lapses between the initial occurrence and the moment the damage resulting from that occurrence occurs

This table contains both ‘physical’ and ‘psychological’ indicators. The psychological aspect is important, because it can dramatically influence the government’s agenda, particularly that of politicians. The discussion regarding radiation from GSM towers is an example of this. Physical effects have not yet been demonstrated, but psychologically this is a social problem. For example, people relocate because they live close to such a tower, only to discover that there is a tower in the new environment and they are powerless to do anything about it.

Sources

Klinke A. & O. Renn (2002) A new approach to Risk evaluation and management: Risk-Based, Precaution-Based and Discourse-Based strategies, In: Risk Analysis: an international journey: an official publication of the Society for Risk Analysis, Vol. 22, afl.6, pp.1071-1094

22 Cause Consequence Analysis (CCA)

Essence

A Cause Consequence Analysis (CCA) is a combination of a Fault Tree Analysis and an Event Analysis. This method combines a Cause Analysis with a Consequence Analysis. The objective of a CCA is to identify chains of events that can result in a undesired final event. When the different events are familiar or can be calculated, this model can be used to completely chart the risks of the system.

Preparation, steps and follow-up

The Cause Consequence model asks the following two questions:

- What can go wrong?
- What (serious) consequences can that have?

Step 1. As the example in the figure shows, the first step in the model is selection of the starting event. Then the following two questions are posed:

- What will happen if the reaction to the starting event *is* adequate?
- And what will happen if the reaction to the starting event *is not* adequate?

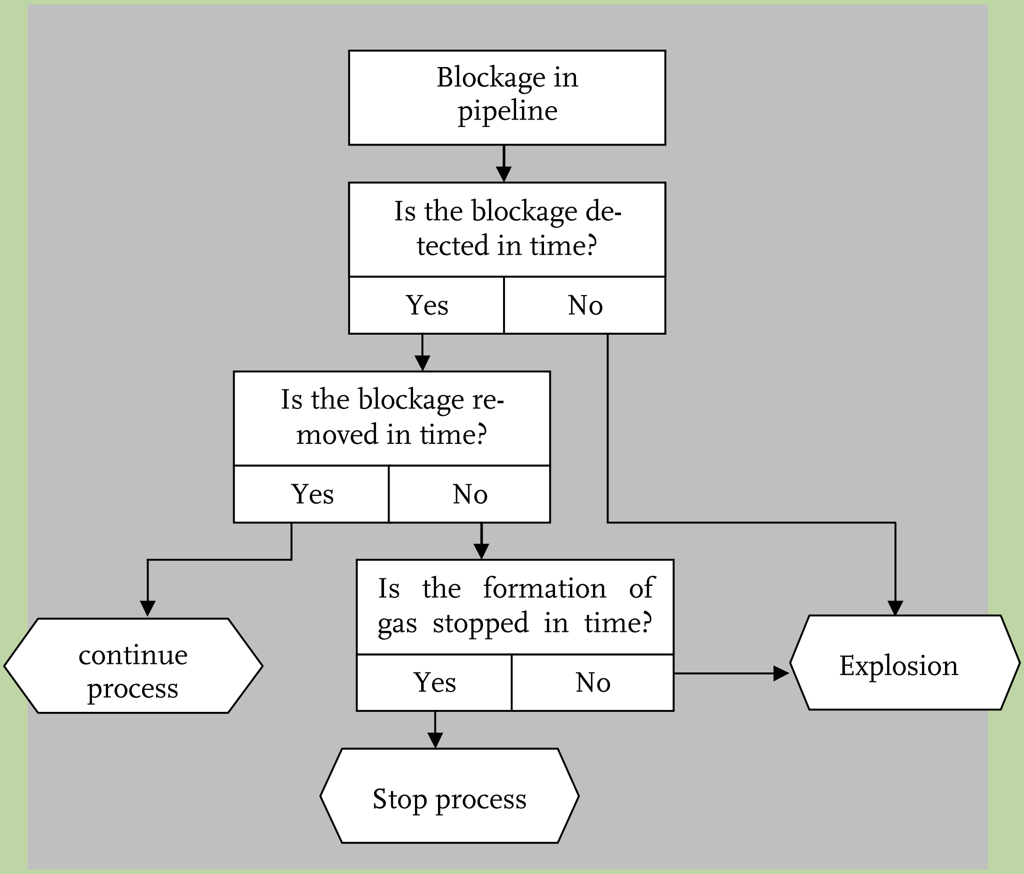
Step 2. In this step, the subsequent events for both situations are described and the question of what will happen if the reaction is adequate and what will happen if the reaction is inadequate is posed.

Step 3. The steps described above can be repeated until a final event is reached for each of the situations described in the model. For the starting event 'blockage in the pipeline', the model describes three possible consequences (for different reactions): continuation of the process, termination of the process or an explosion.

Checklist of conditions

To use this model, expertise in the sector, product or service under investigation is required. Global analysis is inadequate. Plotting the different effects of a single starting point is only useful if all possible consequences are identified at detail level. To ensure that the requisite expertise is available, it is important to involve parties from the sectors involved in the analysis process.

As is the case with path analysis, execution of Cause Consequence Analysis should be executed directly on the object involved to ensure that the proper insight is obtained into the nature of the object and the real weaknesses involved.


Blockage in pipeline
Is the blockage detected in time?
Yes
No
Is the blockage removed in time?
Yes
No
continue process
Is the formation of gas stopped in time?
Yes
No
Explosion
Stop process

Sources

Center for Chemical Process Safety; "Guidelines for Hazard Evaluation Procedures; 2nd Edition with Worked Examples" 1992 (461 pp); American Institute of Chemical Engineers

Burdick, G.R. and J.B. Fussell; "On the Adaptation of Cause- Consequence Analysis to U.S. Nuclear Power Systems Reliability and Risk Assessment;" in "System Reliability and Risk Assessment," JBF Associates, Inc., Knoxville, TN, 1983

Lees, Frank P.; "Loss Prevention in the Process Industries;" Buttersworths; 1983 (1316 pp – two volumes)

Greenberg, Harris R. and Joseph J. Cramer; "Risk Assessment and Risk Management for the Chemical Process Industry;" Van Nostrand Reinhold; 1991 (369 pp)

23 Chance-effect matrix

Essence

A chance-effect matrix is a model that describes the link between the chance and seriousness of a risk. The model has two axes: the effect (or the consequences) that a threat produces and the chance of the threat occurring. A risk in the white area can be considered less serious than a risk in the shaded area of the matrix. In cases in which a logarithmic scale is used, the colours in the matrix take on a different distribution.

The model is particularly feasible because of its simplicity and the possibility of viewing and comparing different threats at a single glance. The model is appropriate for use as a quick scan, but can be used for other purposes as well.

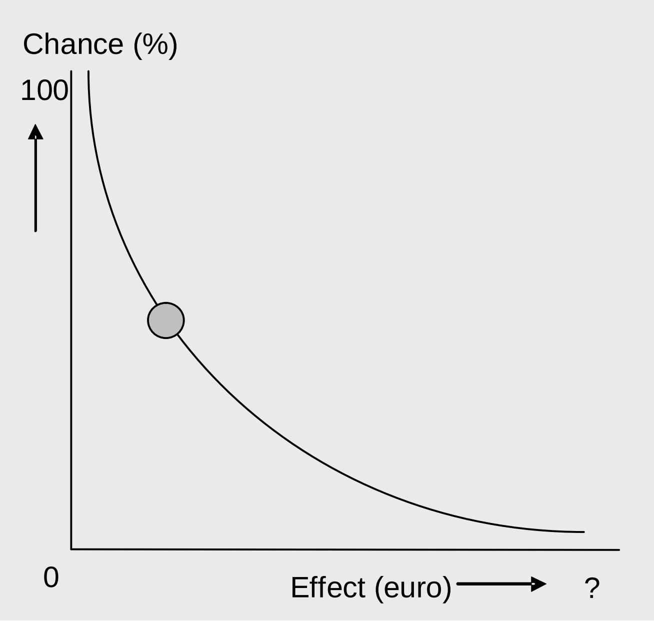
Preparation, steps and follow-up

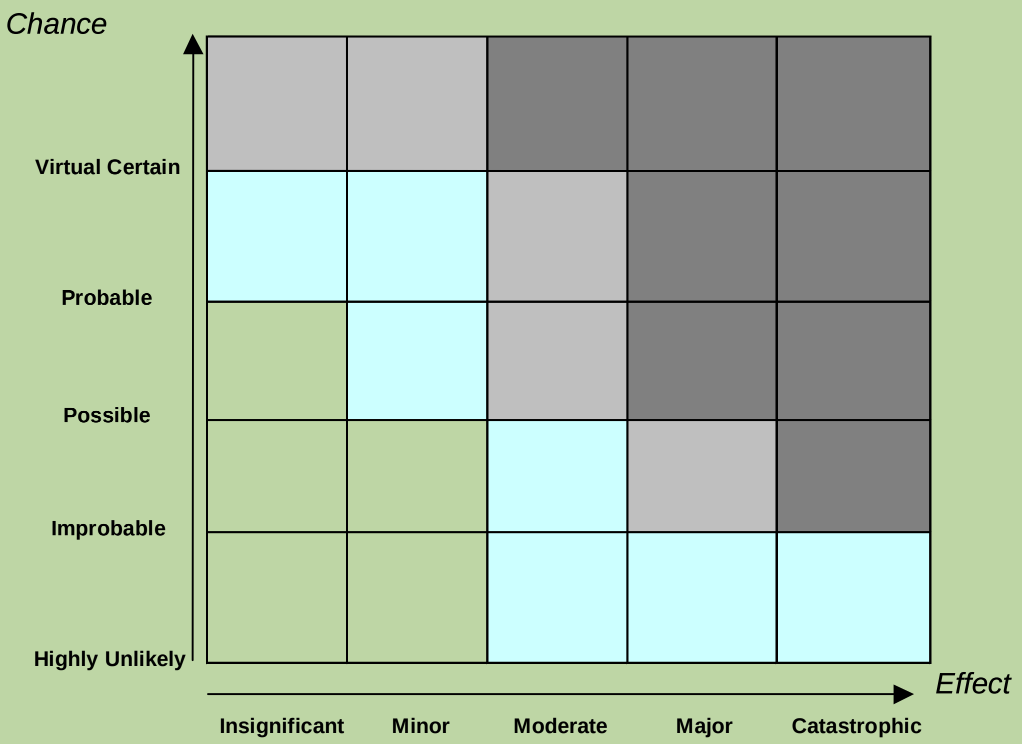
Step 1. The first step in the application of the chance effect matrix is to determine the set of events for which the chance-effect combinations must be charted. Depending on the objective of the risk analysis, the possible events can be determined based on a deed-perpetrator analysis or use of the cause consequence-model. The set of events can be reduced using ranking techniques.

Step 2. The next step is to determine the categories on the axes of the matrix. In the figure, the axes consist of five unquantified categories. The chance of a threat (vertical axis) is divided into five chance categories: from very probable to very unlikely. The horizontal axis shows five effect categories: from catastrophic to insignificant.

Another option is to assign values to the categories, e.g. chance can be expressed in exact percentages, for instance, or in multiples of 20%: 0-20%, 20-40%, etc. The central question is: how large is the chance that a specific effect will occur as a result of a specific occurrence. The effect can expressed in money, for instance, or in the number of fatalities.

Additionally, an exact scale or a cumulative scale must be selected. On an exact scale, the chance of a specific occurrence can be directly tied back to a value of X for the damage if that specific occurrence becomes a reality (e.g. X fatalities). A cumulative scale, on the other hand, shows the chance of X or more fatalities for a specific occurrence. The latter classification is frequently used in cases in which it is difficult to give an exact estimate of the damage resulting from an occurrence. The magnitude of the damage depends on a multitude of different factors and exact predictions regarding whether or not all or some of these factors will arise are impossible. An example of a chance-effect matrix based on a cumulative scale is given below.





The cumulative chance-effect matrix in the figure shows the chance of an effect of X Euros in damage or more for a specific event. The chance of 0 Euros in damage is always 100%. After all, the effect 0 Euros or more includes all possibilities (including the possibility that nothing will happen). The figure also shows that the chance of infinite Euros in damage is estimated at zero. The slope of the graph depends on the specific characteristics of the occurrence, including the development of damage in time. Suppose, for instance, that the figure represents ICT breakdowns in an organisation. Also suppose that this organisation can switch to existing fall-back infrastructure within minutes of a breakdown at all times. In that case, the damage will probably not increase very quickly and can also be estimated with reasonable precision in advance.

Step 3. In this step, events are positioned in the matrix (in the case of an exact matrix) and lines are constructed in the case of a cumulative analysis. The coloured areas of the matrix indicate critical chance-effect combinations or low-urgency chance-effect combinations.

Step 4. At this point, the possible measures can be explored. The events in each cell of the matrix can each be analysed in advance to determine whether they must be paired with new measures. This can be achieved by multiplying the chance and effect. However, this does not yet complete the analysis. In some cases, for instance, the product of chance and effect does not form a convincing incentive for the deployment of measures because the chance of a specific event occurring is extremely small. However, the possible effect can be so great that allowing the threat to exist unchecked would be completely unacceptable. In other words: events with an extremely small chance, but an enormous impact probably will require preventive measures. Similar reasoning applies to events that occur frequently, but have little effect. This is why the graph for this model shows an ellipse that includes the upper left-hand quadrant and the lower right-hand quadrant. Measures are always required for events in the upper right-hand quadrant.

On one hand, the measures can be designed to prevent an event or reduce the chance of the event occurring, while they can also be designed to limit the effects that an occurrence of the event has on the other.

Because making predictions regarding the chances and effects of events that have never before occurred is not a simple task, a working structure based on brainstorming, with expert participation, is a self-apparent choice. In other cases, historical data on malfunctions can be used: the historical analysis model (or data gathering).

Checklist of conditions

An adequate level of expertise in the service or sector under investigation is required to use this model. The knowledge of content required to estimate chances and, particularly, the effects of events, can only be guaranteed if sector and knowledge institutions are involved in the analysis. One danger here is that non-experts can become too involved in chance estimation or effect estimation, e.g. in a group meeting. Another danger is that the first estimate can be accepted as valid by one of the participants, while others intuitively feel that the estimate is incorrect, but feel that they are unable to raise the issue, e.g. because argumentation for their intuitive standpoint does not exist. Furthermore, the fact that the values of results generated using this model depend on the composition of the team of analysts must be taken into effect. After all, scoring events with corresponding risks can be based in part on personal perceptions of the effects.

Finally, it is important to note that the team of experts required to estimate the chance of an event may be an entirely different team than that required to estimate the effects of the event. This is true, for instance, in cases involving chance and effect estimates for conscious human acts. The AIVD has a great deal of knowledge in the area of chance estimation, while sectors such as the energy and telecom sector have greater insight into the magnitude of the damage (i.e. the effect).

Sources

Dunn, M. & I. Wigert, (2004) *CIIP Handbook 2004, Critical Information Infrastructure Protection: An Inventory and Analysis of Protection Policies in Fourteen Countries*, p. 236

24

Impact of risk in time

Essence

This model shows how the impact occurs in the event of a malfunction.

For some risks, the effect immediately after the manifestation of the risk is as great as the effect as time progresses (risk 3). For other risks, however, the effect increases as time progresses (risk 2). For some risks, the negative effect decreases as time progresses (risk 1). In such cases, the system, product or service has self-recovery capacity.

Insight into the progression of the impact is extremely important if effective measures are to be deployed. After all, if the effect increases with time, there is also a chance to recover after the malfunction, thus preventing a more serious effect. However, if the effect decreases in time, which means that the effect is greatest immediately after a malfunction, then return on investments in preventive measures will be greatest: preventing the malfunction from occurring in the first place. In addition, in situations in which the effect remains unchanged as time progresses, the adequate deployment of measures is of less importance than in situations in which the effect increases without the deployment of measures.

Preparation, steps and follow-up

As preparation for use of this model, a chance-effect analysis can be performed to provide an initial overview of the events that may require measures. The model described here can then be used to deepen insight into the damage: is the damage instantaneous or does it occur as time progresses? This insight is also important when proposing measures. A historical data analysis (data-gathering) may also be helpful because it allows collection of reliable information on the impact in time.

