3 Risk Analysis

One standard definition of →*Risk* is that risk is a function of the *likelihood* of a given *threat source* displaying a particular potential *vulnerability*, and the resulting *impact* of that adverse event.[37] *Risk analysis* refers to the processes used to evaluate those probabilities and consequences, and also to the study of how to incorporate the resulting estimates into decision-making processes. As a decision-making tool for the security sector, risk assessment methodologies aim to assure that the priority or appropriateness of measures used to counter specific security threats is adequate for the existing risks.[38] Outcomes of the risk assessment process are used to provide guidance on the areas of highest risk, and to devise policies and plans to ensure that systems are appropriately protected.[39]

What is Risk Analysis?

The modern techniques of the research discipline of risk analysis originate in the engineering professions and may be traced back at least to the beginnings of the US space program. They have been developed most vigorously in the nuclear power industry.[40] However, independent developments have also taken place in various other fields.

In the context of CIP/CIIP, risk analysis could theoretically address any degree of complexity or size of system. However, when the boundaries of the evaluated system are set too wide, the lack of available data makes accurate assessment difficult or even impossible. The three most important single steps of the risk analysis process (namely threat, vulnerability, and impact analysis) are discussed in more detail in separate chapters.

[37] Stoneburner, Gary, Alice Goguen, and Alexis Feringa. *Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology.* NIST Special Publication 800–30 (Washington: U.S. Government Printing Office, January 2002), p. 8. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

[38] Commonwealth of Australia, Information Security Group. *Australian Communications-Electronic Security Instruction 33 (ACSI 33) Handbook 3, Risk Management* (draft version). http://www.dsd.gov.au/_lib/pdf_doc/acsi33/HB3p.pdf. The Australian government is currently developing a new manual: http://www.dsd.gov.au/library/acsi33/acsi33.html.

[39] Commonwealth of Australia, *ACSI 33*, *Handbook 3*, *Risk Management.*

[40] In the nuclear power industry, these techniques are subsumed under the rubric of *Probabilistic Risk Assessment* (PRA).

Risk analysis is an approach that is widely used in different communities. The risk estimate is produced mainly from the combination of threat and vulnerability assessments. It analyzes the probability of destruction or incapacitation resulting from a threat's exploitation of the vulnerabilities in a critical infrastructure. In the least, risk analysis encompasses risk identification, risk quantification, and risk measurement, according to the three classic questions:

a) What can go wrong?
b) What is the likelihood of it going wrong?
c) What consequences would arise?[41]

Often, this is followed by risk evaluation, risk acceptance and avoidance, and risk management, according to the following questions:

a) What can be done?
b) What options are available, and what are their associated trade-offs in terms of cost, benefits, and risks?
c) What impact do current management decisions have on future options?[42]

Even though risk analysis is extremely well established and used in different communities, it has many shortcomings. These include especially the lack of data to support objective probability estimates, persistent value questions, and conflicting interests within complex decision-making processes. There are both theoretical and practical difficulties involved in estimating the probabilities and consequences of high-impact, low-probability events – and this is what we are dealing with in the context of CIIP.

There are many approaches that focus on information security for IT systems. Predominantly, this category covers locally applied measures with a localized focus within a business, agency, or organizational context. These approaches are based on the supposition that sufficient protection at the technical system level nullifies threats to the larger system of CI.

Systems-based approaches often include standard security safeguards, implementation advice, and aids for numerous IT configurations typically found in IT systems today. →*Information Security Guidelines* are suggestions or recommendations on how to address an area of →*Information Security Policy*. Technical protection manuals recommend security measures for selected IT systems.[43] The aim of these recommendations is to achieve a reason-

[41] Haimes, Yacov Y. *Risk Modeling, Assessment, and Management* (New York, 1998).

[42] Ibid., pp. 54–55.

[43] Bundesamt für Sicherheit in der Informationstechnik. *IT Baseline Protection Manual. Standard Security Safeguards* (updated July 2001). http://www.bsi.de/gshb/english/menue.htm.

able security level for IT systems that is adequate to protection requirements ranging from normal to high degrees of protection. Others provide models for the design, the development, or the implementation of secure IT systems, taking into consideration the four →*IT-Security Objectives*.[44] Most of them are business-oriented and centered on organizational information systems, which precludes them from being directly applicable to larger systems.

Steps Included in an IT Risk Analysis

Risk assessment methodologies are step-by-step approaches. The number of steps may vary and can also be adjusted to the specific needs. As mentioned, the classic definition of risk is a function of the *likelihood* of a given *threat source* displaying a particular potential *vulnerability*, and the resulting *impact* of that adverse event.

In order to identify all the elements necessary under this definition, no less than five steps must be undertaken. Figure 13 shows a possible nine-step risk analysis approach for IT systems.[45] It is easy to do a risk analysis for a small, restricted system – but much harder or even impossible for larger, more complex systems such as an entire CI.

The nine steps are described in the following sections.

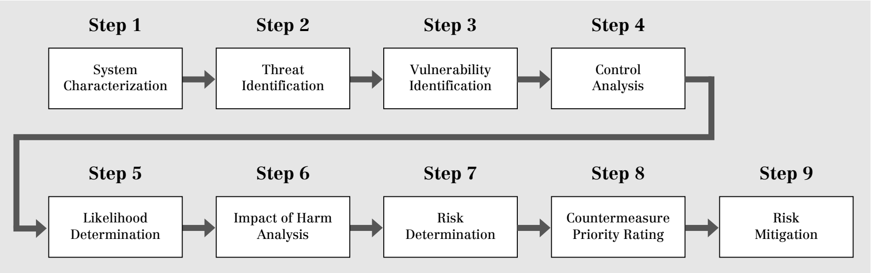

Figure 13: Possible Steps in Risk Assessment Methodology

[44] Stoneburner, Goguen, Feringa, *Risk Management Guide for Information Technology Systems*.

