DEMA's Approach to Risk and Vulnerability Analysis for Civil Contingency Planning

On risk and vulnerability analysis in Denmark

Risk management techniques, including risk and vulnerability analyses, are used by many private sector companies in Denmark and promoted by various industry associations. Such analyses are not uncommon in the public sector either, and are carried out regularly on subjects such as environmental impact studies, food safety, public health, transportation regulation, infrastructure projects, etc. Within most central government institutions in Denmark, however, systematic use of risk and vulnerability analysis is still not an integrated part of their wider civil contingency planning responsibilities.

The Danish *National Vulnerability Evaluation (National Sårbarhedsudredning)* – an inter-departmental, cross-sector evaluation from 2004 – aimed to alter this situation. The evaluation's main report and its seven sub-reports can in themselves be said to represent ambitious, but very general, risk and vulnerability analyses for the nation as a whole and for selected sectors of society. The evaluation stressed that risk assessment methods was a still a new area that more central government authorities ought to implement. And one of the 33 specific recommendations was that a generic risk and vulnerability analysis model should be developed for civil contingency planning.

This project was subsequently assigned to DEMA, and the model (presented below) was completed in late 2005. The official launch took place at a 14 December 2005 National Preparedness Conference, where the model was made available in parallel with DEMA's first annual *National Vulnerability Report*. The model is (as yet) unfortunately only available in a Danish-language version.

Although the tendency should not be exaggerated, interest in risk and vulnerability analysis is now rising among public sector organisations in general, whether to follow up on the *National Vulnerability Evaluation*, as a result of separate initiatives or to comply with new national and international legislation. A recent "quick scan" by DEMA has shown, that specific models for risk and/or vulnerability analysis are currently or will soon be used among local fire and rescue services, harbour authorities, electricity and natural gas suppliers, the Danish central bank, the police Security Intelligence Service, the National Centre for Biological Defence, and the National IT-and Telecom Agency. To further this trend, DEMA's office for Civil Sector Preparedness will actively promote its new model for risk and vulnerability analysis throughout 2006.

The benefits of risk and vulnerability analysis

In DEMA's view, risk and vulnerability analysis is a tool that can serve the following seven functions:

- New knowledge and overview: The analysis increases participants' knowledge and overview of threats, risks and vulnerabilities. This can in turn help them to identify and prioritise countermeasures, which may prevent incidents, limit impacts, and reduce vulnerabilities. The analysis can also help map unnecessary measures or more effective alternatives.

- A reliable basis for decision-making: The analysis gathers essential information and recommendations on risks, vulnerabilities and possible countermeasures. This provides an organisation's senior management with a solid background for making decisions about preparedness issues.

- Effective communication: The analysis can be used to argue the case for suggested or implemented countermeasures – both internally and externally. This increases confidence in the organisations preparedness level among both employees and the surrounding society.

- Exercises: The analysis can be used in connection with scenario-based exercises, training and other competence-building activities

- Co-ordination between authorities: The analysis can uncover risks and vulnerabilities across society's sectors, organisations and critical functions. Knowledge of the crosscutting dependencies and interdependencies may be used to co-ordinate responses between the various authorities with preparedness responsibilities.

- Control: The analysis can assist in double-checking that the organisation conforms to relevant legislation, national and international security standards, etc.

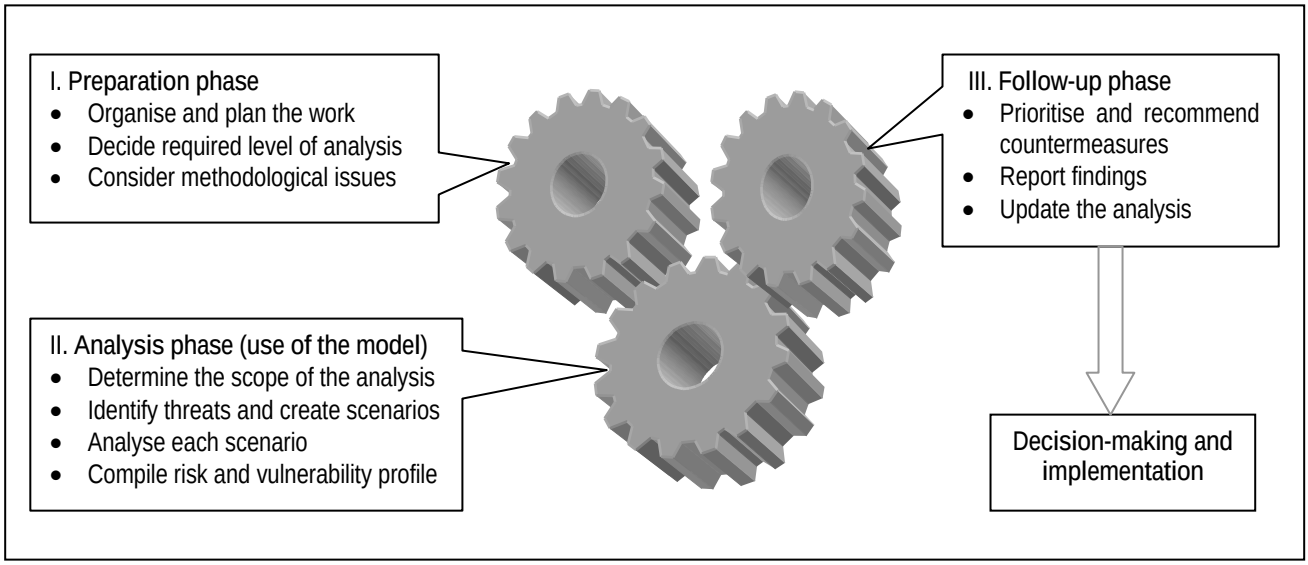
- Strengthening of a "preparedness culture": Systematic work with risk and vulnerability analysis may heighten the preparedness culture within an organisation, by making management and staff aware of the threat they could face, and what is required to handle them effectively. If the analyses are conducted regularly, they may also contribute to integrating safety and security issues into ordinary planning activities and business functions.