The following steps can be distinguished:

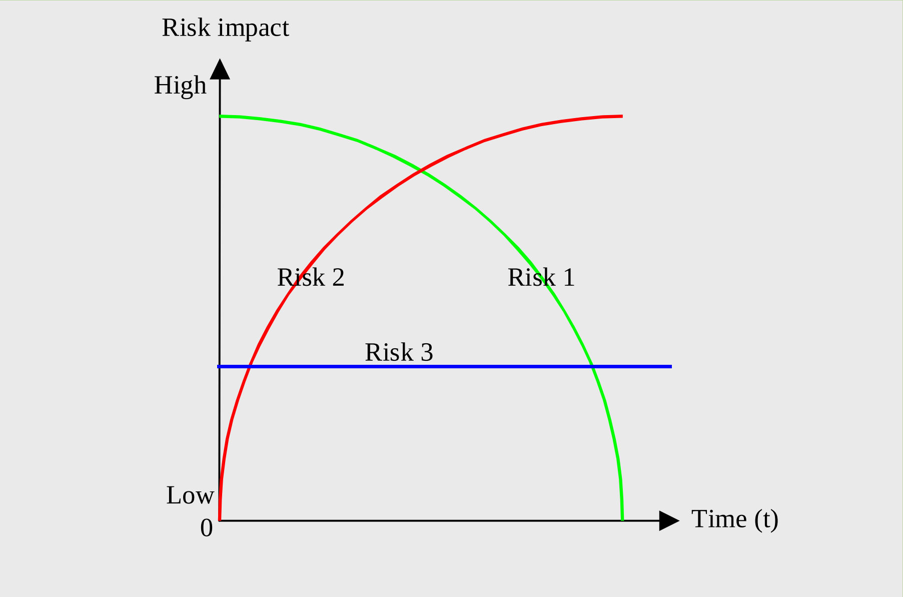
Step 1. Select the events for which the impact in time must be charted.

Step 2. Define the appropriate axes units. Hours can be placed on the horizontal axis, for instance, or days, months or any other unit of time. The dimensions used on the vertical axis for effects must also be defined. The choices in this regard depend on the product or service involved. If the analysis involves a product for which the impact displays greater fluctuation immediately after a malfunction, for instance, use of hours on the scale may be a relevant choice.

Step 3. Construct the impact line.

Step 4. Define the consequences with regard to required measures based on the impact lines. As mentioned above, different types of impact in time require different types of measures, with deployment of preventive measures on the one hand and deployment of repressive measures on the other.

To develop greater depth in the consideration of possible measures, use of the Impact-Recovery Model after using this model can be useful. The Impact-Recovery Model is described below.



Checklist of conditions

Analysing risk in time requires specific knowledge of a product or service. This model is therefore less appropriate for use in group meetings with participants with expertise in different areas.

Much of the requisite information can be derived from historical data analyses and error logs. Use of such resources is a basic point of departure for this model.

Sources

Henley E. en H. Kamamoto (1981) *Reliability engineering and risk assessment*, Englewood Cliffs: New York. (p. 180)

Papazoglou, M., & Heuvel, W.J.A.M. van den (2000). Configurable business objects for building evolving enterprise models and applications. In: W.M.P. van der Aalst, J. Desel, & A. Oberweis (Eds.), Business Process Management: Models, Techniques and Empirical Studies (LNCS, 1806) (pp. 328-344). Berlin: Springer-Verlag.

25 Impact-recovery matrix

Essence

The chance-effect matrix charts the relationship between chance and effect (impact). This matrix does not take into consideration the fact that impact does not suddenly appear, but can also develop and fluctuate over time. It also does not explicitly take into consideration the fact that recovery from specific events can have specific characteristics. After all, recovery may only be possible in the longer term in some cases.

The matrix above shows the link between impact and recovery speed. The principle is derived from the so-called Markov chains.

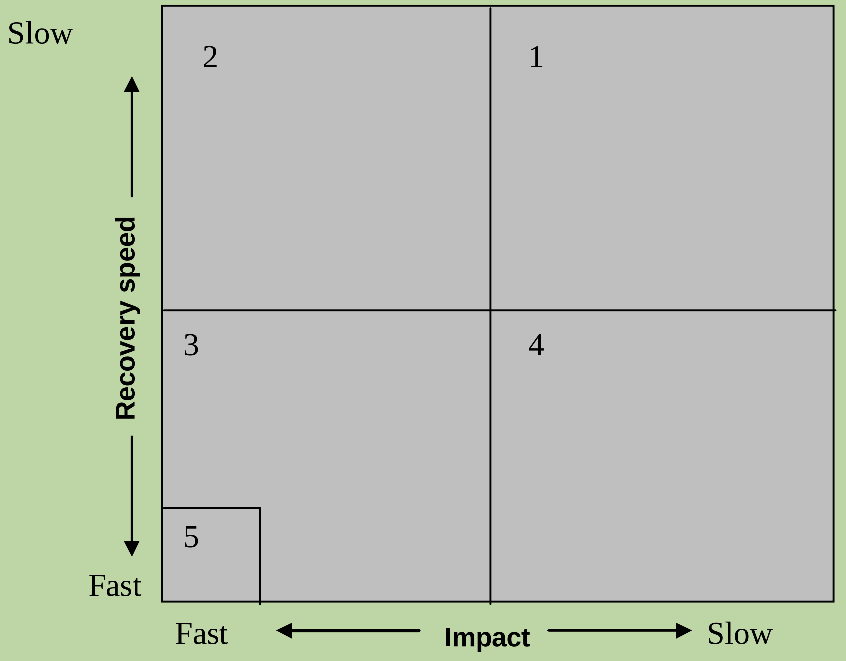
Preparation, steps and follow-up

As preparation for this model, chance-effect analyses, analyses of the impact of the risk in the time and historical data analyses can be performed. The model described here can then be used to determine what repressive measures are advisable and to provide argumentation for deploying preventive measures rather than repressive measures that would have limited effect.

Step 1: Select the events and malfunctions that are to be analysed. For example: an analysis in the framework of the project Protection of Vital Infrastructures could use a global list of vital products and services, similar to the one included in the 'checklist of initial events'. Pre-selection of the most important events and malfunctions is a self-apparent preparatory activity.

Step 2: Position the events and malfunctions in the model.

Step 3: Exploration of possible measures. The different types of events and malfunctions require different approaches. Should investments be made in measures to limit the risk in the preventive phase or should investments be made in measures in the response phase to limit the risk? Obviously, this consideration must be based in part on the duration of recovery and the impact of the risk involved.



The table below gives suggestions regarding where the focus can be placed:

	Category	Type of measure
1	Slow impact, slow recovery	A combination of preventive and repressive measures is self-apparent, but the accent should be placed on prevention. After all, recovery takes a long time.
2	Fast impact, slow recovery	Strong accent on preventive measures. Recovery is always too late.
3	Fast impact, quick recovery	On the one hand, repressive measures that can be deployed quickly. Extra attention is required for proper preparation of these measures, so that they can also be applied immediately in the event of malfunctions.
4	Slow impact, quick recovery	Accent on repressive measures. There is enough time for these measures.
5	Very fast impact, very quick recovery	On the one hand, repressive measures that can be deployed very quickly. Extra attention is required for proper preparation of these measures, so that they can also be applied immediately in the event of malfunctions.

Checklist of conditions

Use of the model requires technical knowledge of the recovery characteristics accompanying the malfunction, which means that contributions of specific expertise must be made.

The danger to be avoided in using this model is use of the model as an objective in itself rather than as an instrument for the development of appropriate measures.

Bronnen

TNO: FEL 03-C002: Bescherming vitale infrastructuur: Quickscan naar vitale producten en diensten.

Harn, K. van & P.J. Holewijn (2003) *Markov-ketens in discrete tijd*, Epsilonuitgaven: Utrecht

26 Event tree

Essence

An event tree can be used to determine what sequence of events will result in a specific level of damage, also in quantified terms. The model graphically depicts the events and resulting damage. The risk is the starting event mentioned in this case. An event tree shows how this starting event in combination with the occurrence or non-occurrence of subsequent events leads to specific consequences.

Drawing up an event tree is particularly helpful in situations in which the starting event and subsequent events can have several different types of consequences. If only one consequence is important, a fault tree analysis is more appropriate

Preparation, steps and follow-up

In During preparations, the relevant initial events are selected and prioritised.

Step 1. An event tree begins with the starting event, which is shown to the far left of the tree.

Step 2. Add subsequent events. The subsequent events occur as a consequence of the event they follow and are depicted to the right of the previous event.

Step 3. Add branches to the tree. For each subsequent event, the possible consequences are shown as branches (e.g. 'event occurs' and 'event does not occur'). Systematically defining each branch results in the consequences of the different combinations of events in each branch of the event tree.

An event tree can be used to quantify the chances of the different events, but the chance of the starting event occurring must be specifically defined, as must the chance of each subsequent event occurring or not occurring. For each complete branch in the event tree, the chances of events in the branch occurring can be quantified by multiplying the chances in the branch in question. When drawing up the event tree and calculating the chances of the events, various types of software can be used.

Checklist of conditions

The model is an outstanding tool for concrete situations, making contributions to the collection of very detailed information. It is particularly helpful when used with software to generate clear, quantified conclusions.

One disadvantage of the model is that the it does not take factors into account that appear in the first instance to have no influence and are therefore excluded from analysis, e.g. external factors. This can result in conclusions that do not correspond completely with the actual situation.

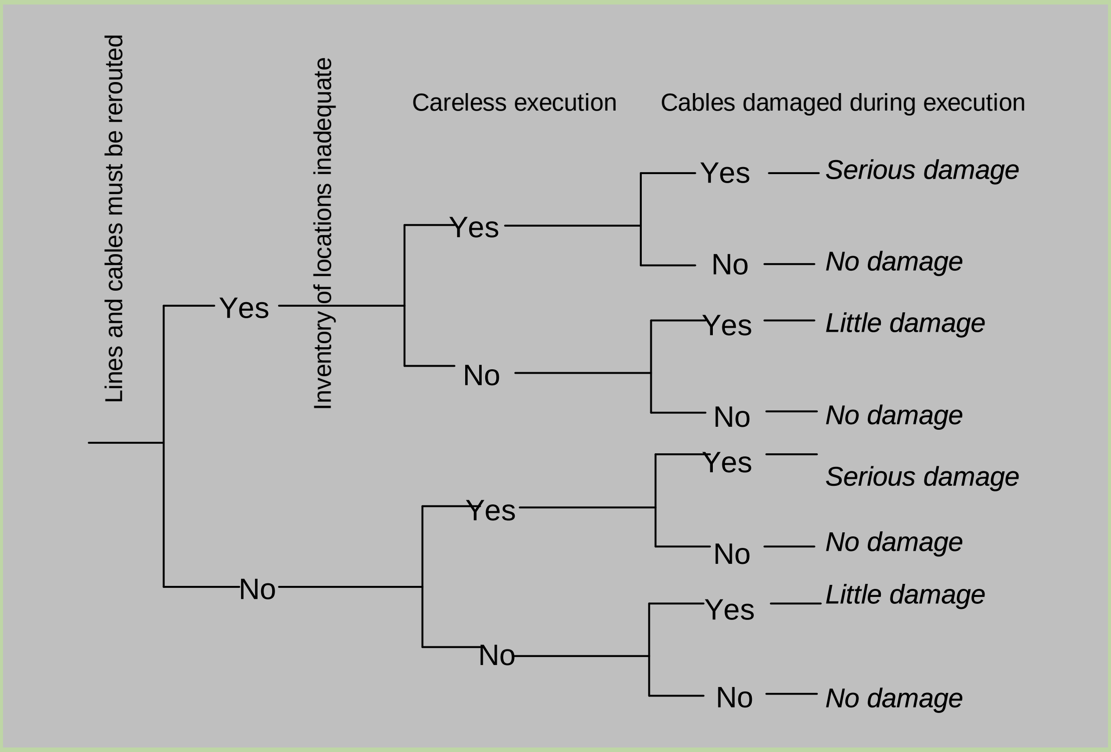
It is important to select a restricted set of appropriate initial events to limit the size of the analysis.

Sources

www.risman.nl

www.event-tree.com

Belm, G.K. & B.F. Hobbs (1997) Event Tree Analysis of Lock Closure Risks, In: *Journal of water resource planning and management*, Vol. 123, adfl. 3, pp. 169-178


Lines and cables must be rerouted
Inventory of locations inadequate
Careless execution
Cables damaged during execution
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Serious damage
No damage
Little damage
No damage
Serious damage
No damage
Little damage
No damage

27 Prioritise vulnerabilities

Essence

Using the preceding model, vulnerabilities and the seriousness of the vulnerabilities can be prioritised per management area. Additionally, levels are distinguished in the model, e.g. individual citizen level, company level and national and international level. This model is particularly appropriate in situations in which the responsibility for the eradication of the different vulnerabilities is fragmented. The management of vulnerabilities may lie in the hands of a company in some cases, while it lies in the hands of national or even international government in others.

Preparation, steps and follow-up

A starting events model can be used as preparation for this model. The starting events model can be used to specify the most important vulnerabilities.

Then the following steps can be distinguished:

Step 1: Prioritise the initial events so that the most important vulnerabilities appear at the top of the matrix and the less important events at the bottom. Before prioritising the events, a list of criteria for assigning a vulnerability a high or low priority must be drawn up.

Step 2: The second step is to determine the relevant management areas. In this example, a distinction is made between citizen, company, national and international. However, in another situation, inclusion of other categories may be relevant, e.g. regional.

Step 3: In this step, the responsibilities of the 'managers' with respect to the different vulnerabilities are charted. In the figure, a distinction is made between three types of responsibility. The red areas indicate that the party involved has a high level of responsibility for vulnerability. A light grey area indicates that deployment of measures to limit vulnerability is not the responsibility of the party in question. Based on this analysis, an implementation plan can be drawn up to specify the actors (management areas) responsible for eradicating vulnerabilities. The most suitable options can be determined for the different types of actors based on the applicable criteria. In this context, a Costs Benefits Analysis or a Vulnerability Analysis can be a useful instrument

Checklist of conditions

The value of the results depends on the composition of the risk analysis team. This must be taken into consideration when interpreting the results.

Because the prioritisation of vulnerabilities is largely based on the seriousness perception of the analyst using the model, a team of analysts with different backgrounds can be useful when using this model. Work studio sessions and expert meetings are therefore appropriate work forms.

Sources

Luiijf, Eric, M. Klaver, J. Huizinga. The Vulnerable Internet: A study of the Critical Infrastructure of (the Netherlands Section of) the Internet. Den Haag, 2001.

Most important Internet vulnerabilities	*Beheergebied*			
	Burger	Bedrijf	nationaal	Internationaal
Service integrity & privacy	🟥	🟥	🟥	🟥
Virusses and Trojans		🟥	🟥	🟥
(Distributed) denial-of-service attacks	░	░	🟥	🟥
Lack of basic security		▓	🟥	🟥
Facilities (electricity)		▓	🟥	▓
Capacity (SPoF, quality of service)	▓	▓	🟥	▓
Computer criminality		▓	🟥	🟥
Inadequate education/training	░	░	▓	▓
Mobile Internet access	░	░		
Chain dependencies	░	░	░	░

🟥	Priority 1
▓	Priority 2
░	Priority 3

28 Security chain actor analysis

Essence

Security Chain Actor Analysis is a methodology that is particularly appropriate for the generation, selection and prioritisation of measures. The model is a tool that can be used to identify the measures the different types of actors –government, sector and end-user – can deploy in the different phases of the security chain..

Preparation, steps and follow-up

As preparation for this model, the impact-recovery matrix can be applied to obtain insight into the most important phases of the security chain in which measures must be applied. Subsequently, preventive measures can be generated to limit the chance of events with a large impact and slow recovery time.

Step 1. The first step in the application of the security chain analysis is drawing up the matrix. The five links in the security chain can be defined as follows:

- Pro-action: measures that stop an event from occurring (e.g. structure and design of buildings, shopping centres and public space).
- Prevention: measures that decrease vulnerability by reducing the chances of an event occurring (e.g. security measures, permits, screening, surveillance).
- Preparation: measures to reduce the impact or damage caused by the occurrence of an event (e.g. training, drills, and back-ups).
- Repression: measures that reduce the duration of a malfunction or calamity to a minimum and that support recovery to the ‘normal situation’ as quickly as possible.
- Follow-up care: measures related to issues such as financial settlement (e.g. legislation to make reimbursement by insurers of specific types of damage mandatory, mandatory insurance deductible for certain types of damage).

The distinction between government, sector and end-user is relatively global. Depending on the issue involved, a more refined classification structure can be used. In the case of ‘government’, for instance, a distinction can be made between policy, execution and supervision or between the different layers of government (central, regional, local government). In the case of ‘sector’, for instance, a distinction can be made between the different links in the industrial column of a given sector. In the case of ‘electricity’, for instance, a distinction could be made between producers, Tennet, regional network managers and suppliers.

Step 2. In the second step, the possible measures are generated, e.g. during a brainstorming session. If the list of measures is too long, collective prioritisation can be used to limit the selection of possible measures.

Step 3. In this step, the phase of the security chain to which the measure applies and the party responsible for deployment of the measure are determined.

Different objectives

This model can also be used to achieve another objective, i.e. to chart an existing package of measures. When used for this purpose, a determination of who takes what action with regard to what measures is analysed on a cell-by-cell basis.