[45] It is a combination of the US approach as described in: Stoneburner, Goguen, Feringa, Risk Management Guide for Information Technology Systems, and the approach favored by Standards Australia / Standards New Zealand. Risk Management AS/NZS 4360:1999 (Strathfield, 12 April 1999).

Step 1: System Characterization

Step 1 is defining the scope of the effort and the boundaries of the system assessed. This includes the identification of all kinds of resources, assets, and information that constitute the system. An "asset" can be a tangible item (such as hardware), a grade or level of service, staff, or information. The strategic, organizational, and risk management context in which the rest of the process will take place are also established in this first step. Furthermore, criteria against which risk will be evaluated should be established, and the structure of the analysis has to be defined.[46]

Step 2: Threat Identification

Step 2 includes the determination of (1) the nature of external and internal threats, (2) their source, and (3) the probability of their occurrence. Threat probability is a measure of the likelihood of the threat being realized. Quantitative information on the nature and source of external threats can be derived from police reports, computer security surveys and bulletins, reports of an audit analysis, or actuarial studies. Information on internal threats can be estimated using previous experience and data, generic statistical information, or a combination of both. However, when dealing with actor-based threats such as terrorism, we are dealing with a "people business" that is intrinsically non-quantifiable and thus poses significant problems for a traditional risk analysis aproach[47] (→see also Chapter 4 on *Threat Assessment*).

Step 3: Vulnerability Identification

Step 3 is about the development of a list of system vulnerabilities that could be exploited by the potential threat-sources. Recommended methods for the identification of system vulnerabilities are the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist. There are several sophisticated approaches to a separate vulnerability assessment process (→see also Chapter 5 on

[46] Emergency Management Australia. *Critical Infrastructure Emergency Risk Management and Assurance Handbook* (Mt. Macedon, 2003). http://www.disaster.qld.gov.au/publications/pdf/Critical_Infrastructure_handbook.pdf.

[47] Zimmermann, Doron. *The Transformation of Terrorism. The "New Terrorism," Impact Scalability and the Dynamic of Reciprocal Threat Perception, Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung no. 67* (Zurich, 2003), p. 61, http://www.isn.ethz.ch/crn/extended/docs/ZB67.pdf and Metzger, Jan. "The Concept of Critical Infrastructure Protection (CIP)". In: Bailes, A. J. K. and Frommelt, I. (eds.), Stockholm International Peace Research Institute (SIPRI), *Business and Security: Public-Private Sector Relationships in a New Security Environment* (Oxford, forthcoming 2004).

Vulnerability Assessment). Again, assessing the vulnerabilities of a relatively restricted IT system such as a business network is far easier than doing the same at a higher system level. It is quite possible that critical vulnerabilities, and even the worst consequences of infrastructure disruptions, will not be traceable in any useful way to single technical subsystems, mainly due to already overwhelming system complexity.

Step 4: Control Analysis

In step 4, an organization would analyze planned or implemented controls, in order to minimize or eliminate the likelihood (or probability) of a threat exploiting any existing system vulnerability. Security controls encompass the use of technical and non-technical methods: Technical controls are safeguards incorporated into computer hardware, software, or firmware. Non-technical controls include management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security.

Step 5: Likelihood Determination

In determining the likelihood of a threat, one must consider threat sources (step 2), potential vulnerabilities (step 3), and existing controls (step 4). The likelihood that a potential vulnerability could be exploited by a given threat source can be described in terms of different →*Categories* (e.g. high, medium, low). Furthermore, there are several techniques to estimate probabilities in risk analysis.[48]

Step 6: Impact or Harm Analysis

In step 6 of the exemplified risk analysis approach, the adverse impact resulting from a successful threat exploitation of a vulnerability is determined. The impact of possible harm to an asset is best determined by a business executive, an asset owner, or an asset manager. The impact strongly reflects the actual value of the asset. The adverse impact of a security event in an IT system can be described in terms of loss or degradation of any, or a combination of, the →*IT-Security Objectives* (other categories might be applied if risk analysis is conducted for more abstract systems). Some tangible impacts can be measured in a quantitative manner in terms of lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused

[48] Such as statistical inference, scenario technique, fault trees, and event trees; see also Stromquist, Walter R. *Uses and Limitations of Risk Analysis*. Prepared for the Royal Commission on the Ocean Ranger Marine Disaster Risk Analysis Seminar, 1 May 1984. http://www.chesco.com/~marys/ORanger.htm.

by a successful threat action. Other impacts (e.g., loss of public confidence, loss of credibility, damage to an organization's interest) cannot be measured in specific units, but can at least be qualified or described in terms of high, medium, and low impacts (→see also Chapter 6 on *Impact Assessment*).

Step 7: Risk Determination

The purpose of step 7 is to assess the level of risk to the (IT) system. The determination of risk can be expressed as a function of the likelihood that a given threat source will attempt to exploit a given vulnerability (step 5) and the magnitude of the impact, should a threat source successfully exploit the vulnerability (step 6). A →*Risk Scale* and a →*Risk Level Matrix* are appropriate tools for measuring the resultant risk.

Step 8: Countermeasure Priority Rating

The countermeasure rating expresses the difference between the required risk (desired "risk level" as set by the management authority of the system) and the resultant risk (step 7). It is used to provide guidance as to the importance that should be placed on security countermeasures. Again, applied values and categories may vary widely. Table 3 is an example of a *Risk Assessment Table*, which helps to calculate the level of the Countermeasure Priority Rating (column 7). Column 7 is simply the difference between the resultant risk and the required risk (Columns 6 and 5 in the example) expressed as a figure.

