National Efforts for CII Analysis

Introduction

This chapter introduces country-specific efforts to analyze and evaluate various aspects of CII. This not only serves as a country guide but also provides examples for various methodological elements mentioned throughout the book.

Table 2 shows specific approaches developed in the surveyed countries and the examples they provide for methodological elements.

Country	Approach	Examples for
Australia	• PreDICT (Predict Defence Infrastructure Core Requirements Tool)	• Interdependency/Vulnerability Matrix • Sector Analysis • Vulnerability Assessment Process • Vulnerability Profile Chart • Vulnerability Rating Table
Canada	• National Contingency Planning Group Model • Infrastructure Protection Process	• Dependency/Interdependency Matrix • Infrastructure Profiles • Layer Model • Risk Rating Matrix • Risk/Impact Scattergram
The Netherlands	• BITBREUK Model • KWINT Report Model	• Layer Model • Sector Analysis • Vulnerability Analysis
Norway	• Multi-Criteria Model of the "Protection of Society" Projects (BAS)	• Multi-Criteria Decision Approach • Vulnerability Analysis
Switzerland	• InfoSurance Sector Model and CIIP Framework	• Process and Technology Analysis • Sector Model
United States	• Department of Energy (DoE) Layer Model • CIAO Vulnerability Assessment Process/ Project Matrix	• Layer Model • Vulnerability Assessment Process

Table 2: Outline of Approaches Used in Surveyed Countries

Australia

A number of studies have been conducted in Australia on threats to, and vulnerabilities of, CII. Among the official methodologies in use is the risk assessment methodology as introduced in the *Australian Communications-Electronic Security Instruction – Protective Security Manual (PSM)*.[1] Another important publication suggests a hierarchy of threats facing Australia's CI in descending order of probability of serious damage.[2] An official governmental assessment of 1998 (*Protecting Australia's National Information Infrastructure*) also suggests measures to protect Australia's information infrastructures.[3] The most comprehensive report to date, however, is an effort by the Australian National Support Staff and KPMG to study Australia's most important infrastructure sectors, with special relevance to defense. The methodology employed is presented in more detail below.

Predict Defence Infrastructure Core Requirements Tool (PreDICT)

In 1998, government officials decided to analyze the Australian national defense-related infrastructure in order to develop strategies to remove, ameliorate, or avoid identified vulnerabilities. A multi-step →*Vulnerability Assessment* Process was developed for the project.[4] In a first phase, the study identified vulnerabilities in fifteen infrastructure sectors and highlighted their interdependence. A second phase of the project identified preliminary strategies aimed at removing the vulnerabilities, with a special focus on defense needs.

1 Commonwealth of Australia, Information Security Group. *Australian Communications-Electronic Security Instruction 33 (ACSI 33)*. http://www.dsd.gov.au/infosec/acsi33/HB3.html.

2 Cobb, Adam. *Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks*. Foreign Affairs, Defence and Trade Group, Research Paper 18. (29 June 1998).

3 Attorney-General's Department. *Protecting Australia's National Information Infrastructure. Report of the Interdepartmental Committee on Protection of the National Information Infrastructure*. (Canberra, December 1998). http://www.law.gov.au/publications/niireport/niirpt.pdf, 13.

4 See KPMG / National Support Staff. Predict Defence Infrastructure Core Requirements Tool (PreDICT). http://www.defence.gov.au/predict/general/predict_fs.htm.

One key output of the process was the web-based decision support tool entitled *PreDICT (Predict Defence Infrastructure Core Requirements Tool*), which presents the data gathered during the project, and makes it available to defense planners and other interested parties. PreDICT is a tool that records the background, vulnerability, and interdependencies of ten national critical infrastructure sectors of relevance to defense.[5]

Methodology: Interdependency and Vulnerabilities Charts

Sector interdependencies in all sectors were discussed and rated by experts (both industry and defense representatives). The interdependencies were charted over the three time periods of 1999, 2005, and 2020, with additional summary pages detailing the nature of the interdependency and reasoning behind each rating (Figure 1 is an example of an interdependency chart).