If the objective of using the model is to define a broad and balanced package of measures and to allocate responsibilities to different parties, it can be useful to define a suitable measure for each cell in the matrix.

	pro-action	prevention	preparation	repression	follow-up care
government			drills		
sector					
end-user				emergency power generator	

This model is also feasible in situations in which an already defined package of measures must be justified. Without proper justification, the package of measures is open to questions by the sector, such as: ‘‘Has a study into the effectiveness of the package of measures proposed by the government been done?’ ‘Why must we implement measures if the government and end-users are doing much less?’. Other questions can also arise: ‘Why are investments in repression being made when preventive measures have the potential to generate a far greater effect at lower costs?’ Via this instrument, the relationships between the responsibilities borne by government, sector and end-user and the relationships between the different links in the security chain can be made explicit. In that context, this instrument contributes to the argumentation used to justify the chosen measures.

Checklist of conditions

When performing this analysis, it is important that all perspectives are represented. The parties involved can tend to focus on measures that others must implement and ignore those for which they would be responsible. The parties involved can also tend to feel that the links in the security chain for which they are responsible are already properly arranged and that greater gains in security can be achieved by deploying measures in other links of the chain. For these reasons, the analysis must take into account the viewpoints of all of the actors involved (government, sector and end-user). More refined classification structures can also be used in the analysis. If, for example, the sector consists of multiple organisations that are all part of the industrial column, these organisations should all be allowed to contribute to the analysis.

When using the method, a clear distinction must be made between the generation of a global list of measures (via brainstorming-based techniques) and the prioritisation of the selected measures. If that distinction is not made, some measures may not be considered at all because the brainstorming session is disrupted by premature discussion of the effectiveness of the measures.

During creation of the global list, the parties involved can play an important role, as long as all perspectives are taken into account. During prioritisation, however, it is important that the situation is looked at with independent viewpoint, e.g. by content experts with no vested interest in the results.

29 Vulnerability analysis

Essence

The vulnerability analysis is based on a table that is used to chart the existing measures for the reduction of risks in a sector or part of the sector (sector layer). A distinction is made between five types of measures: financial-economic measures, legal measures, communication measures, technical measures and organisational measures. The vulnerability analysis is a simple method to show what parts of sector facilities are affected and of what the nature these facilities is.

Preparation, steps and follow-up

The model is particularly appropriate for generating estimates of the level to which facilities are affected as a basis for reduction of risks or the resulting consequences. Per layer (see also the layer model described above), an inventory is made of the existing risk reduction measures. For the electricity sector, for instance, existing policy for the layers production, transport, distribution and delivery is reviewed separately, which is why these layers are shown in the figure above

Checklist of conditions

The objective here is to create the most comprehensive picture of the existing measures possible. This eliminates development of preventive measures at a later stage that have already been deployed by the sector. In that context, enough facilities must be examined to ensure that all existing measures are actually uncovered.

Type of measure Layer in the industrial column	**Financial-economic**	**Legal (rules and regulations)**	**Communication**	**Technical**	**Organisational**
Production (of electricity)					
Transport (of electricity)					
Distribution (of electricity)					
Delivery (of electricity)					

30 Management of public confidence and awareness

Essence

In addition to quantification of real threats in terms of chance and effects, ‘public perception’ is an important concept that must be taken into account when developing and considering the relative merits of possible measures. The chance of an accident may be small in quantitative terms, but the public may still feel that there is a significant threat, and vice versa. When developing measures, it is therefore important to determine whether the measure reduces a real threat or a perceived threat, i.e. that the measure will reduce feelings of insecurity on the part of citizens. The effort to reduce perceived threats is also referred to as management of public confidence.

Preparation, steps and follow-up

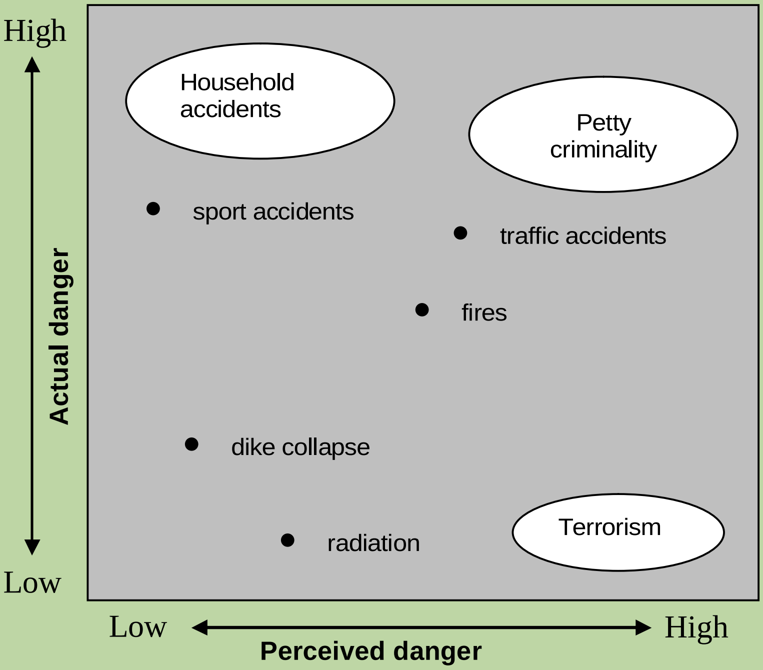
A chance-effect matrix can be used as preparation for this model. This matrix can be used to specify the level of real threat, as a basis for positioning possible events I the model. Using a starting event list, the set of relevant events or threats that require measures can be specified.

Step 1: The first step in use of this model is to determine the threats or possible events for which measures must be developed.

Step 2: The second step is to specify the real probability of the different threats or possible events based on the risk (chance-effect combination). To score the threat for ‘feeling of insecurity’, a group of possible victims must be studied. The study can be based on a questionnaire or telephone interviews. Based on the real and perceived threat scores, the threats and possible events can be positioned in the matrix.

Step 3: In this step, a set of measures is formulated to reduce the risks. The question here is whether the measure must be aimed at reduction of a real threat or a perceived threat. The figure shows that ‘terrorism’ has a very low level of real threat, but that the public sees the threat as very real. In efforts to increase security, public perception and feelings of insecurity therefore play a very important role.

Step 4: Finally, it is important to determine what the side effects of measures to increase public confidence are, e.g. reduced attentiveness. From that perspective, management of awareness can be beneficial, provided the focus is placed on generating awareness of the risks in a way that allows citizens to anticipate those risks.



Checklist of conditions

When using this model, endless discussion regarding the desirability of focusing on feelings of insecurity must be avoided. The fact that some feel that government should not be lead by feelings, but by real risks, is a given. It is also a given that others feel precisely the opposite.

In addition, deployment of the measures demands extraordinary meticulousness. The government can alleviate feelings of insecurity, but if citizens become victims due to a lack of awareness, strong feelings of powerlessness and distress can arise. Management of public confidence can also have certain negative results.

The results of this model are subject to feelings that arise as a result of risks recently publicised or given extra attention in the media. The results must therefore be seen in light of factors that can change very quickly, which means that the shelf life of this analysis is limited and that the analysis must be updated as events unfold.

Sources

Rosenthal, U. Staal, B. Storm, K.J, (2002) *Als je leven je lief is*, Max Geldens foundation for social renewal, p.7

Slovic (1992) Perception of Risk: Reflections on the psychometric paradigm, In: *Social theories of risk*, New York: Plenum, pp. 117-152

Slovic (1999) Trust, emotion, sex, politics, and science: surveying the risk-assessment battlefield, In: *Risk Assessment*, vol. 19, pp. 689-703

Vlek. Ch. (2001) Risicopsychologie: elk voordeel heeft zijn risico, In: *Hypothesis, Research and science quarterly*, volume 8, no. 31, pp.12-15, The Hague: NWO

31 Field of influence-analysis model

Essence

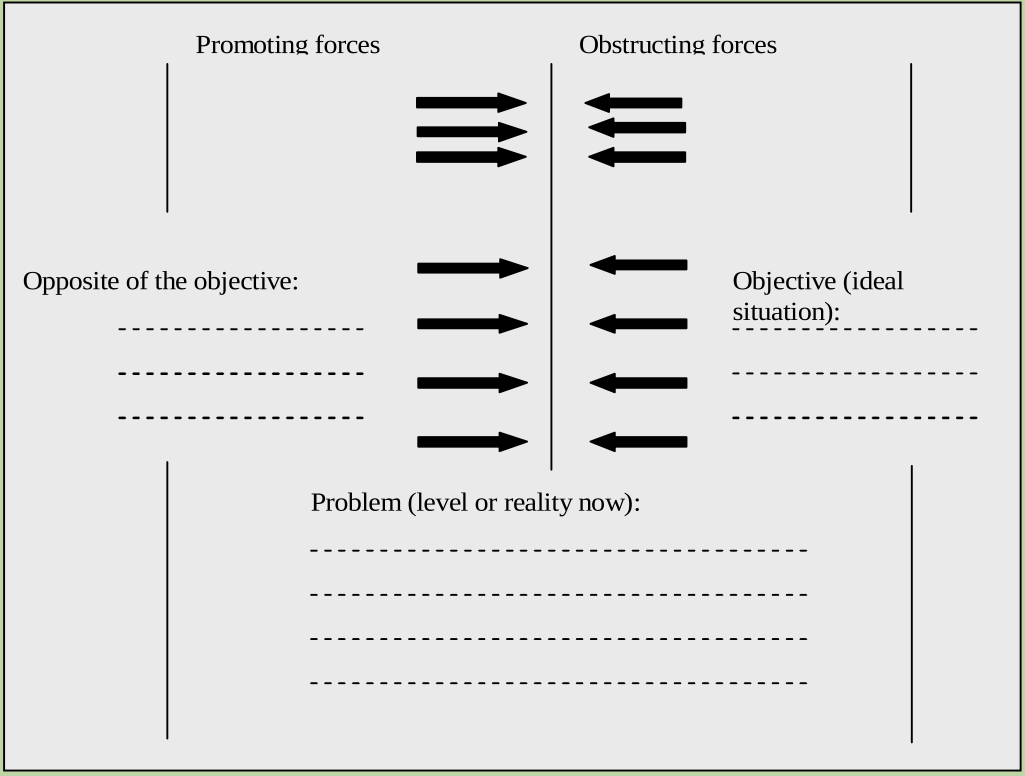
Actors exert their influence and power on the environment. Their powers may be limited or extensive (quantitative) or strong or weak (qualitative). Each power, or force, can hinder or stimulate realisation of policy objectives. The field of influence-model can be used to chart the forces that promote and obstruct realisation of the ideal situation (policy objective).

Preparation, steps and follow-up

The following approach can be used when applying this model:

1. Write a summary of the problem on the lines in the lower half of the form (see figure)
2. On the lines in the upper right-hand side of the form, describe the ideal situation: the best case scenario
3. On the lines in the upper left-hand side of the form, describe the precise opposite of the ideal situation: the worst case scenario
4. Under the heading 'Promoting forces', note the most important forces that promote realisation of the ideal situation
5. Under the heading 'Obstructing forces', note the most important forces that obstruct realisation of the ideal situation, thus promoting realisation of the worst case scenario
6. Prioritise the promoting and obstructing forces, e.g. by ranking them or assigning scores to them
7. In cases involving a group setting, discuss the individually completed forms with the other parties involved
8. Find solutions and measures that decrease the influence of the obstructing forces
9. Find solutions and measures that increase the influence of the promoting forces
10. Develop a concrete action plan to eliminate discrepancies between the real situation and the envisaged ideal situation.

The field of influence-analysis is quite similar in many respects to the PEST-SWOT model described earlier in this manual.


Promoting forces
Obstructing forces
Opposite of the objective:
Objective (ideal situation):
Problem (level or reality now):

Checklist of conditions

The results of the field of influence model are not static, but must change in response to changes in environmental factors. A promoting force, for instance, can change in a very brief time period into an obstructing power. This must be taken into account when interpreting the results. The usability of the model increases when the analysis is repeated periodically.

In the application of this model, *all* obstructing and promoting forces and developments in the environment must be included in the analysis, including developments that may seem highly improbable. Variety in the team of analysts is a basic prerequisite for this type of analysis. An expert meeting, with brainstorming activities, is a suitable work form for the use of this model.

Sources

Berg, R. van den (1984) *Voorlichting: Strategie tot verandering*, Boom: Amsterdam

Support curve

Essence

The support curve gives insight into the level of acceptance of a given measure on the part of a target group, e.g. parties in a sector, and the level to which that measure is implemented by the target group. In other words: the model gives insight, during the risk analysis phase, into the level of co-operation that can be expected from the parties involved with regard to a measure intended to alleviate a given risk..

Preparation, steps and follow-up

As preparation for the model, the security chain actor model can be used to define distinctions in the target group. Does the situation involve citizens, for instance, an entire industry or a subset of professional organisations (e.g. universities and hospitals)? This model is also related to the field of influence analysis model described above.

Step 1: In the first step, the different target groups are specified.

Step 2: In this step, measures are formulated that could contribute to reduction of a specific risk. For each measure, a line indicating the level of acceptance is then drawn. Depending on the characteristics of the measures, the line may deviate from the theoretical line at specific points.

The model makes a distinction between Innovators, Early Adaptors, Early majority, Late majority and Laggards. Innovators accept a measure very quickly, creating a snowball effect, and pass their eagerness to implement on to the Early Adaptors, who then pass the spirit on to the Early majority group, etc. The different acceptance levels are described below:

§ Innovators: this group is a fearless, intrepid group consisting of people who push the measure forward. The innovators are exploited in the communication to the early adaptors and the early majority group.

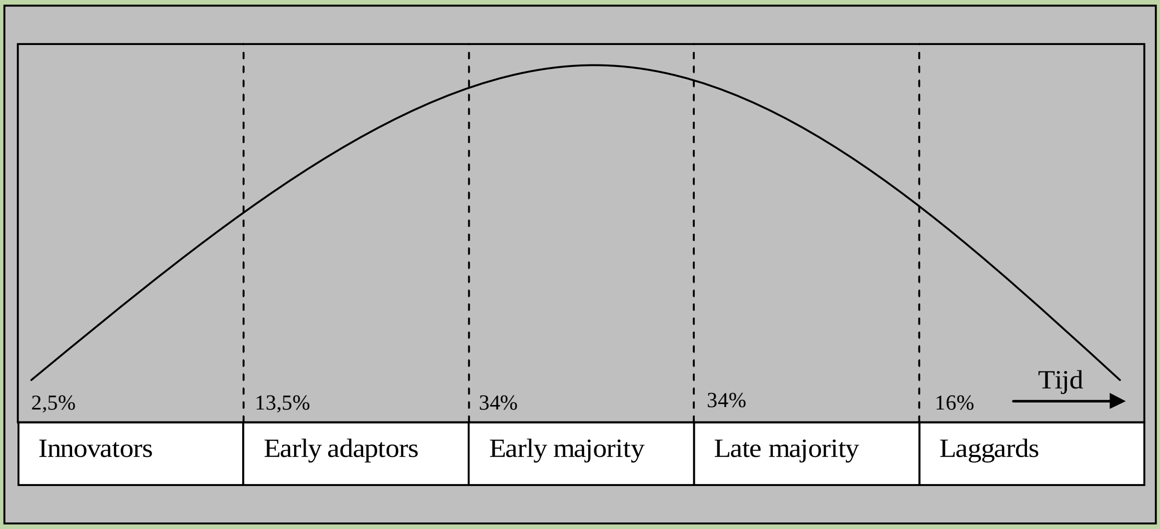
§ Early adaptors: this group consists of opinion-makers from different environments who are willing to try out new measures at an early stage, but they do demonstrate a certain cautiousness. This group communicates the benefits of the measure.

§ Early majority: this group is characterised by cautiousness. The members of the group are careful, unwilling to walk in the forefront of new developments, but quicker than average to adopt measures.

§ Late majority: this group consists of sceptics. The members of this group remain unconvinced of the benefits of measures until the majority have applied them.

§ Laggards: this group ascribes great importance to tradition and distrusts change. The members of this group do not accept change until the change itself has become a tradition.

Step 3: Once the support curves have been drawn for the different measures, the relative merits of the measures can be considered based on factors such as the objective of the measure and the period of time in which the measure must deliver results. If, for instance, the effect of a measure must be visible in a very short timeframe, measures that involve a group of Innovators and Early adaptors that is larger than the theoretical model suggests should be selected or measures for which a rapid transition from Innovators and Early adaptors to the Early majority group can be realised should be selected.



Checklist of conditions

The success or failure of implementation of a measure by a given sector largely depends on whether the innovators and early adaptors can be found to get the process of implementation moving. Only after these groups dedicate themselves to implementation will the later groups start considering implementation of the measures.

This model is particularly useful when considering measures with a high degree of uncertainty. These measures must result in positive examples to generate further support.