Column 1 **Asset Identification**	**C 2** **Threat to the Asset**	**C 3** **Threat Likelihood**	**C 4** **Harm**	**C 5** **Resultant Risk**	**C 6** **Required Risk**	**C 7**
Row 1: Reliability of e-commerce-related web-site	Accidental electrical power or equipment failure	Medium	Grave	Critical	Nil	4
Row 2: Accuracy of publicly available web information	Loss of confidence or goodwill due to "hacking" of web page	High	Minor	Medium	Low	1
Row 3: Secure access to internal network services by authorized staff, from external networks	Loss of crypto token or keys required to access the secure channel(s)	Very Low	Serious	Medium	Low	1

Table 3: Risk Assessment Table[49]

[49] Commonwealth of Australia, *ACSI 33. Handbook 3*, *Risk Management*. Appendix, http://www.dsd.gov.au/_lib/pdf_doc/acsi33/HB3Ap.pdf.

Step 9: Risk Mitigation

Step 9 is about risk mitigation and involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls suggested by the risk assessment process. Because the elimination of all risk is usually impractical or near impossible in reality, it is the stakeholders itself that must use the *least-cost approach* and implement the *most appropriate controls* to decrease mission risk to an acceptable level.[50]

Control actions occur frequently in IT systems. Different kinds of security controls can be applied at the technical, management, and operational levels, or a combination of such controls, with the goal of maximizing the effectiveness of controls for IT systems and organizations.

- *Technical security controls* for risk mitigation can be configured to protect against given types of threats. These security controls may range from simple to complex measures. They usually involve system architectures; engineering disciplines; and security packages with a mix of hardware, software, and firmware. Technical security controls can be grouped into three categories, according to primary purpose: supporting, preventing, and detecting and recovering.
- *Management security controls*, in conjunction with technical and operational controls, are implemented to manage and reduce the risk of loss and to protect an organization's mission. Management controls focus on the stipulation of information protection policy, guidelines, and standards.
- *Operational controls*, implemented in accordance with a base set of requirements (e.g., technical controls) and good industry practices, are used to correct operational deficiencies that could be exploited by potential threat sources.

Examples of Risk Analysis Processes for CI/CII

Below, the following eight examples are described:

- Example 1 (Australia and New Zealand) – Risk Management Standard (NSW)
- Example 2 (Canada) – Infrastructure Protection Process by the Critical Infrastructure Protection Task Force (CIPTF)
- Example 3 (European Union) – The CORAS Project (CORAS)
- Example 4 (France) – EBIOS Method (EBIOS)

[50] Stoneburner, Goguen, Feringa. *Risk Management Guide for Information Technology Systems.*

- Example 5 (Norway) – Protection of Society Project (BAS)
- Example 6 (Switzerland) – Swiss Roundtables Risk Analysis Methodology (Roundtables)
- Example 7 (United Kingdom) – NISCC Building Blocks (NISCC)
- Example 8 (United States) – OCTAVE Methodology (OCTAVE)

Example 1 (Australia and New Zealand) – Risk Management Standard (NSW)

The *Australian and New Zealand Standard for Risk Management* (AS/NZS 4360:1999) is the standard by which all critical infrastructures are assessed to assist with the review of risk management plans for prevention (including security), preparedness, response, and recovery.[51] The AS/NZS 4360:1999 standard provides a generic guide for the establishment and implementation of the risk management process involving identification, analysis, evaluation, treatment, and ongoing monitoring of risks. In accordance with AS/NZS 4360, it is necessary to establish the strategic context. In the current security environment, security risk assessments should also consider terrorism in all its forms.[52]

The Australian *Defense Signal Directorate* (DSD) has also released a new version of the *ACSI33 Government IT Security Manual* in an attempt to consolidate and restructure a number of existing Australian IT security policy documents into a single, cohesive manual.[53] The *New South Wales Office of Information and Communications Technology*'s (OICT) website additionally features a long list of guidelines for information management and information security:[54] The *Information Security Guidelines Part 1* is concerned with risk management.[55] Its objective is to assist government agencies in the identification and management of information security risks.

[51] Yates, Athol. *Engineering a Safer Australia: Securing Critical Infrastructure and the Built Environment* (Institution of Engineers, Australia, June 2003). http://www.ieaust.org.au/SafeAustralia/Engineering%20a%20Safer%20Aust.pdf.

[52] Ibid., pp. 10, 27, 30, 65.

[53] Draft ACSI 33 Information, Government IT Security Manual. http://www.dsd.gov.au/library/acsi33/acsi33_draft_information.html.

[54] http://www.oit.nsw.gov.au/pages/4.3.Guidelines.htm.

[55] New South Wales Office of Information and Communications Technology's (OICT). *Information Security Guideline for NSW Government Part 1 – Information Security Risk Management*. No. 3.2, first published in September 1997, current version: June 2003. http://www.oit.nsw.gov.au/pages/4.3.16-Security-Pt1.htm.

Its components are: assets, asset values, threats, vulnerabilities, security risk, security requirements, and security controls (Figure 14).