DEMA's generic model for risk and vulnerability analysis

Focus: According to the Danish preparedness act, the individual ministers are responsible for planning for the continuity of 'society's functions', each within their respective areas. However, the act does not specify exactly what these functions are. Correspondingly, DEMA's model focuses on the need for continuity of 'critical functions' in case of large-scale disturbances, accidents or outright catastrophes. By critical functions the model refers to activities and services that are indispensable for society. Their importance is such, that any entire or partial loss could have grave consequences for life, health, property, or the environment.

Target group: Risk and vulnerability analyses are rarely required by law or regulation in Denmark, and use of DEMA's model will be on a voluntary basis. The model is primarily intended for central government departments and agencies, which hold political oversight and contingency planning responsibilities within their respective sectors. However, all interested parties are welcome to use the model, especially public and private sector owners and operators of critical infrastructure. Potential users may freely adopt the model in full, adapt it to individual requirements, or merely use it as an inspiration. Some will undoubtedly prefer alternative models that are much more detailed and tailored to specific needs. They are encouraged to continue doing so, if experiences are satisfactory. It is the results that count.

Structure and contents: DEMA's model presupposes a process with the three phases illustrated below:



The model itself (phase II) consists of four main sections:

1. *Determine the scope of the analysis:* Initially it must be decided what to include and exclude. The goal for the user organisation should be to identify and focus on those critical functions that must be maintained in case of large-scale disturbances, accidents or catastrophes. This will invariably entail difficult choices as to what constitutes "critical functions" as opposed to "merely important functions".

2. *Identify threats and create scenarios:* The model contains six pre-defined threat scenarios, along with a "catalogue of threats" to inspire users to formulate their own additional scenarios. The ideal is to outline realistic scenarios where critical functions are significantly affected ("breaking point"), and which therefore require extraordinary countermeasures. Both "worst-case" scenarios and frequently occurring events should thus be excluded from the analysis.

3. *Analyse each scenario:* In this section, users are asked to assess vulnerabilities that may exist in regards to upholding the critical functions under study as well as the risks associated with each scenario. Vulnerabilities are assessed according to existing capacities (or lack thereof) to prevent, mitigate, plan for, respond to and recover from the incident described in the scenario. In order to estimate overall risk levels, numerical values must subsequently be given to likelihood and consequence levels. These values must be chosen with due consideration to the identified relative levels of vulnerability/robustness.

4. *Compile a risk and vulnerability profile*: The model's final section contains an overall risk-matrix (5 by 5). This provides an illustrative graphical comparison of the various threat scenarios analysed in section 3. Furthermore, the profile's diagrams present a visual overview of the most frequently occurring and crosscutting vulnerabilities. The risk and vulnerability profile can thus contribute to subsequent deliberations regarding which possible countermeasures that ought to be prioritised and recommended.