In specific processes, the model can generate advance (global) insight into the role and viewpoints of the different actors with regard to a specific measure. These actors should be informed and involved immediately to ensure that the required snowball effect starts promptly.

Sources

Rogers, E.M. (193) *Diffusions of Innovations* , New York: Free Press

33 Actor quadrants

Essence

Often, multiple actors are involved in realisation of a measure. By placing the parties involved in this matrix, the viewpoints of the actors and what issues the different actors consider important become visible at a single glance. Different approaches can also be used to define the four quadrants.

There is a clear relationship between this model and the support curve model described earlier in this manual. This model is based on the relative importance of the different actors and on their respective levels of sympathy for a given measure. This model takes these factors into account and links them to the importance ascribed by the actors to the subject.

Preparation, steps and follow-up

As preparation for application of this model, the problem or measure confronting the actors must be formulated. Once this has been done, the following steps must be completed:

Step 1: Inventory of the actors involved. At this point, the importance of the actor (in terms of power) does not yet play a role. The interested party whose perspective is under evaluation is placed in the upper right-hand quadrant of the model. In this figure, this party, the problem owner, is the Ministry of Economic Affairs.

Step 2: In the second step, the importance of the different actors is shown in the matrix. The larger the circle in which the actor is placed, the more influence held by the actor.

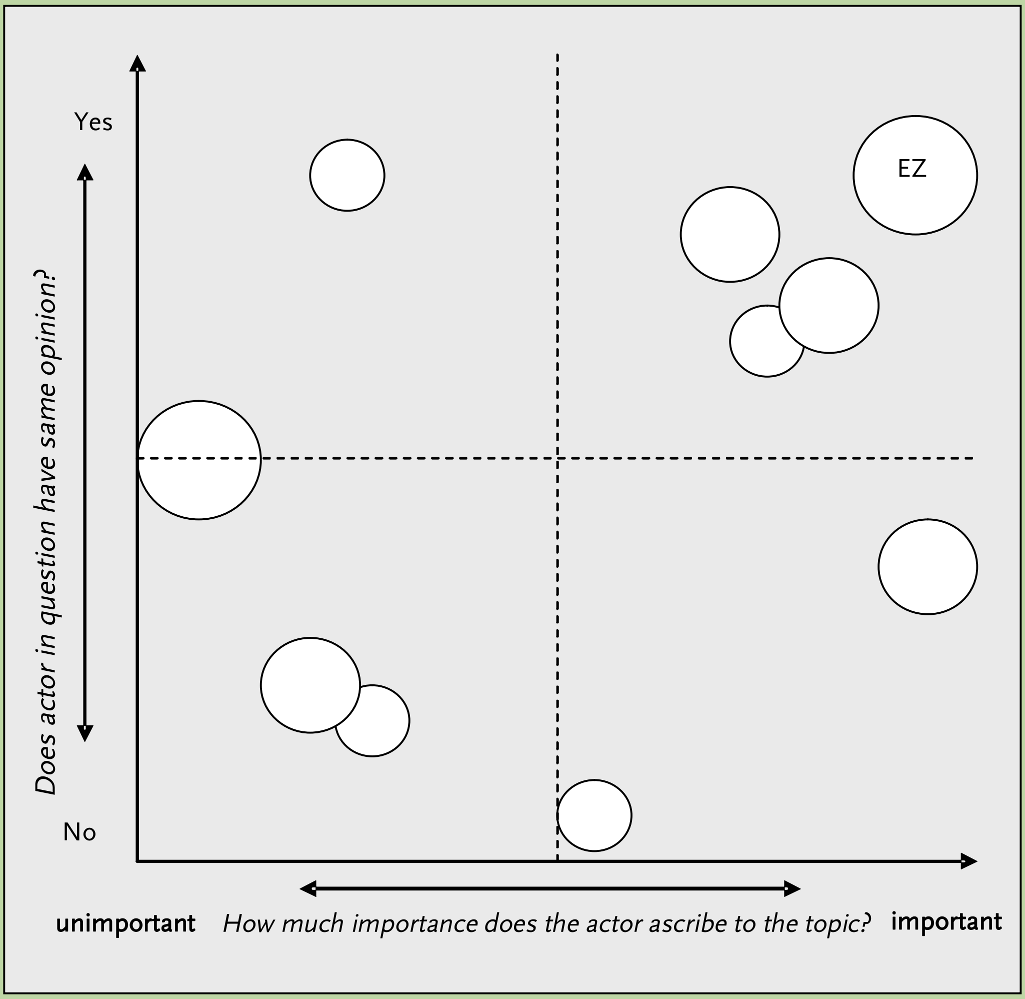
Step 3: Based on media analyses, brainstorming or interviews, the actors are positioned in the matrix. The *Resistance ladder* is a helpful tool at this point. The vertical axis shows the level of agreement between the actors and the problem owner (Economic Affairs in this case). The horizontal axis shows the level of importance ascribed to the subject or the measure involved by the different actors.

Step 4: Once they have been positioned in the matrix, strategies can be developed for approaching the actors. The parties in the lower left-hand corner of the matrix, for instance, may be allies. Although they do not agree with Economic Affairs, the matrix reveals that they find the subject relatively unimportant, which means that there may be opportunities for discussion and compromises with these parties. A suitable strategy for approaching the different parties can be developed for the other quadrants in a similar manner. In the upper right-hand quadrant, for instance, an open approach can be employed. The lower right-hand quadrant, on the other hand, contains actors who ascribe relatively great importance to the subject, but viewpoints that oppose that of the problem owner. A strategy in which the problem owner emphasises the positive aspects of the intended measures and negotiates compensation for the negative aspects with the actors would be appropriate for this quadrant.

Checklist of conditions

The positioning of parties in the figure can very time-dependent, which means that the analysis must be performed periodically and that the results must be interpreted as a snapshot in time with an extremely limited shelf life.

Because explicit definitions of the level of broad-based support for a given measure can have a counterproductive effect, this model is primarily intended for internal use.


Yes
EZ
Does actor in question have same opinion?
No
unimportant
How much importance does the actor ascribe to the topic?
important

34 Barrier model / Resistance-ladder

Essence

The barrier model or resistance ladder describes the resistance that may occur in conjunction with formulation and implementation of a measure. The model can be used for various types of barriers, including political-managerial barriers, technological barriers, economic barriers and legal barriers..

Preparation, steps and follow-up

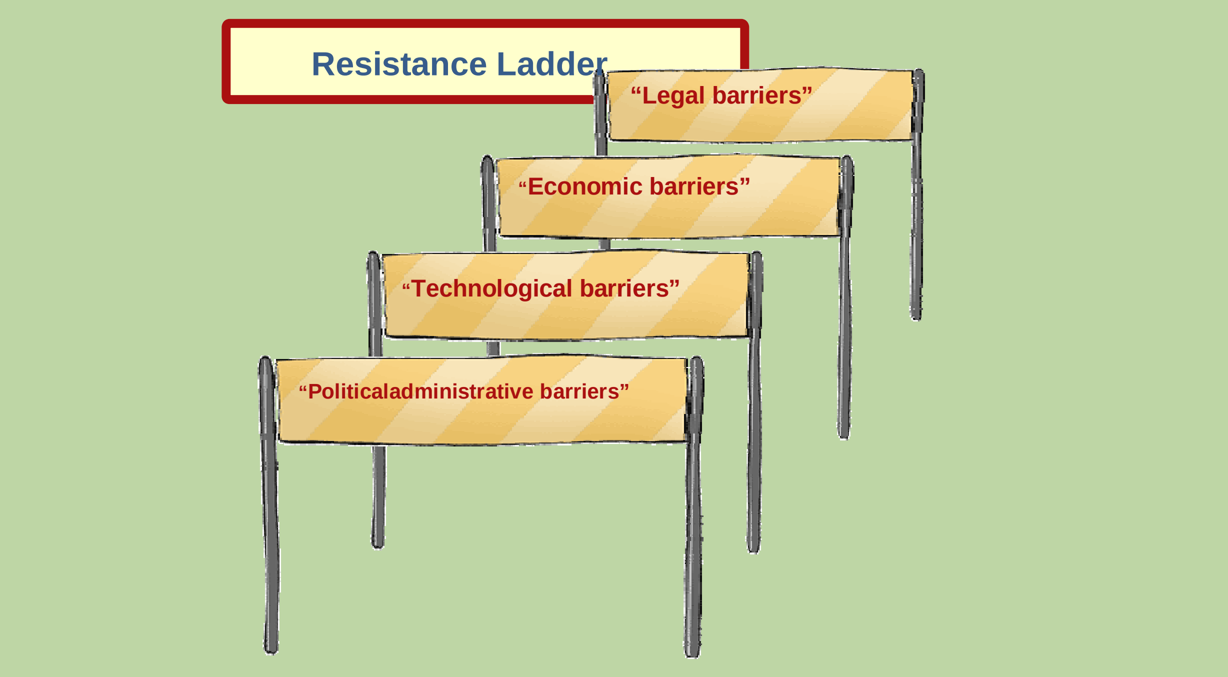
As preparation for the application of this model, the measure or measures for which barriers must be charted must be specified.

Once the measures are specified, the following steps must be completed:

Step 1. What are the barriers for implementation of the measure involved? A political-managerial barrier may be involved in cases in which a proposed measure conflicts with earlier policy or regulations, for example, while a technological barrier may be involved in cases in which a proposed measure cannot be implemented because of technological limitations. By the same token, an economic barrier can be caused by a lack of funding for a proposed measure, while a legal barrier could be thrown up by a conflict between a proposed measure and (European) legislation. Of course, the model can also be used to explore other barrier categories. When using the model, the question of whether the barrier is a real barrier (current regulations or conditions that make implementation of a measure impossible) or the barrier is a barrier that has been thrown up by the actors and can be breached with relative ease during negotiations with the parties involved must be taken into account.

Step 2. In the second step, the actions that are required to allow implementation of the measure despite the barriers are defined. This involves formulating actions that remove the barriers or formulating supplemental measures that counteract the negative effects of the barriers. In cases involving seemingly insurmountable barriers, other measures may be preferable.

There is a clear relationship between this and other models. The support curve model can be used as input for this model, for instance, as can the actor quadrants model.



Checklist of conditions

This model is particularly helpful for internal use in governmental agencies as an environment charting tool. It helps to anticipate possible barriers.

The real value of this model is only revealed when, subsequent to identification of possible barriers, the possible solutions for counteracting or eliminating the possible barriers are defined. This is an issue that requires special attention when using this model.

Sources

Mil, B.P.A. van (2006) Zes lessen voor het opsplitsen van energiebedrijven

Raad voor Verkeer en Waterstaat, Tussen droom en daad, 2003 (zie www.raadvenw.nl). Dit is een voorstudie uitgevoerd door Berenschot in opdracht van de Raad voor Verkeer en Waterstaat, ten behoeve van het advies ‘Hoezo marktwerking’ dat in 2004 verscheen

35 Cost of risk reduction

Essence

This model is charts the costs for all of the charted measures and associated the yields in terms of risk reductions (or the yield in terms of security). With this model, a choice can be made between efficient and less efficient measures in a relatively short period of time.

Preparation, steps and follow-up

As preparation for this model, the set of relevant measures must first be specified. A chance-effect matrix can then be applied to determine the effectiveness of each measure. In this context, the initial risk of a threat is reduced by the risk remaining after implementation of a given measure. Finally, this model is used to chart the relative efficiency of the different measures.

Step 1. In the first step, the measures are scored on the 'risk reduction' axis. Then, the costs of the different measures are estimated. Costs and risk reduction are used in the matrix as the positioning coordinates for the measures.

The example shows that measure 10 costs a great deal of money, while resulting in a minimal yield in terms of risk reduction. Conversely, the yield for measure 1 is extremely high, while the costs are relatively low.

Step 2. In this step, the measures are prioritised based on a number of factors. If, for example, the objective is to reduce the risk by a given quotient, at whatever cost (under political pressure), the level of risk reduction will be a more important criterion than the costs of the measure. Measure 6 would be preferred over measure 4 in this case, despite the fact that measure 4 is relatively inexpensive.

Step 3. In another version of the cost of risk reduction model, the 'costs of the measure' axis is replaced by an 'duration of the implementation' axis. This use of the model makes it possible to make well considered choices regarding measures that can be quickly implemented, but only result in a marginal reduction in risk, and measures that take a long time to implement, but result in a more significant reduction in risk.

Checklist of conditions

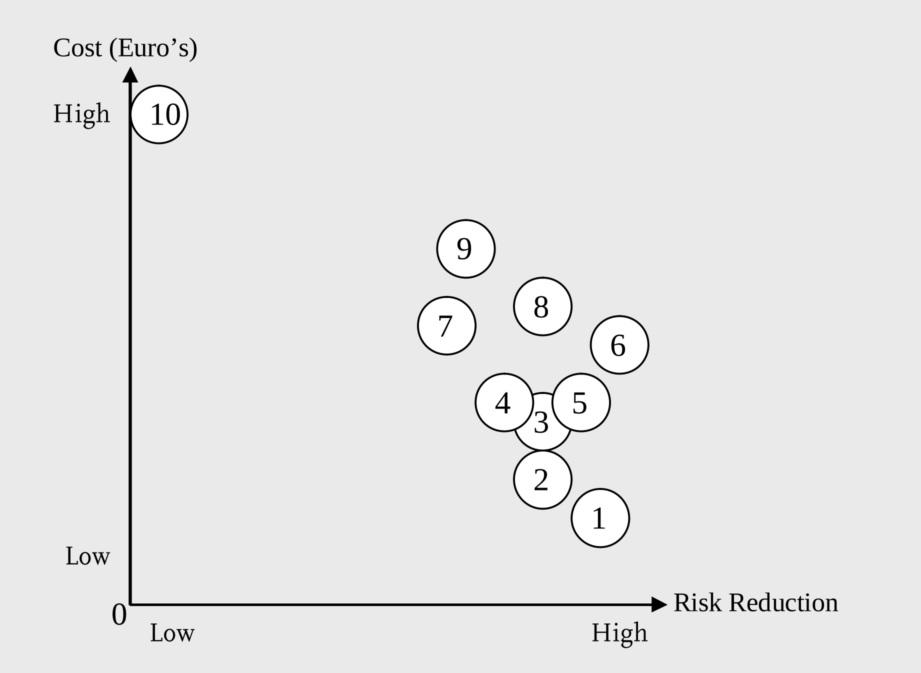
The model does not require meticulous evaluation of the individual measures during the quick scan phase, but is intended for use as a scoring tool that can be used to determine the relative efficiency of different measures.

The model does require some knowledge of the costs that are associated with implementation of the different measures. Greater knowledge levels are also required in cases involving an in-depth analysis, which can be performed subsequent to the quick scan.

When using this model, it is important to have a clear picture of the different types of costs involved. For example: Do the costs relate to policy staff who are working on development of the measures or are the costs to be paid by the parties to whom the measure applies? Or are the costs under consideration total costs? To what extent are the costs incidental, one-time costs and to what extent are the costs recurring costs that will be incurred for a long period of time? And finally, who reaps the benefits and who pays the costs?

Sources

Henley E. en H. Kamamoto (1981) *Reliability engineering and risk assessment*, Englewood Cliffs: New York. (p. 39)


Cost (Euro's)
High
10
9
8
7
6
4
5
3
2
1
Low
0
Low
High
Risk Reduction

36 Multi-Criteria Analysis (MCA) for measurement prioritisation

Essence

To support implementation of the appropriate measures for a given situation, the ability to compare potential measures (to alleviate the same threat) based on a restricted number of criteria can be useful. This model offers support for scoring measures based on multiple criteria and gives a visual depiction of the considerations that apply to each of the different measures.

Preparation, steps and follow-up

In preparation, global list of possible measures must be formulated. The measures that appear most promising can be short listed at this point if desired.

Step 1. The first step is to define the criteria that are deemed important. In the example, five criteria have been selected: low costs, fast implementation, government enforceability and broad-based support in the sector.

These criteria are all positively formulated, i.e. a high score is a good score. This is why 'low costs' was selected as a criterion rather than just 'costs'. A measure scores well if it achieves high scores for all criteria. In this case, the measures that achieve high scores are cheap measures that deliver higher security yields, that can be implemented quickly, that can be enforced by government – if necessary and desirable- and that enjoy broad-based sector support.