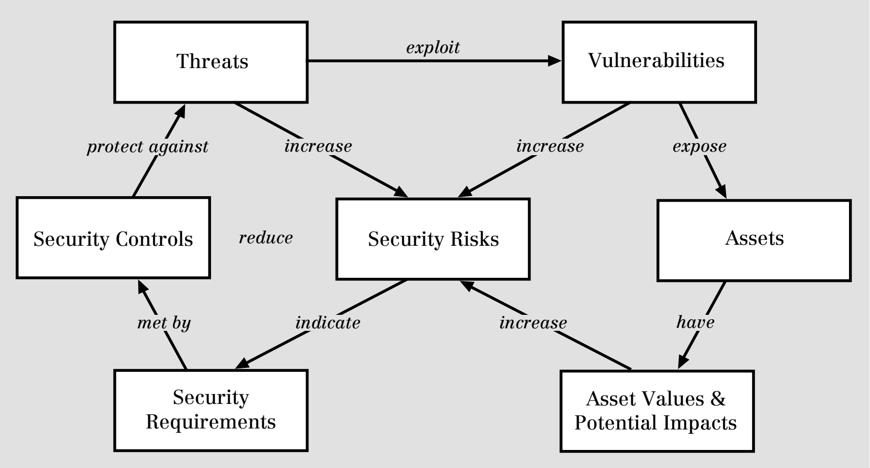

Figure 14: Risk Concept Relationship

This guideline is based on the *Australian/New Zealand Handbook on Information Security Risk Management* (HB 231:2000). It should also be read in conjunction with the *Information Security Guidelines Part 2 – Examples of Threats and Vulnerabilities*[56] and the *Information Security Guidelines Part 3 – Information Security Baseline Controls*.[57]

[56] New South Wales Office of Information and Communications Technology (OICT). *Information Security Guideline for NSW Government Part 2 – Examples of Threats and Vulnerabilities*. No. 2.0., first published in September 1997, current version: June 2003. http://www.oit.nsw.gov.au/pages/4.3.17-Security-Pt2.htm.

[57] New South Wales Office of Information and Communications Technology (OICT). *Information Security Guideline for NSW Government Part 3 – Information Security Baseline Controls*. No. 3.0, first published in September 1997, current version: June 2003. http://www.oit.nsw.gov.au/pages/4.3.18-Security-Pt3.htm.

Example 2 (Canada) – Infrastructure Protection Process by the Critical Infrastructure Protection Task Force (CIPTF)

♦ The CIPTF approach also appears in *Chapter 1: Sector Analysis*, and in *Chapter 2: Interdependency Analysis*.

In the spring of 2000, the *Critical Infrastructure Protection Task Force* (CIPTF) was established within the *Canadian Department of National Defence*. The CIPTF developed an extensive review process for critical infrastructures in Canada. One of the goals was to better understand risks (Figure 15).[58]

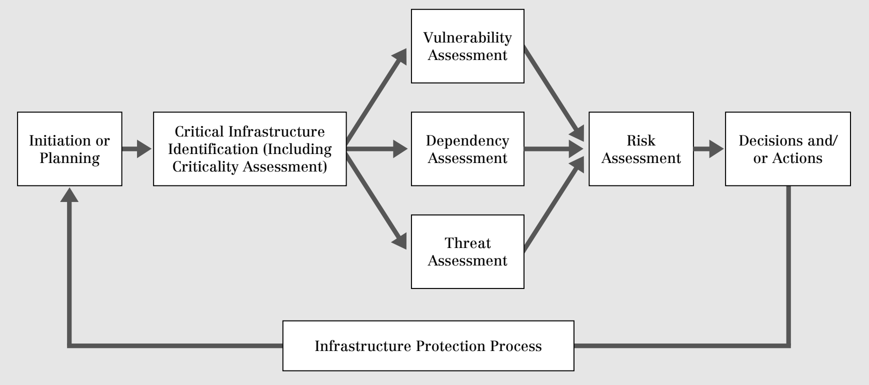
Initiation or Planning
Critical Infrastructure Identification (Including Criticality Assessment)
Vulnerability Assessment
Dependency Assessment
Threat Assessment
Risk Assessment
Decisions and/ or Actions
Infrastructure Protection Process

Figure 15: Canadian Infrastructure Protection Process

Risks were determined by using a →*Risk Rating Matrix* that multiplies threat values with vulnerability values. This method allows for a comparison of relative risks between components of an infrastructure element, between layers in the infrastructure model, and between infrastructure elements, which are called specific risks.

It was taken into account that risks accumulate when the risks of dependencies are propagated (→*Cascading Effect*). Therefore, the Canadian process conducts a →*Cumulative Risk Assessment* through dependencies. The assessment of impacts can be done with a →*Risk/Impact Scattergram*.[59]

[58] Grenier, Jacques. "The Challenge of CIP Interdependencies". *Conference on the Future of European Crisis Management* (Uppsala, 19–21 March 2001). http://www.ntia.doc.gov/osmhome/cip/workshop/ciptf_files/frame.htm.

[59] Grenier, The Challenge of CIP Interdependencies, slide 25.

Example 3 (European Union) – The CORAS Project (CORAS)

The EU-funded *CORAS*[60] project (IST-2000-25031) developed a tool-supported methodology for model-based risk analysis of security-critical systems. The project was initiated in January 2001 and completed in September 2003. The CORAS framework consists of terminology, languages for system modeling, processes for system development and risk management, and methodologies for security risk analysis as well as computerized tools.

The CORAS methodology for model-based risk assessment (MBRA) applies a standardized modeling technique to form input models to risk analysis methods that are used in a risk management process. This process is based on the *AS/NZS 4360:1999 Risk Management* standard.