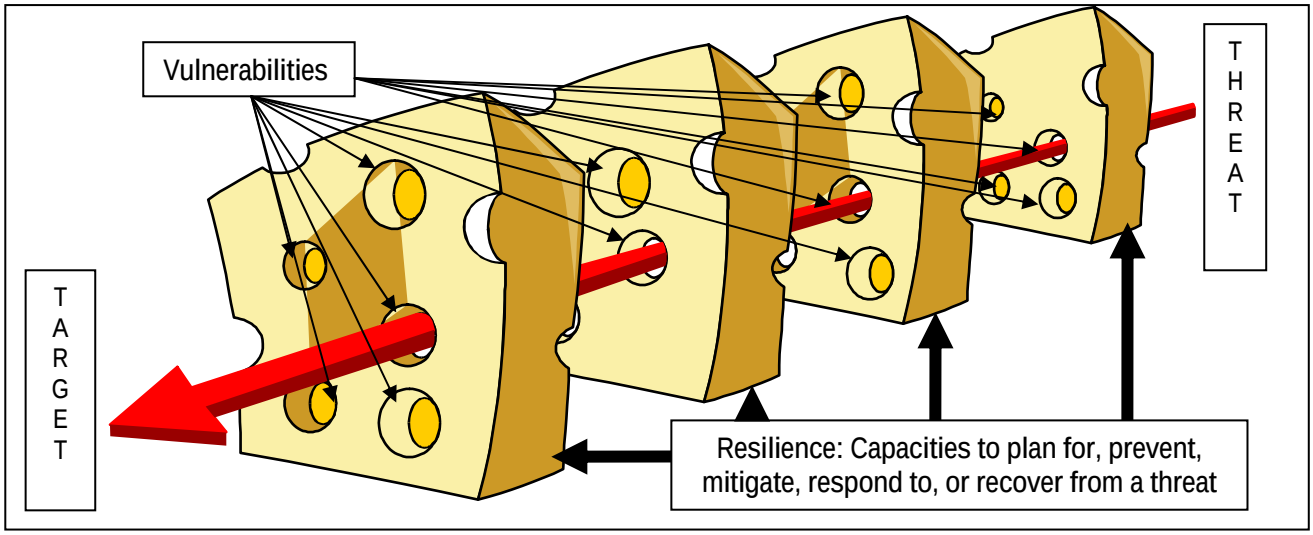
Terminology: Definitions of terms such as risk and vulnerability are notoriously inconsistent - as even the most sporadic review of literature on the subject will show. Given this fact, DEMA's finds it important not to get bogged down in detailed discussions about which precise definitions may be considered "true". All definitions are true - per definition! The point of any definition is simply, that it must be useful, concise and mutually comprehensible in the specific context it is used in. In the context of DEMA's model, the following definitions are offered, with an explicit acknowledgement that alternative interpretations are fully possible.

Risk and vulnerability analysis: An analytical tool with which users may systematically identify and evaluate threats, risks and vulnerabilities, with a view to formulating prioritised suggestions for countermeasures.

Threat: Any adverse circumstance, indication, potential incident or other disruptive challenge. A threat may stem form natural, human, organisational, or technological factors. A threat may be malicious/intended or accidental/unintended, and it may be pre-warned on unexpected. A threat-scenario is an imagined sequence of events, where one or more threats may come into play. *Threat-identification* asks questions regarding the sources, characteristics, causes, and targets of threats. The likelihood and potential consequences if a threat materialises into an incident, on the other hand, are dealt with in the subsequent risk-assessment.

Risk: Risk is a product of the *likelihood* of an incident (a materialised threat) and its possible *consequences*. However, both likelihood and consequences are affected by the vulnerabilities within the system the threat is directed against. *Risk assessment* can therefore not be carried out in isolation, but must take into account the relative degree of vulnerability/resilience. For malicious threats it is particularly difficult to produce likelihood assessments, due to the uncertain "human factor" and lack of historical data. It is typical therefore for these assessments to be treated as indications of the *plausibilit*y, and surrogate measures for likelihood.

Vulnerability: A measure of a given systems strengths and weaknesses concerning its *ability* to function effectively, when faced by threats. A system is vulnerable if it lacks or has a significantly reduced capacity to plan for, prevent, mitigate, respond to or recover from a materialised threat. The opposite of vulnerability is resilience. Vulnerability assessment can be illustrated by the figure below (inspired be James Reasons 'Accident Causation Model' (also known as the 'Swiss cheese model').



Format and underlying principles: DEMA's model has been developed in a user-friendly electronic format. Practical use takes place via a team-based approach, where participants must reach consensus in formulating relatively short answers to the numerous questions in the model. The users are guided through this process by a combination of open-ended text fields, predefined checklists, drop-down menus and wizards. The team-based environment stimulates structured brainstorming sessions, and the composition of the analysis team is in many ways the prime guarantee for the success of the project. The broader the areas of expertise, the more credibility will be assigned to the results.