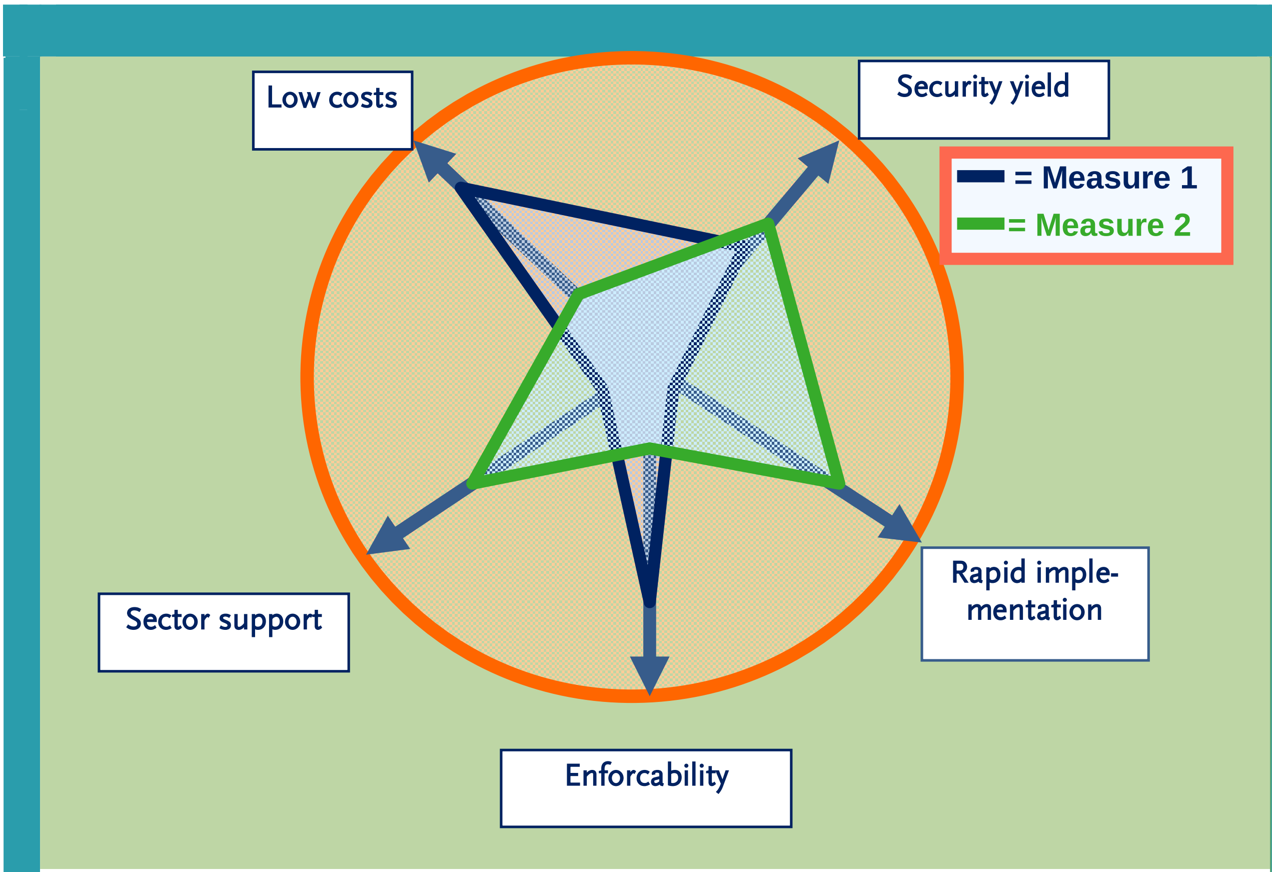
Step 2. In the second step, a 'spider web' is constructed per measure, by scoring the individual measures based on the five criteria and then linking the points. The example shows that measure 1 costs less than measure 2, but that measure 2 can be more quickly implemented and also enjoys greater broad-based sector support.

The 'spider webs' for each of the measures can be constructed in different ways, in a group session if desired. Individuals or subgroups can construct their own webs on a transparency and, once completed, the webs can be overlaid and then projected on an overhead projector. This approach quickly uncovers differences of opinion between the parties involved. An electronic boardroom approach can also be used to quickly process the scores assigned to the measures by individuals in the group and to generate interesting secondary data, including averages and standard deviations. These data can also be used as input for discussion. This step ends with achievement of a good level of consensus regarding the scores per criteria.

Checklist of conditions

Simplicity is important. Simultaneous analysis of large numbers of criteria and measures is seductive, but does not necessarily result in results that can be interpreted effectively or easily. The recommended approach is to restrict analysis to a limited number of measures and criteria per analysis.

Computer support can contribute to the usefulness of this model because it facilitates aggregation of the scores assigned by a group of individuals and uncovers differences of opinion quickly based on calculation of standard deviations.


Low costs
Security yield
= Measure 1
= Measure 2
Rapid imple-mentation
Sector support
Enforcability

37 (Societal) Costs-Benefits Analysis (SCBA)

Essence

The costs-benefits analysis makes the costs and benefits per measure understandable as well as distribution of the costs and benefits over individual actors. This analysis offers quick insight into what measure offers the best costs-benefits ratio, what party incurs the costs and what party reaps the benefits. Discrepancies uncovered when using this model between where the costs are incurred and where the benefits are generated indicate market failures in the implementation of measures.

Preparation steps and follow-up

Different perspectives can be used for the Costs-Benefits Analysis. In this manual, four logically linked perspectives were selected.

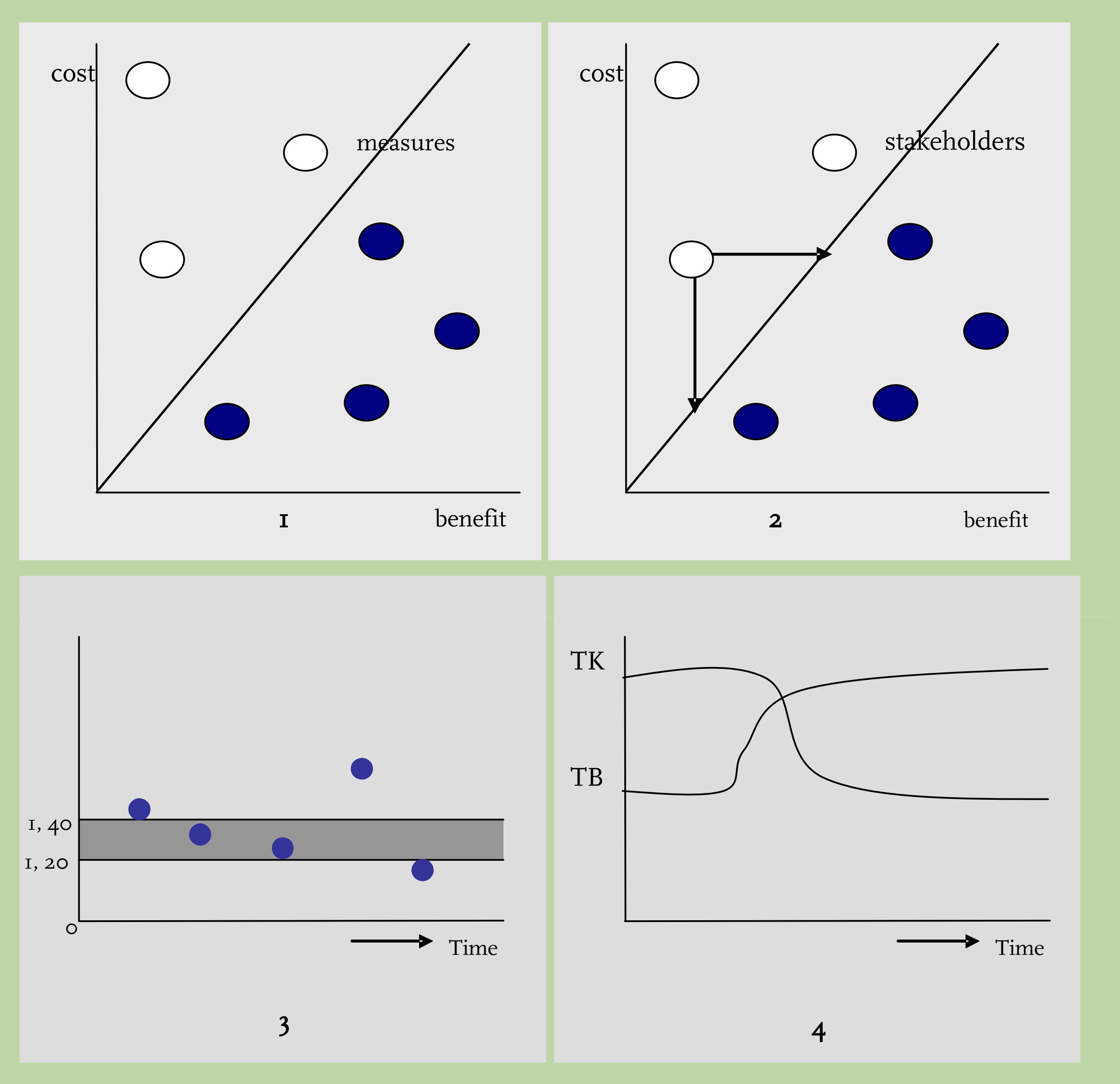
Before we go on to describe the four perspectives, we must note that it is important to realise that coverage of excessive damage is impossible to guarantee. An extreme example of excessive damage is a meteor striking the earth. The chance of that happening is extremely small, but the damage would be enormous. This is damage that simply cannot be covered. When preparing to use this model, threats must therefore be evaluated to determine whether they can actually be prevented and, if not, whether some type of insurance can be closed to mitigate the catastrophic effect they may have.

If the estimated damage can be covered, a simple Costs-Benefits Analysis can be drawn up, similar to the example in variant 1 in the figure above. In principle, if the benefits of a measure are greater than or equal to the associated costs, the measure is efficient. The analysis can also be based on total costs and benefits or on marginal costs and benefits. In principle, the outcome is specified by selecting the basis for comparison. In variant 1, this means that the measures in blue may be more interesting measures to apply.

Variant 2 in the figure above is another visualisation of the Cost-Benefits Analysis. In this variant, the costs and benefits of a given measure for the individual actors are specified. The circles in the graph represent the different actors who will bear the costs or receive the benefits of a specific measure. If the costs related to a specific measure are higher than the benefits for an individual organisation, that organisation (or actor) will not want to participate in implementation of the measure. From a business economics standpoint, participation would be illogical and irresponsible. In this approach to the model, the impact of implementation on the different actors can be seen per measure, i.e. it is immediately clear which actors have an interest in implementation and which do not, at least in terms of the distribution of costs and benefits. If a specific actor bears responsibility for implementing a measure, but an SCBA reveals that the actor in question will bear the costs, but not reap benefits, there is a failure on the part of the market and the government must step in to ensure that the costs and benefits are properly distributed or to compensate the actor involved.

The issue of how to approach actors who are required for implementation, but who will bear costs greater than the benefits they receive must be tackled at this point. One possible solution is to compensate these actors so that the costs fall below the benefits. Another option is to ensure that the actors in question reap greater benefits.

Once these issues are tackled, the question of what action must be taken with regard to which individual organisations before implementation can be started arises. How can the costs of important measures that fall into the lap of an organisation that stands nothing to gain by implementation be better divided over the organisations in the field of influence? Is compensation of organisations that pay the costs, but that do not profit from the benefits necessary? Can organisations that do not profit from the benefits (because the costs exceed the benefits) be pulled into contributing to implementation with companies that do enjoy the benefits? Etc.



Once the measures that appear interesting in the primary instance have been specified, future financing can be considered. Using Return On Investment (ROI) and Accounting Rate of Return (ARR) modelling, the option that is most profitable over a specific period of time can be determined. In the business economics world, ROI is used to express profit (after taxes) as a percentage of the (average) invested capital. ROI is based on the assumption that a specific measure generates a yield. If the objective is an ROI over a ten-year period of 10%, the measure has to not only pay for itself in ten years, but also generate 10% of the invested amount as profit.

Variant 3 shows this ROI concept, with the ROI value of the measure specified as a yield of between 20% and 40%. The measure on the right has an ROI of less than 20%, which makes it a less interesting investment than the other measures, all of which have an ROI of more than 20%. If, for instance, the ROI percentage is less than 10%, it becomes more interesting to set the investment amount off against a specific interest. There is a possibility that the costs incurred to pay damages after a disaster are lower than the yield on the investment that the party with that specific interest could earn by placing the money in a savings account at a bank.

The last variant is more dynamic in nature. After all, not all costs and benefits occur simultaneously or are completely incurred or reaped at moment X. Usually, the cost must be incurred before any benefit is seen. This means that costs and benefits for a specific period can only be matched at a later date. Variant 4 creates insight into this situation by positioning the costs and benefits in time. The points at which the lines representing the costs and benefits cross are points at which the costs equal the benefits. Based on this information, which is correlated with the business economic payback time of an investment, decisions can also be made regarding whether or not investments should be made in a measure.

Even though the different variants described above are closely related, they each have specific features that make deliberations regarding the question of whether to invest or not to invest possible from different perspectives. However, because of these different perspectives, it can be extremely useful to use the different variants simultaneously, partly because the results are complementary.

Checklist of conditions

An extensive analysis of the position of actors, the benefits of measures and the total costs-benefits overview can be a time-consuming activity, one that requires a great deal of expertise. Properly defining the scope of the objectives to be achieved when using the model is extremely important, to avoid being caught up in endless calculations and discussions.

The initial quick scan should be performed by a risk analyst, but to obtain optimal insight into the costs and benefits, it is important to involve the organisations under evaluation in the analysis, to ask them the appropriate questions, to find out what alternatives, compromises and compensation they have in mind.

Commonly used work forms for execution of a CBA are expert meetings, interviews and work conferences. During work conferences, discussions between experts such as business economists, risk analysts and damage experts can contribute valuable information and insights.

The models succeed or fail based on the estimates that are made during modelling. Costs can be expressed in terms of investment with relative ease, although the appropriate choice of methodology does have to be selected. But expressing societal effects such as fatalities in monetary terms is considerably more difficult.

Finally, in some cases, specific information regarding the positioning of actors in the matrix is of significant strategic value. Sensitive strategic and business economic information must be handled at all times with the greatest of care.

Sources

Heezen, A. (1999) *Basisstudie Bedrijfseconomie*, Houten: Stenfort Kroese

Horngren, C.T. e.a (2002) *Management and Cost Accounting*, London: Prentice Hall

Measure-effect model

Essence

The measure-effect model gives insight into the relation between different possible measures, the effects that must be reduced and the secondary effects that arise due to implementation of the measures. The purpose of this model is to chart the positive effects of a specific measure, but also to gain insight into unintended side effects that occur as a result of the measure.

Preparation, steps and follow-up

As preparation for this model, the measures that must be subjected to measure-effect analysis must be selected. The model is then applied as follows:

Step 1: Inventory all effects that can occur as a result of manifestation of the risk. The effects are depicted in ovals in the matrix and the selected measures are placed in rectangles.

Step 2: Per measure, indicate whether the measure makes a positive contribution to (reduction of) the effects.

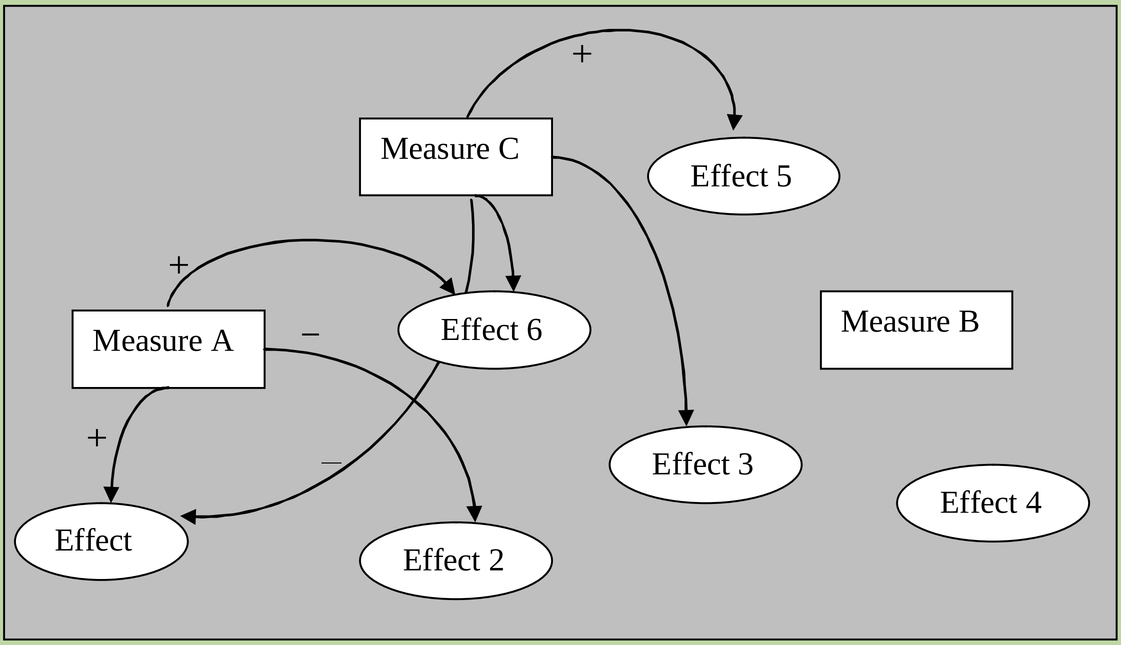
Step 3: Inventory side effects that occur as a result of implementation of the measure. Then determine whether each measure makes a positive or negative contribution to these effects.