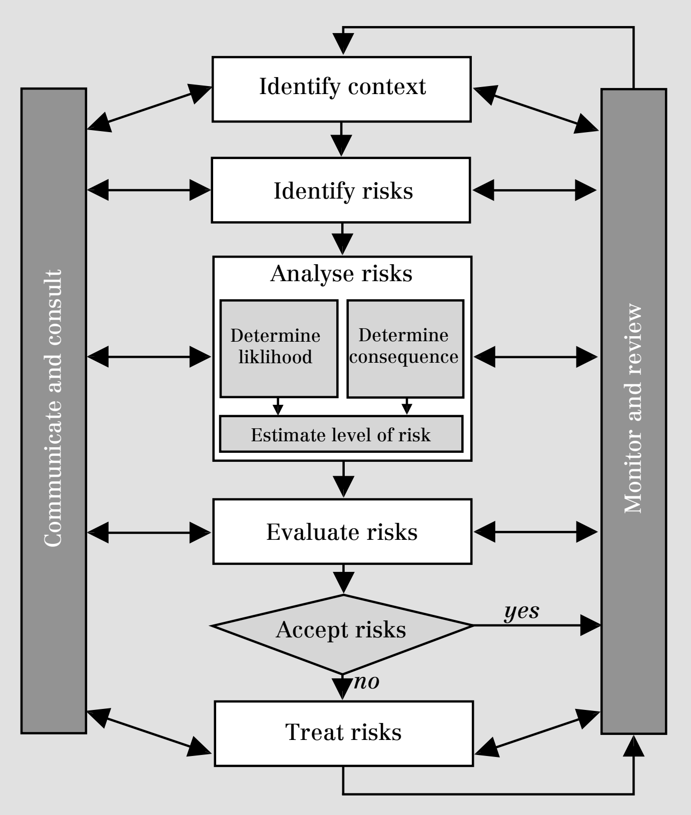

Figure 16: The CORAS Risk Management Proces

[60] http://coras.sourceforge.net/

Figure 16 indicates that the AS/NZS 4360 standard provides a sequencing of the risk management process into sub-processes for context identification, risk identification, risk assessment, risk evaluation, and risk treatment. In addition, there are two implicit sub-processes targeting "communication and consultation" as well as "monitoring and review" running in parallel with the first five steps.[61]

Example 4 (France) – EBIOS Method (EBIOS)

The methodological approach EBIOS (*l'Expression des Besoins et l'Identification des Objectifs de Sécurité*) belongs to a group of methodological guides published by the *Service Central de la Sécurité des Systèmes d'Information* (SCSSI). This methodology is used in the information system-planning phase. The main goal is to allow any organization – especially the state administration – to define necessary security actions.

In addition, several other methodologies are used for design, development, and implementation, as well as the operation and maintenance of information systems (see Figure 17). The outcome of an EBIOS study provides information needed to establish the security objectives for the system and is generally useful in developing the secured functional architecture:

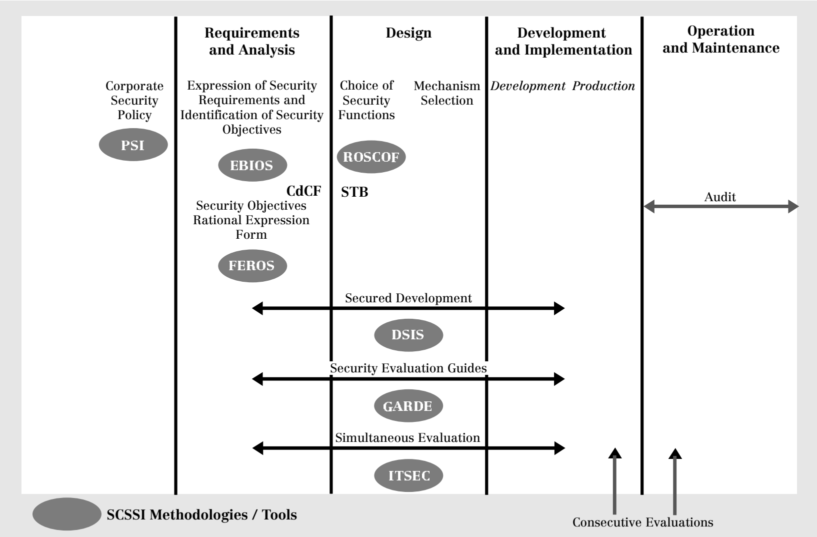
Requirements and Analysis
Design
Development and Implementation
Operation and Maintenance
Corporate Security Policy
PSI
Expression of Security Requirements and Identification of Security Objectives
EBIOS
CdCF
Security Objectives Rational Expression Form
FEROS
Choice of Security Functions
Mechanism Selection
ROSCOF
STB
Development
Production
Audit
Secured Development
DSIS
Security Evaluation Guides
GARDE
Simultaneous Evaluation
ITSEC
SCSSI Methodologies / Tools
Consecutive Evaluations

Figure 17: Security Activities during the system development life cycle (SDLC).

[61] Gran, Bjørn Axel. *The CORAS Methodology for Model-Based Risk Assessment*, version 1.0, WP2, Deliverable 2.4. (29 August 2003).

The EBIOS method takes into account all technical (software, hardware, networks) and non-technical entities (organization, human aspects, physical security). It also involves all players concerned with information systems security problems. It further proposes a dynamic procedure favoring interactions between different businesses and departments of the organization. With the help of the EBIOS method, the entire life cycle of a system can be studied (design, production, implementation, maintenance, etc.).[62]

There are four principles of the EBIOS method (Figure 18):

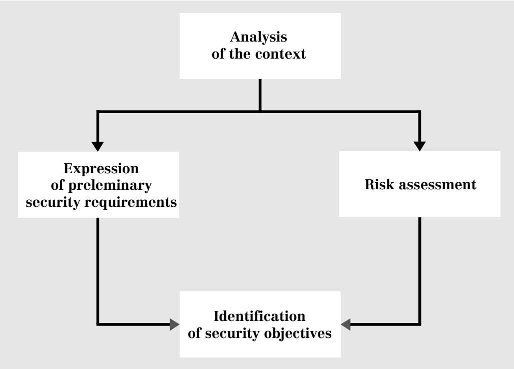
Analysis of the context
Expression of preleminary security requirements
Risk assessment
Identification of security objectives

Figure 18: EBIOS Method Diagram

1) *The context study*: An information system is based on elements, functions, and information, which make up the added value of the information system for the organization. These elements are related to a set of different types of entities: hardware, software, networks, organizations, personnel, and sites.
2) *The expression of security needs*: Each element has a specific security need if the business is to operate correctly. This security need is expressed according to different security criteria such as availability, integrity, and confidentiality. If this need is not met, there will be an impact on the organization. This impact may come in different forms such as financial losses, disruptions of the smooth progress of activities, damage to the brand image, influence on personnel safety, pollution, failure to comply with laws and regulations, etc.
3) *The threat study*: In general, an organization is exposed to various potential threats from its environment. A threat may be characterized according to its type (natural, human or environmental), its cause (accidental or deliberate), and its influence on security criteria (availability, integrity, confidentiality, etc.). For an accidental cause, a certain kind of threat can also be described in terms of

[62] Methods to Achieve Information Systems Security. Expression of Needs and Identification of Security Objectives (EBIOS). Memo – Version 1.4. http://www.ssi.gouv.fr/en/confidence/documents/memo-gb.html.

its exposure and the available resources. For a deliberate cause, a threat can also be characterized by expertise, available resources, and motivation.