Given that risk and vulnerability analysis will invariably be subject to a great degree of uncertainty, DEMA's model relies almost exclusively on qualitative rather than quantitative assessments. Rather than hard data and objective truths, perceptions of risks and vulnerabilities will depend on individual competencies, experiences, beliefs and even ethics among the users of the model. From this follows, that the process cannot be planned or carried out in a strictly scientific or objective manner. Or as Albert Einstein once put it: *"Not everything that can be counted counts and not everything that counts can be counted."*

Since normative elements cannot be avoided, the users should strive for the highest possible degree of transparency. A precondition for this is a free and open dialog throughout the process – something that will also help avoid "group-think", where critical thinking is suppressed in order to facilitate feelings of unity.

Broader framework: The model can be treated as a stand-alone tool, but its use should ideally be viewed as an integrated part of wider risk management practices. As such, it may be seen at the first step in a process, which DEMA refers to, as the "Comprehensive Preparedness Planning Cycle". The latter includes a total of six steps: i) The establishment of objectives and organisation; ii) Risk and vulnerability analysis; iii) Prevention; iv) Preparedness; v) Competence development; and vi) Evaluation.

The development of DEMA's model and its methodology

To ensure that the requirements of potential users of the model were taken into account, DEMA appointed a focus group with representatives from the Danish Security Intelligence Service, the National IT and Telecom Agency, the Danish Energy Authority, and the electricity and natural gas sectors. The broad guidelines agreed to by the focus group included that the forthcoming model should:

1. Be easy to use and operate with a concise and easily comprehensible terminology
2. Be scenario-based and primarily rely on qualitative rather than quantitative data
3. Involve structured, team-based, and preferably multi-disciplinary work processes
4. Adopt a flexible format which allows for sector-specific adjustments and modifications
5. Consist of an electronic tool rather than just a written guide - given that the latter often prove more difficult to operationalise when analyses are conducted in praxis

In developing the model, DEMA also drew inspiration from the comprehensive literature on risk management and on risk and vulnerability analysis. In particular, we reviewed handbooks, manuals, self-assessment tools etc. from Canada, the US, the UK, Norway, Sweden, Switzerland, Germany and the Netherlands. Our studies included open-source material from both central and local governments, research institutions and private companies. Close attention was also paid to relevant on-going work within the EU, NATO and the OECD.

On the above background, it was decided to base DEMA's model on the method known as "Preliminary Hazard Analysis" (PrHA). There are a number of advantages associated with this method, including that it:

- Does not require prior knowledge of risk and vulnerability analysis among users
- Can be applied in connection with general analyses of most systems and activities
- Can be applied even though users do not have access to detailed technical or statistical data

Can be carried out by a small group by means of review meetings and, if applicable, field inspections

In addition to relying on PrHA, DEMA's model is characterised by the so-called 'all-hazards approach', which means that it can take into account all types of threats regardless of their cause. Similarly, the model promotes an approach whereby 'contingency planning' (where focus is mainly on risks, i.e. probabilities and consequences) complements 'continuity planning' (where focus is mainly on vulnerability/resilience).

Case Study: Adaptation of DEMA's model for the electricity and natural gas sectors

Following new legislation issued in January 2005, 'vulnerability assessments' will become mandatory within the Danish electricity and gas sectors from 2006. The vulnerability assessments must be carried out by each individual company, and subsequently used in collective vulnerability assessments by Energinet.dk - the state-owned transmission system operator for electricity and gas. The vulnerability assessments will form the basis for much more comprehensive contingency and continuity plans at both company and sector level.

In order to assist the companies, Energinet.dk has adapted DEMA's model for risk and vulnerability analysis to sector-specific needs and requirements. Energinet.dk's model maintains the basic structure and content

but it has been modified in regards to certain scenarios, questions, and graphics. Moreover, the scope has been limited exclusively to risk and vulnerability with respect to upholding the provision of electricity and gas.

A few differences of opinion emerged during the collaboration between DEMA and Energinet.dk, which illustrate that definitions of terms vary considerably. For instance, DEMA’s model defines risk as a function of likelihood and consequences. These two variables are divided into five levels, resulting in a risk matrix with 25 risk level categories. In contrast, Energinet.dk chose to concentrate on consequences and exclude likelihood, which they see as either predetermined in the scenarios or beyond the expertise of ordinary users to assess. As a result, Energinet.dk’s model merely has a consequence matrix with 5 categories.

Feedback from seven electricity companies participating in a pilot project has indicated overall satisfaction with the model. Some issues have been raised, however, demonstrating that a uniform understanding of all aspects of the model is not easily obtained. A few companies have, for example, expressed that they find the predefined scenarios lacking in detail – whilst others find that they are in fact too detailed. The pilot project has also shown that the companies find it easier to assess consequence for their own business, than to assess derived consequences that failure to maintain energy supply may inflict on the surrounding society.