Step 4: Use arrows to link the different measures and effects, with a + or – to indicate whether the link represents a positive or negative contribution.

An example is the risk of privacy infringements by hackers in cases involving digital employee data. Privacy protection measures can include security measures for the computers involved, such as log-in codes and security screens. These measures make a positive contribution to the effect 'privacy infringement'. On the other hand, however, if data stored on another user's computer must be accessed quickly in an emergency, these same measures can cause unnecessary delay. This delay is an unintended side effect of the measure.

Step 5: Summarise the effects per measure in a table similar to the one below:

Effects	Desired	Undesirable
Intended	§ Effect Y § …	§ Effect Z § …
Unintended	§ Effect X § …	§ Effect W § …



Checklist of conditions

The power of this model is that it can be used to systematically identify unintended effects, e.g. the unintended delay in an emergency described above. Where possible unintended effects are uncovered, the model gives clear insight into whether a security measure ultimately delivers yields by providing information on negative side effects that could effectively cancel out the original positive effect of that measure.

Sources

Jensen (1996) *An Introduction to Bayesian Networks*, Springer Verlag

39 Table of Eleven

Essence

The human factor plays an important role in the analysis of risks. A risk becomes more serious as the level of compliance with rules and regulations decreases. The Table of Eleven is a model that is used to determine the level of compliance with rules and regulations. The model is a list of factors that play an important role in compliance. The model makes it possible to uncover the strengths and weaknesses in maintaining compliance. The model is constructed from eleven dimensions. Not does this model offer the ability to review enforcement efforts for effectiveness, it can also be used as a checklist when developing policy and legislation.

Preparation, steps and follow-up

As preparation for use of the Table of Eleven, the objective of the analysis must be specified. Is the objective to predict the effectiveness of potential measures, for instance, or is the objective to investigate inefficiencies in the current package of measures?

The model can be used by policy makers, civil law experts and consultants and can be applied to the preparatory phase, execution phase and evaluation phase of legislation. The analysis consists of eleven dimensions, divided into three groups: spontaneous compliance, control dimensions and sanction dimensions. These groups are based on the type of contributions the elements in the groups make to the compliance dimension: voluntary compliance on the one hand and more forced compliance on the other. The development of the different dimensions during formulation of new regulations gives an indication of the compliance level applicable to the regulations.

The dimensions for spontaneous compliance:

- Knowledge of regulations

This dimension relates to the recognition and clarity of law as viewed by the target group. Unfamiliarity with the regulations can result in (unconscious) violations. Vagueness or complexity in the legislation can cause (inadvertent) errors in compliance. A number of aspects can be distinguished, for example scope of the regulations, vagueness of the regulations and complexity of the regulations.

- Costs and benefits

This dimension relates to the (im)material advantages and disadvantages that result from compliance or violation, expressed in time, money and effort. The dimension covers all financial-economic and immaterial costs and benefits of compliance and non-compliance, expressed in time, money and effort. Four categories can be distinguished:

  - costs of compliance
  - costs of violation (violation barrier)
  - benefits of compliance
  - benefits of violation

- Acceptance

Acceptance involves the (perceived) reasonableness of the policy proposed by government and the resulting norms. Acceptance can relate to the opinion of the target group regarding a regulation in general terms, but it can also relate to the opinion of the target group regarding the consequences of that regulation on their personal lives. The manner in which policy is executed can also play a role. In some cases, government and citizens are separated by an interim layer (professional group/executive agency) that plays an essential role in policy design and, hence, in acceptance of the regulation. The level to which the target group feels responsible for realisation of the policy is also an indication of the target group's acceptance of the policy.

- Adherence to norms

This is the level of willingness on the part of the target group to bow to the authority of government. Some people do what government or law mandates as a matter of course. This sub-dimension relates to the general level of respect for government in the target group. This respect for authority is sometimes also related the authority of the executive or enforcement agencies. In general, this dimension has a more basic and continuous character than the 'acceptance of policy' dimension. The dimension relates to the more or less constant attitude towards government of the target group.

- Informal control or non-government control (self-regulation)

The chance of positive or negative sanctions being imposed as a result of their behaviour by parties other than government, as estimated by the target group. Non-government control can consist of informal control of adherence to the imposed norms or a formal form of control exerted by the target group or professional association over its own members. In the latter case, this form of control is referred to as horizontal supervision. Social control is exerted by the inside and outside of the target group's environment: by family, friends, colleagues, internal or external accountants, local companies and competitors. The following aspects play a role in this respect:

  - the perceived chance of a violation being noticed;
  - the level of disapproval or approval of the violation voiced by the environment;
  - the level of responsibility for the violation felt by the environment and the resulting action taken by the environment (social sanction).

Horizontal supervision is a form of formal social control: non-government control focussed improving the quality of products and services within specific professional groups or sectors, e.g. professional codes of conduct, certification systems and seals of approval.

<u>The dimensions for control:</u>

- Informal notice

The chance, as estimated by the target group, of a violation that has been noticed by a party other than government being reported to a public body. This dimension relates to the perceived chance of a violation being discovered without government control, e.g. via a tip hotline, coincidental detection or submission of a complaint.

- Chance of being checked

The chance, as estimated by the target group, of being checked for violations by the government. The chance of being checked is a specific quantity, based on the frequency of checks, e.g. the number of checks per 100 target group members per year. The objective chance of being checked deviates from the subjective chance of being checked for various reasons, including awareness of control policy and the visibility of the checks. The subjective chance of being checked plays a decisive role in compliance. Distinctions can also be made between different types of checks (e.g. administrative and physical).

- Detection chance

The chance, as estimated by the target group, of being caught in a violation when checked by the government. Being checked does not necessarily mean the same thing as being caught. This dimension relates to the effectiveness of the different checks, i.e. whether they result in actual detection. This is dependent on the type of violation and the thoroughness of the checks. In some cases, the violation is easy to detect, but the violator is difficult to find. The objective detection chance is based on the relationship between the number of observed violations and the number of actual violations (usually unknown).

- Selectivity

The (increased) perceived chance of being checked and caught in a violation based on pre-selection of companies, individuals, activities and areas for checking. This dimension relates to the ability of the parties doing the checking to check those who do not comply more often than those who do. In principle, the quality or effectiveness of this form of selective control (possible based on risk analysis and crime analysis) can be quantified based on the relationship between the number of violators caught during selective checks and the number caught during random checks. Selection increases the chance of violators being caught.

<u>The dimensions for sanction:</u>

- Sanction chance

The chance, as estimated by the target group, of being sanctioned for a violation detected during a check. The sanction can be imposed by a criminal justice agency, the police or a judge, for instance, but also by a board of directors.

- Sanction severity

The sanction severity is the combination of the sanction amount and sanction type applicable to the violation, plus the additional disadvantages resulting from the sanction. The sanction severity relates to the duration of a prison sentence, the amount of a fine, the effort that must be expended to reverse sentence, the amount of a fine or the effort required to recover from the damage caused by a sanction. Costs for legal assistance can also play a role. The process of being sanctioned can also result in additional, immaterial disadvantages such as loss of status and reputation as a result of run-ins with the justice system. The severity of the different types of punishments does not have the same impact on all perpetrators however.

Checklist of conditions

This model is particularly useful when dealing with enforcement issues, e.g. in ex-ante evaluations of measures for maintaining law and order and enforcing compliance.

Sources

‘De ‘Tafel van elf’, Beknopte toets voor de handhaafbaarheid van regels’, Ministry of Justice Law Enforcement Expertise Centre, The Hague, November 2004

''Naleving en handhaving van regelgeving'', R.M.M. Vossen and M. Prinsen, Justitiele Verkenningen, annual 29, no. 9 2003 '

De Tafel van Elf, P. van Reenen (editor), Sdu Publishers, The Hague 2000 'The Table of Eleven, a versatile tool', Law Enforcement Expertise Centre, November 2004.

‘Nieuwe instrumenten voor de rationalisering en optimalisering van beleid en wetgeving: vergelijking van ketenbenadering en Tafel van Elf’, P. van Reenen, D. Ruimschotel, H.M. Klaasen, in: Beleidsanalyse, 1996-4

‘De Tafel van Elf, een conceptueel kader en een instrument bij rechtshandhavingsvraagstukken’, D. Ruimschotel, P. van Reenen, H.M. Klaasen, in: Beleidsanalyse, 1996, no. 3, p. 4 et. al.

40 Realisation test (Government implementation influence)

Essence

De The realisation test can be used to plot the influence that a ministry such as the Ministry of Economic Affairs can exert in the implementation of a measure.

Three factors can obstruct or facilitate implementation of measures desired by the Ministry of Economic Affairs: the ministry's own organisation, other organisations and autonomous developments.

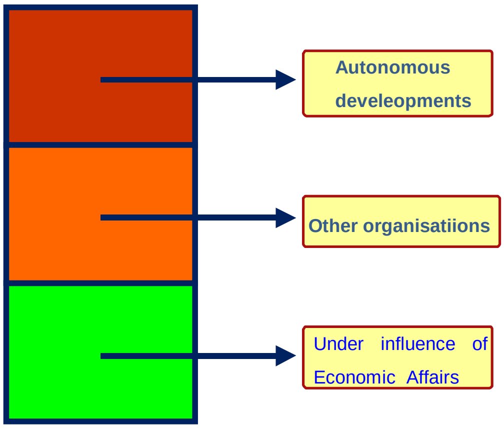
In other words, the Ministry of Economic Affairs can exert a certain amount of influence in the implementation of measures (e.g. by handling the implementation itself), but is also dependent on other organisations (which can of course also be influenced, but which are not under the full control of the ministry) as well as on autonomous developments over which it has no influence at all. Measures for the prevention of an attack on a nuclear reactor are a good example in this context. The Ministry of Economic Affairs can exert its influence to increase security by imposing requirements in the area of physical safety and security. However, the ministry is also dependent on the contributions made by other parties in this area. The Department of Housing, Regional Development and the Environment (VROM) plays an important role, but so does the organisation that runs the nuclear reactor. In addition, autonomous developments play a role, e.g. the increased threat of terrorism.

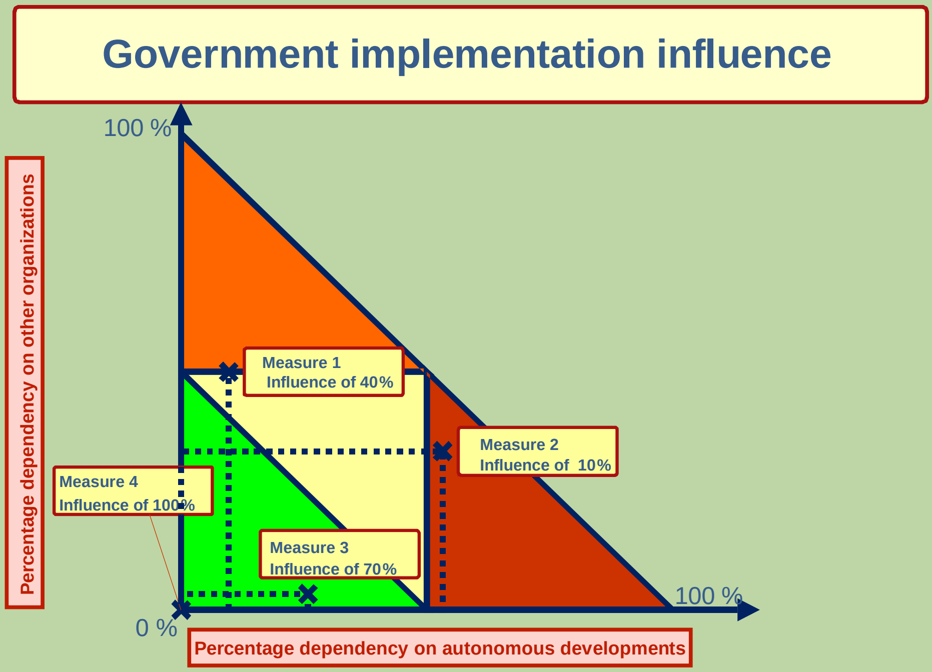
During selection of measures, aspects such as these must be taken into account. Should the ministry follow an independent strategy because it is able to realise implementation alone or should a co-operative strategy be followed, a strategy that involves investment and collaboration with other organisations?

Preparation, steps and follow-up

The most promising measures for inclusion in the analysis can be selected in preparation for this analysis. Once that is done, the following steps must be performed:

Step 1. For each measure or package of measures, the relative influence that can be exerted by the Ministry of Economic Affairs is expressed as a percentage and the relative influence that can be exerted by other organisations is expressed as a percentage. The extent to which the situation cannot be influenced by the ministry or by other organisations, but is determined by autonomous developments, is also expressed as a percentage. This gives an indication of the ability of the Ministry of Economic Affairs to influence implementation. The relative influence can be visualised in a bar chart:


Autonomous deveoelopments
Other organisatiions
Under influence of Economic Affairs



Step 2. In this step, dependency on other organisations and dependency on autonomous developments, both expressed as percentages, are placed on the axes of a graph. The selected measures – for which the percentages of ministerial influence, outside organisation influence and autonomous development influence were determined in step 1 – can now be positioned in the model, which results in the following figure:

In the case of measure 1, for example, 40% of the influence is exerted by Economic Affairs, 50% by other organisations (score on the vertical axis) and 10% by autonomous developments (score on the horizontal axis).

Step 3. Based on this model, the measures can be classified based on the level of influence that the Ministry of Economic Affairs can exert over their implementation. The different colours used in the figure have the following significance:

- Green: implementation of the measure is primarily influenced by Economic Affairs (influence greater than 50%);
- Orange: implementation of the measure is primarily influenced by others (influence greater than 50%);
- Red: implementation of the measure is primarily influenced by autonomous developments (influence greater than 50%);
- Yellow: this category contains the measures that are collectively dependent on the other three categories.

Based on the analysis results, the ministry can adjust its implementation strategy, e.g. it can opt to focus on measures that are implemented by other organisations in the framework of self-regulation (measures in the orange triangle) or it can focus on measures that it can implement independently (measures in the green area), based on the idea that the ministry has the power to implement and is not reliant on the willingness of other parties. In other words, the ministry has the influence to implement or the power to realise the measure.

A logical follow-up for this model is an actor analysis such as the actors quadrant model, particularly in cases involving measures that other organisations have greater implementation influence over. In the actor analysis, for instance, the extent to which the different actors support implementation can be analysed.

Checklist of conditions

This analysis is particularly useful when defining departmental implementation strategy. When using this model, participation on the part of the officials from the department involved is important.

There is a danger of this analysis being performed as an objective in itself. When this danger is avoided, this analysis is an effective tool for the development of implementation plans and strategies.

41 Deming Circle: implementation monitor

Essence

The Deming Circle (Plan-Do-Check-Act) is used in evaluation systems. In the risk analysis phase, it can be used to monitor implementation of a measure and the effects of the measure. The model is primarily meant for internal use in an iterative process that is based on a constantly recurring cycle of experiences.

Preparation, steps and follow-up

As preparation, clear information must be collected regarding what measure must be monitored, what the original objective of the measure was, what the effects of the measure were meant to be and what the time period in which those effects were to manifest themselves was meant to be

The principle behind the Deming Circle is initiation and continuation of activities to maintain the originally intended risk reduction. The plans for an activity must be followed by execution of the activity, followed by measurement of the results. The results are then compared to the original objectives. Based on this comparison, new activities are formulated. The learning experience from the previous activities are included in the new activities.

This model can be used to monitor activities and can be particularly useful in the management of improvement activities.

Several different versions of this model have been developed, including the DOVE model, which is based on the Diagnose, Design, Change and Evaluate cycle. The different versions are all based on Cybernetics (Ashby).