4) *Expression of security objectives*: All that remains is to determine how elements can be affected by threats.[63]

Example 5 (Norway) – The Protection of Society Project (BAS)

"Protection of Society" (BAS) is a joint project between the *Directorate for Civil Defense and Emergency Planning* (DSB) and the *Norwegian Defense Research Establishment* (FFI). The project uses a methodology for cost-benefit/cost-effectiveness analysis to design and evaluate civil emergency measures. The same methodology was applied in the project "Protection of Society 2" (BAS2).[64] The purpose of the BAS2 project was to study vulnerabilities in the telecommunication system and to suggest cost-effective measures to reduce these vulnerabilities. The analysis was conducted in four interlinked steps (Figure 19):

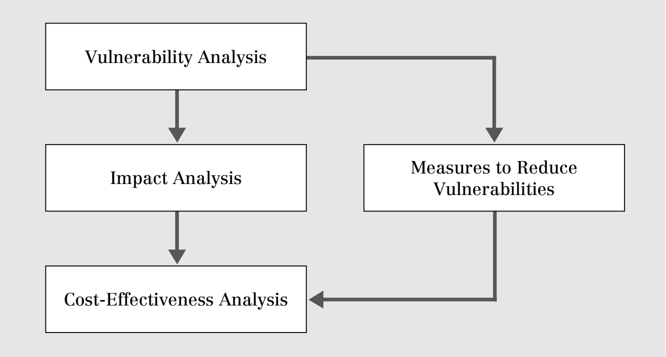
Vulnerability Analysis
Impact Analysis
Measures to Reduce Vulnerabilities
Cost-Effectiveness Analysis

Figure 19: Steps of the Norwegian Vulnerability Analysis

[63] EBIOS website: http://www.ssi.gouv.fr/en/confidence/methods.html. Premier Ministre, Service Central de la Sécurité des Systèmes d'Information. *Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS)*. Technical guide – English version, Version 1.02., February 1997.

[64] Hagen, Janne Merete, and Håvard Fridheim. *Cost-Effectiveness Analysis of Measures to Reduce Vulnerabilities in the Public Telecommunication System.* Paper presented at the 16th ISMOR, The Royal Military College of Science, Norwegian Defense Research Establishment (Swindon, 1–3 September 1999). http://www.isn.ethz.ch/crn/extended/workshop_zh/Norway_Tel.pdf.

In a first step, a →*Vulnerability Analysis* was conducted. By using →*Seminar Games*, BAS2 mapped the dependency of modern society upon telecommunication services in crisis and conflict situations. After this, an impact analysis was conducted. In a next step, measures that might reduce the vulnerabilities were evaluated. Eventually, the actual cost-effectiveness analysis was undertaken.

Because no single method was able to handle all the problems, BAS2 had to use a combination of several techniques and methods to calculate the most cost-effective protection strategy for the telecommunication system. The additional approaches used were seminar games; use of →*Scenarios*, →*Causal Mapping*, →*Fault Tree Analysis*, Probabilistic Cost Estimation, and a →*Multi-Criteria Model*. The →*Multi-Criteria Decision Approach* systematically maps out subjective expert evaluations and combines them into a quantitative measure of effectiveness.

The →*Multi-Criteria Decision Approach* involves structuring the problem in a multi-criteria hierarchy, where measures are linked to a top-level goal through several levels of decision criteria. The top-level goal is the overall objective of the system of analysis. In this process, the complex dynamic system to be analyzed is represented by a simplified linear, easily understandable model. Lower-level technical criteria are aggregated to wider, more general criteria in a rigid linear model. The relationships between criteria at different levels can be quantified by experts expressing their subjective preferences of criteria, i.e. identifying the criteria they consider to be important for the success of the criterion on the level above. In other words, the experts *weigh* the different criteria in the model against each other, and the experts' preferences serve as a measure of the *effectiveness* of one criterion compared to the others on the same level. The top goal of the hierarchy expresses the total effectiveness of the measures involved.

The multi-criteria model used in BAS2 is a hierarchy with two interlinked parts. The top part of the hierarchy describes the "societal sub-system" of the analysis, while the lower part of the hierarchy describes the "technical sub-system". The two sub-systems are connected, so that the top criteria in the technical sub-system are identical to the bottom criteria in the societal sub-system (Figure 20).

Maximizing the protection of society was defined as the top goal. The top goal was further distilled into three sub-criteria, which were: minimizing loss of life, minimizing economic losses, and minimizing the danger of a loss of sovereignty. These three sub-criteria were divided into more specialized sub-criteria (Figure 21).

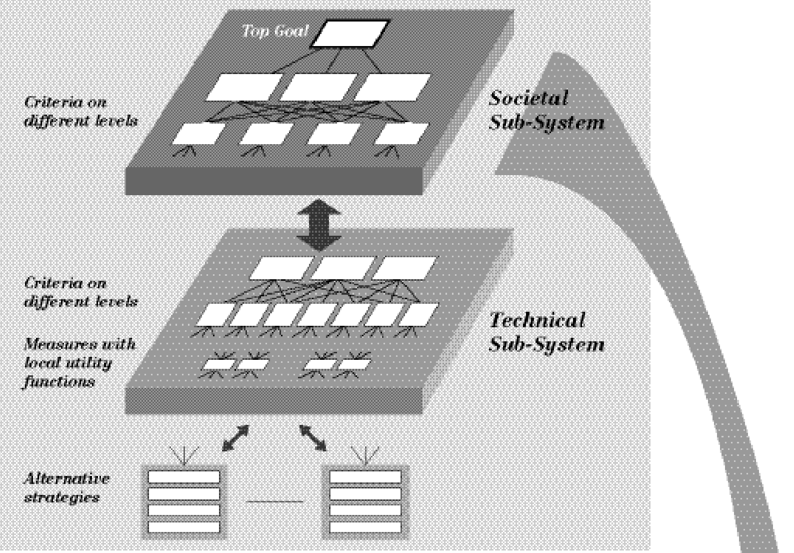
Top Goal
Criteria on different levels
Societal Sub-System
Criteria on different levels
Technical Sub-System
Measures with local utility functions
Alternative strategies

Figure 20: Multi-Criteria Hierarchy

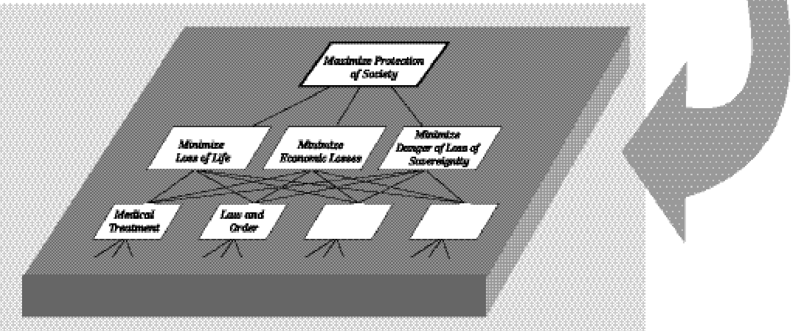

Figure 21: Parts of the Social Hierarchy for the Multi-Criteria Analysis

Creating a →*Multi-Criteria Model* is an iterative process. One of the main problems in the design process was to determine, to the greatest extent possible, exclusive criteria that were independent of the other criteria on the same level in the hierarchy. Still, the design process was extremely useful for establishing a thorough understanding of the problems that were analyzed.[65]

[65] Hagen, J. and H. Fridheim. *Cost-Effectiveness Analysis of Measures to Reduce Vulnerabilities in the Public Telecommunication System*, p. 13.

Example 6 (Switzerland) – Swiss Roundtables Risk Analysis Methodology (Roundtables)

♦ The Sector Roundtable approach also appears in *Chapter 1: Sector Analysis*

Under the auspices of the *Swiss InfoSurance Foundation*, sector specific risk analysis round tables are conducted for ten sectors identified as critical. The methodology used for each of the sectors is a ten-step risk analysis approach as shown in Figure 22:

Four →*Roundtables* that can be amended by working groups are planned for each sector. The processes can be divided into a system analysis and a risk analysis:

- The system analysis aims to gain an overview over structures, elements, and the dependencies in the respective sector (Steps 1–6).
- The risk analysis uses scenarios for identified weak points and focuses on them (Steps 7–10).[66]

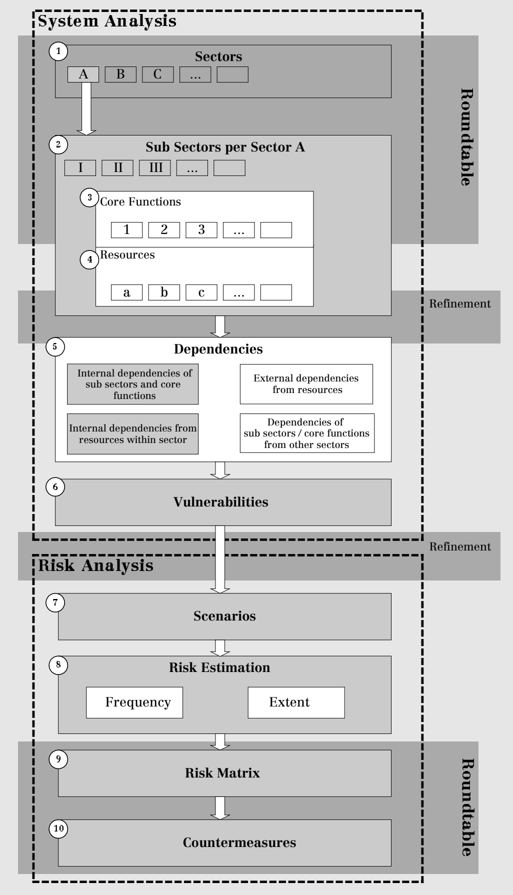

Figure 22: Swiss Critical Sector Risk Analysis Approach

[66] InfoSurance, Wirtschaftliche Landesversorgung, Informatikstrategieorgan Bund. *Sektorspezifische Risikoanalysen: Methodischer Leitfaden* (no date, no place).

Example 7 (United Kingdom) – NISCC Building Blocks (NISCC)

The UK government's CIIP center, the NISCC (*National Infrastructure Security Coordination Centre*), has developed a set of "building blocks" in order to provide protective security advice efficiently. It is an ongoing process already initiated in the UK. The building blocks are described by asking a series of key questions:

- What is critical to the UK?
- Are some sectors more critical than others?
- What would be the impact of disruption?
- What is potentially vulnerable to electronic attack?