Checklist of conditions

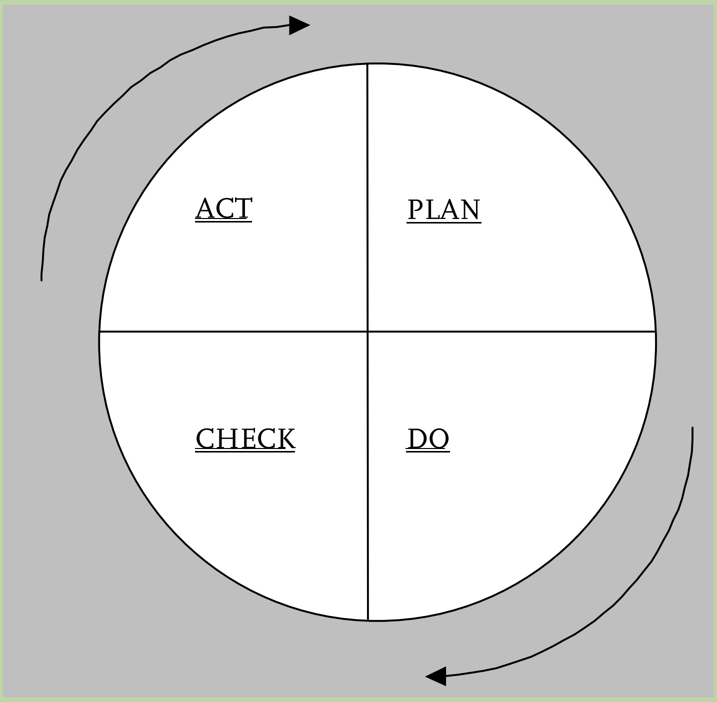
The model requires concrete objectives as a point of departure. Vaguely or inconsistently formulated objectives make development and management of improvements difficult.

It is important to note that this model does not have a clearly defined starting or ending point. It can be used at any point in a process and is iterative in nature. Given the complex and dynamic environment in which measures must be implemented, the model must be continuously redeployed to maintain the links in the Plan, Do, Check and Act cycle.

Sources

Ashby, W. (1956) *An introduction to cybernetics*, London: Chapmann & Hall Ltd.

Have, S. ten e.a. (1999) *Het management modellenboek: zestig ideeën toegankelijk gemaakt',* Elsevier: The Hague


ACT
PLAN
CHECK
DO

WORK FORMS

This section gives a description of a number of work forms that can be used during risk analysis. In this manual, the term work form is used in its very broadest sense. An interview is a work form for our purposes, but a symposium is also a work form. In addition, many work forms are combinations of other work forms or are derived from other work forms. In this section, we therefore distinguish between two types of work forms. Work forms that focus on orientation and investigation (1) and work forms that focus on discussion and debate (2). The descriptions of the work forms consist of a brief description of the *essence* of the work form, followed by information on the *usability* of the work form and, finally, followed by a *checklist of conditions* for use of the work form.

Deskresearch

Essence

A commonly used work form in the initial phase of risk analysis is desk research. Desk research involves consulting secondary sources such as reports, books, memos and policy documents. Desk research is characterised by the use of existing materials by the analyst.

Usability

In the risk analysis phase, consulting earlier analyses and gathering information on events that resulted in damage in the past can be revealing activities. Based on the available material, decisions regarding what items require further study can be made and a strategy for accomplishing that optimally can be developed. Important search locations for desk research include archives, libraries (e.g. university and knowledge institution libraries) and the Internet.

Checklist of conditions

Desk research is time-consuming and can involve a great deal of effort, which is why the issue under investigation and the scope of the research must be clearly formulated in advance.

Interviews

Essence

An interview offers the possibility of gathering qualitative information from experts, the parties involved, decision makers and other actors relevant to the risk analysis with a relatively limited amount of preparation. Interviews can also be conducted by telephone.

Usability

Discussion partners for every study must be carefully selected, e.g. based on expertise or involvement. Because the discussion partners may slant the information they provide based on their own vision or as a result of their personal interests in a given situation, the total population of discussion partners must be properly balanced. In other words, it is important to find different visions – if they exist – so that the visions can be compared and analysed for relevance to the situation.

Checklist of conditions

Even though each interviewer will have his or her own individual interviewing style and this style must be maintained in the interests of authenticity, there are some general guidelines for interviews. It is important to be prepared for the discussion, for instance, and to respond to the interviewee: to listen intently, summarise the points made, ask depth questions and probe at the appropriate moments. The interview must be flexible enough to allow the interviewee to express his or her personal opinions. The interviewer must also be able to intervene in the discussion to steer the discussion in the appropriate direction. There are four types of intervention:

- Content intervention: getting to the core of the issues, making nuances visible, ensuring that the participants are heard and understood by one another, organising the material that has been discussed;
- Procedure intervention: structuring the discussion, using time optimally, working systematically, summarising conclusions before continuing with new topics;
- Interaction intervention: eliminating barriers in the conversation, giving less active participants the chance to express themselves (in group interviews), uncovering hidden agendas, creating an atmosphere of co-operation;
- Emotional intervention: creating an open atmosphere, recognising difficult feelings, creating opportunities to discuss resistance, uncovering underlying interests.

Although conducting an interview does not have to be a time-consuming activity, organising the interview can be, particularly if several interviews must be conducted in a limited period of time. The time and effort required to perform interviews also depends on how the interviews are processed. Writing up an interview takes about two and a half times the original length of the interview.

Excursions

Essence

De An excursion can be organised in the risk analysis phase to obtain insight into processes and organisation of a sector or service. The practical knowledge of the processes and organisation of a specific service or sector obtained during an excursion is a solid and reliable basis for subsequent risk inventory activities.

Usability

Excursions are particularly appropriate for gathering knowledge regarding relatively new services and technologies. The telecommunications sector, for instance, develops particularly quickly and has introduced countless new products and services in recent years. These new products and services are all accompanied by new risks. Because these products and services are developed in the market, policy makers may be confronted with a continuous information backlog. Risk analyses involving new products or services is never a simple task. An excursion makes it possible to obtain insight into underlying processes in a relatively limited period of time.

Excursions are also a good way to maintain close contact with the sector. Policy makers who organise excursions to a company are giving off positive signals, signals of involvement and interest. An involved attitude on the part of the policy maker contributes to a co-operative attitude on the part of the sector. Emitting signals of involvement at an early stage can increase the willingness of the sector to provide information and co-operate in risk analysis later.

Excursions are particularly important in cases involving analysis based on methods such as the External Input Model and Path Analysis.

Checklist of conditions

Proper preparation is essential for a successful excursion. Determining the objective of the excursion in advance keeps the focus during the visit sharp and increases the added value of the visit.

An excursion does take time, particularly if the excursion is planned to obtain greater insight into specific processes. It is also important that the appropriate people from the sector are involved, people with knowledge of the processes under consideration.

Inspection

Essence

An inspection during the risk analysis phase is similar to an excursion in many respects. Both work forms focus on obtaining practical insight into the processes and organisation of a sector or service. However, the scope of the excursion is limited to obtaining a better picture of the factors so that those factors can be included in the risk analysis, while an inspection is not limited to gathering information, but extends to verification. Based on the insight obtained during an inspection, the organisation that has been visited can be warned for non-compliance with regulations or for taking unacceptable risks. Inspections may result in the formulation of extra measures for the organisation, compulsory measures in many cases.

Usability

An inspection is particularly suited to situations in which procedures and regulations already exist for the limitation of (recognised) risks. Inspections can be planned to check procedures and compliance with the applicable regulations. An inspection can also be used to make a sector or institution aware of best practices and improvement possibilities, in part because an inspection committee visits numerous sectors and institutions and is able to contribute the insight obtained from other inspections. In cases in which the inspection committee is composed of experts, an inspection offers the sector or organisation being inspected an opportunity to obtain free advice.

Checklist van voorwaarden

Proper preparation is extremely important and the reason for the inspection must be made clear in advance. Is the inspection intended to spread best practices and to offer recommendations for improvements? Or is the inspection intended to check and enforce (and issue sanctions where necessary)?

The composition of the inspection committee is also important. How well represented are the various types of knowledge and expertise in the committee? Should the committee also include managers of comparable locations to stimulate the exchange of insights and best practices?

Inspections are extremely time-consuming for both the inspection committee and the sector or organisation subjected to the inspection. Both parties must be thoroughly prepared for the inspection.

(Online) surveys

Essence

A survey is a questionnaire-based method for gathering information from a large number of people. The target group is defined based on the purpose of the survey. In the case of a survey designed to gather information on how citizens perceive safety, a representative random sample would be a logical target group choice. If the purpose of the survey is to obtain insight into new threats that have not been analysed in the past, a representative random sample would be neither necessary nor useful. The target group in this case would be limited to a select group of people who are able to think out-of-the-box.

Usability

A survey is an appropriate work form in situations in which a large group of respondents must be questioned or in situations in which geographic considerations make bringing the respondents together centrally impossible. A questionnaire can consist of open questions, multiple choice questions or a combination of the two types of questions. Multiple choice questions are usually used for quantitative surveys, while open questions are generally used in qualitative surveys. Questionnaires can also take different forms: written questionnaires distributed via normal mail or e-mail, online questionnaires (via Internet) and SMS-based questionnaires.

When designing a survey, the following steps can be used:

1. Determine the objective of the survey;

2. Determine the target group (the respondents);

3. Formulate the questions. The questions posed in surveys must be simple and unambiguous. This means that complex questions that actually ask more than one question are not suitable for surveys and that the questions may not be open to multiple interpretations;

Formulate response categories. Response categories must be unambiguous, but also complete.

Checklist of conditions

An important point of attention is motivating the respondents to participate. This demands a personal approach and attention.

Surveys are generally anonymous and generate a result that is a gross average of the responses received. This, plus the fact that part of the target group will not respond, must be taken into account. If the non-response is selective, this fact must be taken into account when interpreting the results. Selective non-response is a failure to respond on the part of a specific subset of the target group, e.g. a group of experts who comprise the most relevant and the largest subset of the target group for a particular survey.

Proper selection of response categories is also important. The possible responses must include all values, from very large (positive, important) to very small (negative, unimportant) for instance. On the other hand, experience shows that use of more than six response categories is not recommended. In addition, the concentration level of the respondents must also be taken into account, which means that the number of questions must be limited.

Drawing up a questionnaire can cost a great deal of time because of the precision and clarity that must be built into the questions, which is why experts are often called in to design questionnaires.

Polls

Essence

A poll is a short electronic survey. In a poll, the participants are asked to respond to a statement, e.g. to indicate whether they agree or disagree. A poll, which can basically be compared to a thermometer, is meant to obtain a quick impression of how participants feel about a (controversial) subject. For instance, a poll could be used to obtain an impression of what percentage of the Dutch population would or would not be happy to live in the vicinity of a GSM mast. The outcome of a poll can constitute relevant policy input.

Usability

A poll is particularly feasible in situations that do not require in-depth questioning, but for which a number of short questions must be asked. The steps followed to design a survey can also be followed when designing a poll:

1. Determine the objective of the poll;

2. Determine the target group (the respondents);

3. Formulate the questions. The questions posed in polls must be simple and unambiguous. This means that complex questions that actually ask more than one question are not suitable for polls and that the questions may not be open to multiple interpretations;

Formulate responses.

Checklist of conditions

Defining the target group and determining how to approach the members of the target group are important points of attention when designing polls.

Polls can be developed with relative speed and ease. No specific expertise is required to design a poll.

Delphi-method

Essence

De The Delphi method is a written survey methodology based on repeated, systematic questioning of a large group of experts on a specific topic.

The principal advantage of the Delphi method is that it can be used to involve a large, geographically distributed group of participants in risk analyses. This makes the Delphi method an appropriate work form for consulting international experts, for instance, provided contact with the experts in question is already structured in a way that motivates them to participate. Another advantage of the Delphi method is that the experts can be asked to respond anonymously. Yet another advantage is that there is no danger of 'group think' when using the Delphi method.

Usability

The Delphi method is particularly useful when a topic requires deeper analysis than can be accomplished with the survey or poll method described earlier in this section. This work form consists of a number of different steps:

1. Define the subject of the risk analysis. This definition must be posed in terms that are not open to multiple interpretation by the experts;
2. Select the experts;
3. Send the questions for the first round. These questions must be open enough to allow the experts to contribute their own personal viewpoints;
4. Experts respond to the first round of questions and return the results;
5. Analyse and summarise the responses from the first round;
6. Send the questions for the second round. In this round, the experts are asked to respond to the results for the first round, e.g. using propositions;
7. Experts respond to the second round of questions and return the results;
8. Analyse and summarise the responses from the second round;
9. Send the questions for the third round. In this round, the experts are again asked to respond to the results for the previous round. Examples of the types of questions asked include questions regarding the conditions under which certain responses from the previous round apply or do not apply;
10. Analyse and aggregate the answers for the third round.

Checklist of conditions

The most important point of attention when using the Delphi method is motivating the target group to participate. The fact that the participant decides when to complete the questionnaire is an advantage on one hand, but also a disadvantage because completing the questionnaire may not be given a very high priority by some participants. To guarantee involvement on the part of the participants, a personal approach and extra contact by telephone may be required. Another point of attention when using this method is the long throughput time it involves. Very well informed analysts are also required to work with the Delphi method. The analysts must interpret the results from each round, summarise them and develop challenging questions for subsequent rounds based on their analysis.

Electronic Boardroom

Essence

An electronic boardroom session is an electronically supported meeting. Each electronic boardroom participant has a laptop that can be used to contribute to the process as it unfolds, at the same time as the other participants, e.g. by delivering a contribution to a brainstorming session. The data entered by the participants appear immediately on a central screen. The input can also be clustered (e.g. in cases involving overlaps) and prioritised by allocating scores to items.

Usability

An electronic boardroom can be very helpful in situations in which as many ideas as possible must be collected in a limited period of time. It is a form of brainstorming (see also the work form ‘Brainstorming’ later in this section). The participants work simultaneously with an electronic system, thus limiting the total required meeting time.

Because the participants submit their contributions at the same time, but separately, the domination effects that can occur in other types of group work forms do not occur in the electronic boardroom, i.e. everyone in the boardroom is equal, despite differences in hierarchical position, verbal skills and personal desire to score. Because the input is anonymous, this work form also makes it possible to uncover risks that might otherwise not receive the attention they deserve.

The electronic boardroom also helps to generate broad-based support. The participants can use the system to quickly and anonymously vote on items entered via the system, immediately generating information on the opinions of the participants regarding the issues. In addition to tallying up votes, the system can also calculate how diverse the opinions are (standard deviations). This information can be used to focus the discussion on issues that are viewed from radically different standpoints.

Checklist of conditions

Create opportunities for verbal discussion. The electronic boardroom is based on written participation, but that is not always enough when a participant really wants to make a point. In that context, the delivery of electronic input via the computer has to be regularly interrupted for discussion moments, e.g. to discuss the results of the brainstorming session.

Also develop a back-up plan for use if the computer system goes down.

Electronic boardroom systems are expensive to purchase, but they can also be hired for short periods. The cost of hiring a system must be taken into account when planning an electronic boardroom session.

Brainstorming

Essence

Brainstorm-technieken Brainstorming techniques are often used to generate creative and appealing ideas in a group. The focus during brainstorming sessions is placed on generating quantity rather than quality. Other important rules for brainstorming include ‘be a good listener’ and ‘wait to give your opinion until you are asked for it’.

Bruikbaarheid

Een Brainstorming can generate a large number of new and original ideas if a stimulating environment is created for the session. A round-table setting, for instance, flip-over charts, coloured markers and stickers for scoring purposes also contribute to a stimulating and creative environment. In addition to the appropriate environment, certain rules need to followed:

- Explain what the working method is and allow the participants to ask any questions thy may have;
- Start with some activities to loosen the group up, to inspire the participants and get them into the right mood for free-style brainstorming;
- Dump the first ideas that come up to create space for new ideas. Many of the first ideas will be more obvious than those generated later;

Generate as many ideas as possible and have the participants clarify them, e.g. by writing them up on a flip-over chart or on cards that can be pasted to a wall (one idea per card). The advantage of using cards is that they can be easily clustered and prioritised later.

Checklist of condtions

The success of a brainstorming session depends on how closely the rules given above are followed. Ignoring one or more of these rules will result in a brainstorming session that is one-sided, dull and lacking in creativity.

The discussion leader plays an essential role in the brainstorming session, by maintaining balance between the different participants. The discussion leader must be well versed in the content of the brainstorming session, but must not force the participants to accept his or her personal opinions.

Brainstorming sessions involving complex issues can take an extremely long time. In cases involving complex issues, different brainstorming rounds should be organised to avoid overtiring the participants and dulling their creativity.

Symposiums

Essence

A symposium is a (large) meeting in which different experts convey their knowledge to a large group of listeners. Many symposiums also include a discussion period during which the participants are given an opportunity to discuss the material with the experts.

Usability

Organising a symposium is a great deal of work and can be quite costly. This work form is appropriate for situations in which adequate time and funding are reserved in the risk analysis process to organise this work form. This work form is also appropriate for situations in which knowledge must be conveyed to a large group, e.g. in cases involving risk analysis for a relatively new product or service and in cases involving new and unclear or controversial developments in a sector. A symposium can be used to distribute knowledge held by a limited number of experts, e.g. regarding the processes and risks of a new product or service, to a newly emerging sector or to a sector that is confronted by information backlogs.

Symposiums are also extremely appropriate for the exchange of experiences and best practices.

Checklist of conditions

A point of attention that must be taken into account when organising a symposium is that the most important stakeholders must be represented at the symposium, e.g. as a speaker, to give the symposium the proper weight. The quality of a symposium also depends on various factors, including the degree to which parties who represent divergent opinions on a given issue are persuaded to participate.