Answers to these questions help to generate a prioritized set of services or mechanisms for the supply of goods, services or resources that are critical to the well-being of the UK and are potentially vulnerable to electronic attack. Subsequently, the following questions are asked:

- Which organizations are responsible for providing these services?
- What proportion of the service is each organization responsible for?

This generates a prioritized set of private companies, government departments, agencies, and other organizations that may be considered as part of the critical infrastructure. These organizations, agencies, and companies are asked to participate in a confidential dialog. In the context of the dialog, the following questions are asked:

- What systems, networks, components, and assets are critical for the continued provision of a critical service by each organization?
- What other services and systems do they depend on?
- Are these systems vulnerable to electronic attack?
- What would be the impact of a successful electronic attack?
- What procedural and technical measures has the organization prepared to protect its systems?

The information gained from these questions gives the NISCC a detailed insight into the protective measures and consequences of failure of these organizations and companies. In order to provide the interview partners with advice, recommendations, and information sharing opportunities, the NISCC assesses the following three points:

- What is the threat?
- How can the respective company improve its resilience?
- How can the sector improve its resilience?

Answers to these building block questions generate a 'map' of CII (networks and services), key organizations, and interdependencies. The information allows the NISCC to give the organizations feedback, including a set of recommendations to improve safety and security; vulnerability analyses on components or networks used by the organization; and a threat assessment based on intelligence and investigatory findings. These inputs allow the organization to manage more effectively their risk management for electronic attack protection.[67]

Example 8 (United States) – OCTAVE Methodology (OCTAVE)

OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*)[68] is an approach to self-directed information security risk evaluations, developed by the US CERT Coordination Center at the Carnegie Mellon Software Engineering Institute[69]. The OCTAVE Method is documented in the 18-volume *OCTAVE Method Implementation Guide* (OMIG).[70] The OCTAVE Method is based on a set of criteria that define the essential elements of an asset-driven, comprehensive, self-directed security risk evaluation for organizations. Since OCTAVE was designed for a target audience of larger organizations, a version called OCTAVE-S has been developed recently for small organizations.[71]

The OCTAVE Method uses a three-phase approach to examine organizational and technology issues, assembling a comprehensive picture of the organization's information security needs (see Figure 23). The method consists of workshops that encourage open discussion and the exchange of information about assets, security practices, and strategies. Each of the three phases consists of several processes. Furthermore, one or more workshops are planned for each process. The three phases of the OCTAVE Method are briefly outlined below.

[67] Barry, Ted. "Critical Information Infrastructure Protection in the United Kingdom". Paper presented at the Critical Infrastructure Protection (CIP) Workshop (Frankfurt a.M., 29–30 September 2003).

[68] http://www.cert.org/octave/.

[69] http://www.cert.org.

[70] Alberts, Christopher and Audrey Dorofee. *OCTAVE Method Implementation Guide*, version 2.0, vols. 1–18 (Carnegie Mellon University, June 2001). http://www.cert.org/octave/pubs.html. See also: Alberts, Christopher and Audrey Dorofee. *An Introduction to the OCTAVE Method.* http://www.cert.org/octave/methodintro.html.

[71] Alberts, Christopher, Audrey Dorofee, James Stevens, and Carol Woody. *Introduction to the OCTAVE Approach* (Carnegie Mellon University, August 2003). http://www.cert.org/octave/approach_intro.pdf.

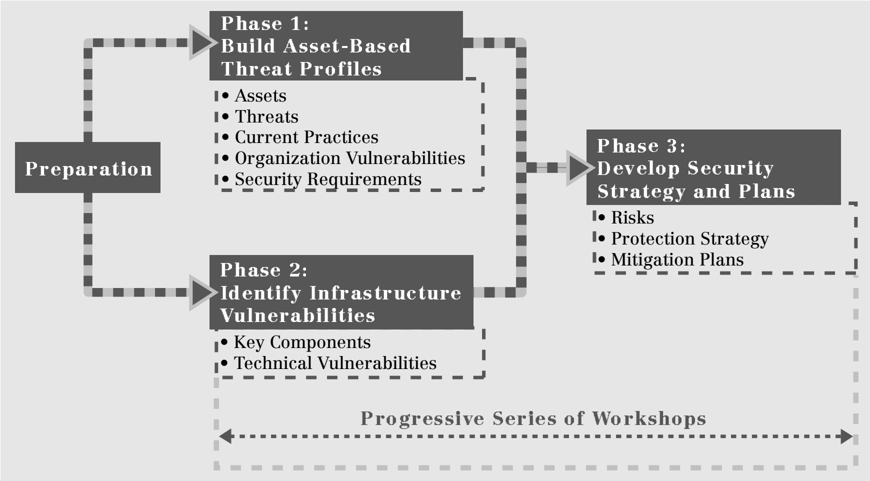
Phase 1:
Build Asset-Based Threat Profiles
• Assets
• Threats
• Current Practices
• Organization Vulnerabilities
• Security Requirements
Preparation
Phase 2:
Identify Infrastructure Vulnerabilities
• Key Components
• Technical Vulnerabilities
Phase 3:
Develop Security Strategy and Plans
• Risks
• Protection Strategy
• Mitigation Plans
Progressive Series of Workshops

Figure 23: Three Steps of the OCTAVE Method

- *Phase 1: Build Asset-Based Threat Profiles*: This is an organizational evaluation. The analysis team determines which assets are most important to the organization (critical assets). The team identifies currently required actions to protect the determined assets;
- *Phase 2: Identify Infrastructure Vulnerabilities:* This is an evaluation of the information infrastructure. The analysis team examines key operational components in terms of weaknesses (technology vulnerabilities) that could lead to unauthorized actions against critical assets;
- *Phase 3: Develop Security Strategy and Plans:* During this phase of the evaluation, the analysis team identifies risks to the organization's critical assets. The team eventually decides on measures for managing the identified risks.