A symposium is difficult to organise in response to immediate, urgent problems. Preparations for a symposium must be extremely meticulous, thorough and professional, which is one of the reasons that symposiums cost a lot of time and money.

(Parliamentary) debates

Essence

A debate is a suitable work form for risk analysis in situations in which a strong consensus regarding the chance of risks, the effects of risk, public perception of risks and appropriate measures for a risk does not appear to exist

Usability

In a debate, two parties discuss a statement based on pre-assigned role. One of the parties is assigned the role of affirmative (supporter of the statement) and the other the role of negative (opponent of the statement). In a previously agreed time period, the parties present and defend their respective standpoints with logical arguments and convincing reasons. There are three rounds in a debate: topic presentation, rebuttal and conclusion:

§ Topic presentation: In this round, the affirmative presents his case with argumentation, then the negative presents his case with argumentation. The respective viewpoints are clear at the end of this round.

§ Rebuttal: In this round, the two parties ask questions and express criticism to rebut the argumentation presented in the first round. To create a strong foundation for their respective viewpoints, the two parties must offer extremely convincing criticism of the viewpoint they oppose.

§ Conclusion: In this round, new argumentation cannot be presented. The two parties summarise the points made during the first two rounds and present their conclusions regarding the statement.

A good debater is able to find a balance between argumentation and power and between opposition and compromise. An audience is present during the parliamentary debate.

Two points of departure are possible for this type of debate. The debaters can be asked to take a reasonable position or a strategic position. In the case of a reasonable position, good argumentation is the primary objective of the debate. In the case of a strategic position, defence of the debater's personal position is the primary objective.

Checklist of conditions

The organiser and the attendees need to realise that a truly good debater is able to defend complete hogwash, which means that certain restrictions apply when interpreting the results of this work form. The primary purpose of the debate is to uncover all relevant argumentation, not to judge one of the debaters the winner of the debate.

It is also important to keep the debate focused. In the heat of the moment, the participants can get caught up in discussions regarding risk analysis related items rather than focusing on the issue under debate.

Digital debates

Essence

During a digital debate, actors from different fields conduct extensive discussions with each other regarding a specific policy problem. The participants can conduct lengthy discussions with each other via the Internet. Anyone with Internet access can participate (unless of course log-in names and passwords are used to limit access to the debate).

Usability

Digital debates have a relative large scope, which makes it possible for large numbers of people to participate and react. This work form is primarily used in the context of 'public participation' in various policy formulation processes.

A digital debate can also be an appropriate work form for risk analysis purposes, e.g. if information regarding how citizens perceive risks is required or if information on whether citizens would be willing to pay extra for higher continuity levels in the electricity network is required. If statistical validity does not play an important role in the risk analysis, a digital debate can be used to identify risks and measures with a large and varied group of participants. Digital debate is also a suitable option when performing risk analyses with cross-border implications because it makes it relatively simple to obtain opinions from the experts and other parties involved in other countries, which broadens the risk analysis perspective.

Checklist of conditions

Het Setting up a successful debate on the Internet is more work than it appears to be at first glance. It takes time and visitors do not just wander onto the debate site uninvited. Just as in a live debate, an experienced discussion leader with knowledge of the issues under discussion is required to keep the digital debate on track. The objective and design of the debate must be clear and the tool used to conduct the debate must work intuitively and offer a good overview of the discussion.

The involvement of influential participants can also help make a digital debate successful because it motivates and increases the input offered by other participants. The results of the debate must also be clearly formulated.

Sources

Leeuwis, C. (1999). Policy-making and the value of electronic forms of public debate. Underpinning, assumptions and first experiences. In: d'Haenens, L. (Ed.), Cyber identities. Canadian and European presence in cyberspace. International Canadian Studies Series. 99-109. University of Ottawa Press. Ottawa.

K. van Doorn and E. Schippers (2003), 'Burgers, overheid en digitale debatten, Handvatten uit de praktijk', Eburon.

Expertmeetings

Essence

Expert meetings are organised to obtain the expert opinions regarding specific ideas or proposals. The number of participants in an expert meeting is usually limited. Based on their individual area of expertise, the experts give their opinion on the idea or proposal or give the required specific information, e.g. specific information on a given target group.

Usability

An expert meeting is particularly useful in situations in which expertise is required, but the time and financial resources needed to organise a larger scale work form are lacking. An expert meeting can be used in almost any phase of an analysis. Expert meetings are easy to organise because of the relative lack of peripheral conditions that must be met.

Checklist of conditions

Timely scheduling is an important consideration when organising an expert meeting. Highly educated professionals must be contacted regarding the expert meeting far enough in advance to free up space in their busy schedules. A personal approach can help.

It is also important to ensure that the right experts talk about the right topics and deliver the right contributions. This is important because the agenda for an expert meeting usually consists of several topics. An expert may want to participate in discussion of a topic for which he does not possess the necessary expertise, thus decreasing the time available to the expert on that topic who is present. Conscious human acts such as terrorism, for instance, fall into a completely different area of expertise than estimation of the impact of such an act on the energy sector. This has to be taken into account because the two issues may be considered simultaneously during an expert meeting, e.g. when chance-effect matrices are handled.

14 Work conferences and work studios

Essence

A work conference or work studio is a work form in which the participants are stimulated to roll up their sleeves and get to work. Various points of departure can be used as the basis for this work form: from presentations to seminars and from discussions to role playing exercises.

Usability

A work conference or work studio can be used to deepen existing insight into a problem and to explore possible solutions. A work studio can be conducted for a group of ten people and could consist of a series of meetings held to intensively explore the different ramifications of a single specific issue.

Checklist of conditions

A work studio demands great effort on the part of the participants, particularly when they are from different geographic regions. The work studio organiser has to make the appropriate investment of time and effort to make the work studio appealing to the participants.

Preparing a work conference takes a great deal of time and, depending on the type of conference, can also cost a lot of money

Simulation and gaming

Essence

A simulation or a game is a simulation of a real situation to uncover the mechanisms that occur in real life. Simulations can be used in risk analysis processes to think through events, organisational forms and measures as a group and to analyse aspects of measures such as effectiveness and broad-based support.

Usability

A good simulation can contribute to awareness of the need for change because it confronts the participants with their own behaviour and also offers alternatives via a reflective process. Feedback and assumption of other roles can influence behaviour. Successful simulation also helps to develop new skills.

Simulations also offer a safe environment for experimentation.

Checklist of conditions

Simulations can only be successful if the participants are completely free to play the roles that they assume. If they feel restricted, e.g. because they have no personal interest in a successful simulation, the simulation will not deliver the desired results.

Software can play an important role in simulations. The costs of hiring or purchasing software must be taken into consideration when planning a simulation.

APPENDIX 1: BERENSCHOT - TU DELFT PROJECT TEAM

This manual was written by a project team consisting of employees of Berenschot Process Management and members of the TU Delft Policy Studies and Security Studies departments.

Project team members from Berenschot:

- B.PA. (Bill) van Mil, project leader
- A.E. (Annelies) Dijkzeul
- R.M.A. (Ronnie) van der Pennen
- F.A. (Frank) Beemer

Project team members from the TU Delft Policy Studies department:

- E.F. (Ernst) ten Heuvelhof
- M.J.G. (Michel) van Eeten

Project team members from the TU Delft Policy Studies department:

- B.J.M. (Ben) Ale
- A.R. (Andrew) Hale
- L.H.J. (Louis) Goossens

The project team made grateful use of suggestions made by the sounding board group. The sounding board group consisted of:

- I. (Ilse) Landa (Economic Affairs)
- S.A. (Simon) van Merkom (Economic Affairs)
- J.S. (Jacqueline) de Braal-Schouten (Economic Affairs)
- A. (André) Griffioen (Ministry of Internal Affairs)
- E.R. (Ed) Buddenbaum (Economic Affairs)

The project team also used suggestions made by the people interviewed for this manual, some of whom also gave feedback on previous drafts of this manual. The project team is extremely grateful for their suggestions and assistance.

APPENDIX 2: LIST OF DISCUSSION PARTNERS

The project team conducted discussions with the following people (listed in alphabetical order by last name):

- Mr. J. Book, Law Enforcement Expertise Centre, Ministry of Justice
- Mrs. J.S. de Braal, Ministry of Economic Affairs
- Mr. R. Brieskorn, Ministry of Housing, Regional Development and the Environment (VROM)
- Mrs. Demon, Ministry of Transport, Public Works and Water Management
- Mr. M. van Doeveren, Dutch National Bank (DNB)
- Mrs. M. Dunn, Center for Security Studies (CSS) Swiss Federal Institute of Technology (ETH Zurich)
- Mr. A.B. Engberts, Ministry of Finance
- Mr. A.F. Griffioen, Ministry of the Interior and Kingdom Relations
- Mr. A.O. Haccou, KPN
- Mr. Hekke, Ministry of Transport, Public Works and Water Management
- Mr. D. Holtrop, Ministry of Ministry of Housing, Regional Development and the Environment (VROM)
- Mr. M. Ligthart, Ministry of Ministry of Housing, Regional Development and the Environment (VROM)
- Mrs. M. Luursema, NCTb
- Mr. T. Muller, Ministry of Transport, Public Works and Water Management
- Mr. Plekkenpol, AT Osborne
- Mr. Race, ING Bank
- Mr. Reterink, Berenschot
- Mrs. Riemersma, Security Research Board (Onderzoeksraad voor veiligheid)
- Mr. L.F. Rog, Telfort
- Mr. R. Ruitenberg, COT
- Mr. M. Schraver, Ministry of Ministry of Housing, Regional Development and the Environment (VROM)
- Mr. M.J.W. Spit, AIVD
- Mr. J.M.A. van de Ven, Hewitt Associates
- Mrs. Verstege, Ministry of Transport, Public Works and Water Management
- Mr. D.A. van den Wall Bake, Berenschot
- Mr. D. Weger, Ministry of Transport, Public Works and Water Management
- Mr. F. Wieleman, Ministry of Economic Affairs
- Mr. Woldring, GasUnie

APPENDIX 3: BIBLIOGRAPHY

- Ashby, W. (1956) *An introduction to cybernetics*, London: Chapmann & Hall Ltd.
- Belm, G.K. and B.F. Hobbs (1997) Event Tree Analysis of Lock Closure Risks, In: *Journal of water resource planning and management*, Vol. 123, part 3, pp. 169-178
- Berg, R. van den (1984) *Voorlichting: Strategie tot verandering*, Amsterdam: Boom
- Bovens, M.A.P. and M. Scheltema (1999) Rechsstatelijke redeneerpatronen, In: *Wetenschappelijke Raad voor het Regeringsbeleid*: *Over publieke en private verantwoordelijkheden, Voorstudies en achtergronden*, The Hague
- Burdick, G.R. and J.B. Fussell (1983) On the Adaptation of Cause- Consequence Analysis to U.S. Nuclear Power Systems Reliability and Risk Assessment, In: *System Reliability and Risk Assessment*, Knoxville: JBF Associates Inc., Knoxville
- Center for Chemical Process Safety (1992) *Guidelines for Hazard Evaluation Procedures,* American Institute of Chemical Engineers
- De Bruijn, Ten Heuvelhof, In 't Field, (1999) *Procesmanagement: over procesontwerp en besluitvorming*, Schoonhoven: Academic Service
- Dunn, M. & I. Wigert, (2004) *CIIP Handbook 2004, Critical Information Infrastructure Protection: An Inventory and Analysis of Protection Policies in Fourteen Countries*, p. 236
- Dunn, M., Wigert, I. (2004) *International CIIP handbook 2004*, Zurich
- Law Enforcement Expertise Centre (2004) *The Table of Eleven: a versatile tool*
- F. Jensen (1996) *An Introduction to Bayesian Networks*, Springer Verlag
- Greenberg, Harris R. and Joseph J. Cramer (1991) *Risk Assessment and Risk Management for the Chemical Process Industry*, New York: Van Nostrand Reinhold
- Harn, K. van & P.J. Holewijn (2003) *Markov-ketens in discrete tijd*, Epsilonuitgaven: Utrecht
- Have, S. ten e.a. (1999) *Het management modellenboek: zestig ideeën toegankelijk gemaakt*, Elsevier: The Hague
- Heezen, A. (1999) *Basisstudie Bedrijfseconomie*, Wooden: Stenfort Kroese
- Helsloot, I & N. Rosmuller (1994) Jaarboek onderzoek 2000
- Henley E. and H. Kamamoto (1981) *Reliability engineering and risk assessment*, Englewood Cliffs: New York.
- Horngren, C.T. et al (2002) *Management and Cost Accounting*, London: Prentice Hall
- Johnson. G and K. Scholes (1999) *Exploring corporate strategy*, Prentice Hall: London

- Cabinet Memorandum (2000) *Privatisering en liberalisering in netwerksectoren*

- Klinke A. & O. Renn (2002) A new approach to risk evaluation and management: Risk-Based, Precaution-Based and Discourse-Based strategies, In: *Risk Analysis: an international journey: an official publication of the Society for Risk Analysis*, Vol. 22, part 6, pp.1071-1094

- Read, F. P. (1983) *Loss Prevention in the Process Industries*, Oxford: Buttersworth-Heinemann

- Leeuwis, C. (1999) Policy-making and the value of electronic forms of public debate. Underpinning, assumptions and first experiences. In: *Cyber identities: Canadian and European presence in cyberspace*, p.99-109. Ottawa: University of Ottawa Press

- Luijf, Eric, M. Klaver, J. Huizinga. (2001) *The Vulnerable Internet: A Study of the Critical Infrastructure of (the Dutch Section of) the Internet*, The Hague

- Ministry of Justice Law Enforcement Expertise Centre (2004) *De Tafel van elf: beknopte toets voor de handhaafbaarheid van regels*, The Hague

- Motion of Lower House member Wijn, 2663 no. 20

- Papazoglou, M., & Heuvel, W.J.A.M. van den (2000). Configurable business objects for building evolving enterprise models and applications. In: *Business Process Management: Models, Techniques and Empirical Studies*, pp. 328-344, Berlin: Springer-Verlag.

- Perrow, C., (1984) *Normal Accidents*, New York: Basic Books

- Porter, M.E. (1998) *Competitive strategy: Techniques for Analysing Industries and Competitors*, New York: The Free Press

- Council for Transport, Public Works and Water Management (2003) *Tussen droom en daad*, a preliminary study, published in 2004, performed by Berenschot for the recommendation 'Hoezo marktwerking'

- Rasmussen J., e.a. (1987) *New Technology and Human Error*, London: Wiley

- Reason, J. (1997) *Managing the Risks of Organisational Accidents*, Aldershot: Ashgate

- Reenen, P. (2000) *De Tafel van Elf*, The Hague: SDu Publishers

- Reenen, P. van, D. Ruimschotel and H.M. Classes (1996) *Nieuwe instrumenten voor de rationalisering en optimalisering van beleid en wetgeving: vergelijking van ketenbenadering en Tafel van Elf,* In: *Beleidsanalyse*, 1996-4

- Rosenthal, U. Staal, B. Storm, K.J, (2002) *Als je leven je lief is*, Max Geldens foundation for social renewal, p.7

- Ruimschotel, D. e.a. (1996) De Tafel van Elf, een conceptueel kader en een instrument bij rechtshandhavingsvraagstukken, *In: Beleidsanalyse*, no. 3, p.4

- Schwartz, B, (1988) Forecasting and scenarios, In: *Handbook of system analysis*, Chichester: Wiley

- Slovic (1992) Perception of Risk: Reflections on the psychometric paradigm, In: *social theories of risk*, New York: Plenum, pp. 117-152

- Slovic (1999) Trust, emotion, sex, politics, and science: surveying the risk-assessment battlefield, In: *Risk Assessment*, vol. 19, pp. 689-703

- TNO FEL 03-C002, *Bescherming vitale infrastructuur: Quickscan naar vitale producten en diensten*, TNO

- TNO-FEL Stratix Consulting Group, (2001) *Samen werken voor veilig internetverkeer*, Final report on the research project 'kwetsbaarheid van het internet (KWINT), on behalf of the Ministry of Transport, Public Works and Water Management

- Twist, M. van, and W. Veeneman (editor) (1999) *Marktwerking op weg: over concurrentiebevordering in infrastructuurgebonden sectoren*, Utrecht: Lemma

- Vlek. Ch. (2001) Risicopsychologie: elk voordeel heeft zijn risico, In: *Hypothesis, Research and Science Quarterly*, volume 8, no. 31, pp.12-15, The Hague: NWO

- Vossen, R.M.M. e.a. (2003) 'Naleving en handhaving van regelgeving', In: *Justitiële Verkenningen*, annual 29, no. 9

Weger D. de (e.a.) (2004) *Leidraad scenario-analyses voor ongevallen in tunnels*, COB Bouwdienst Rijkswaterstaat