Next, industry vulnerability profiles for each of the ten sectors were developed, based on industry analysis and interviews, with a focus on the critical interdependencies that exist between them. The vulnerabili-

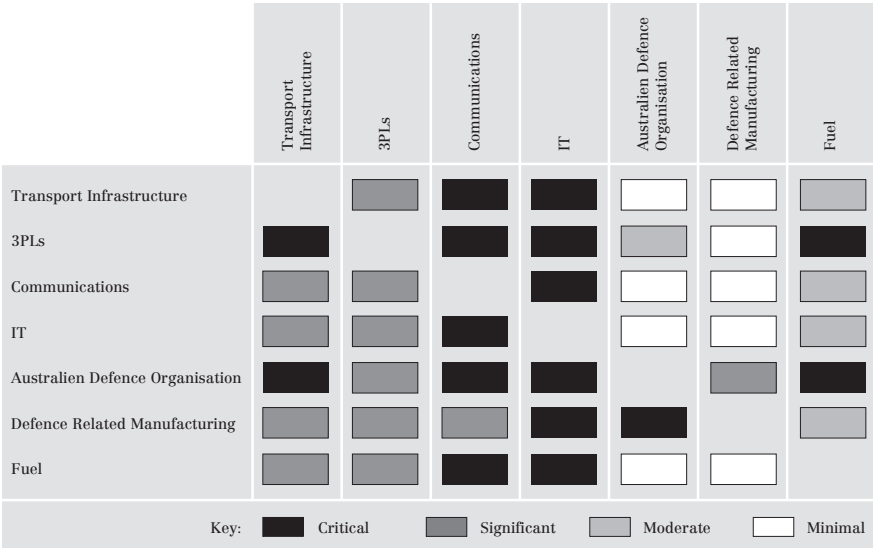

Figure 1: Interdependency Chart (Source: PreDICT)

5 The ten sectors are Transport, Fuel, IT, Utilities, Health, 3PL Providers, Education and Training, Communications, Defense-Related Manufacturing, and Financial Services.

ties were grouped into twelve "Broad Risk Areas" in order to compare and contrast vulnerabilities between industry sectors and defense and to group the vulnerabilities identified into common areas for analysis. The majority of the Broad Risk Area titles were drawn from →*Sector Analysis* (PEST, Porter's analysis, and SWOT analysis).[6]

The magnitude of each vulnerability was rated first by quantifying its consequence by degree (→*Categories*: "insignificant", "minor", "moderate", "major", "catastrophic"), and then by determining the likelihood of its occurrence. The vulnerability rankings for each Broad Risk Area were calculated using a →*Vulnerability Rating Table* and were visually represented on a →*Vulnerability Profile Chart*. (Figure 2)

Vulnerabilities with the highest rating by sector using this method were prioritized for the development of mitigation strategies.[7]

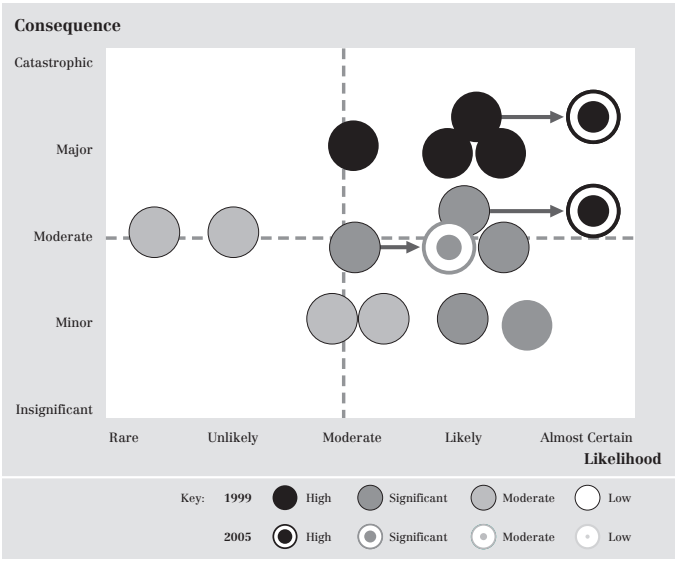

Figure 2: Vulnerability Profile for the Technology Sector (Source: PreDICT)

6 The twelve "Broad Risk Areas" are: Political, Economic, Social/Environmental/Cultural, Technological, Supplier, Customer, Substitutes, Competitor, Barriers to Entry, Operations – HR, Operations – Training, and Flexibility/Adaptability.

7 KPMG / National Support Staff. Predict Defence Infrastructure Core Requirements Tool: Methodology. http://www.defence.gov.au/predict/general/methodology_fs.htm.

Canada

In Canada, the key efforts to analyze the nation's CII are: The National Contingency Planning Group's (NCPG) assembly of an overall picture of infrastructure elements, which resulted in the book "*Canadian Infrastructures and their Dependencies*", and the comprehensive *Infrastructure Protection Process*, with a strong focus on interdependencies, developed by the Critical Infrastructure Protection Task Force (CIPTF).

The National Contingency Planning Group (NCPG) Model

When the National Contingency Planning Group (NCPG) was formed in October 1998, part of its mandate was the production of a National Infrastructure Risk Assessment (NIRA). The NIRA's objective was to better position the country for the transition to the year 2000 by finding out which infrastructures were most at risk. It set out to examine important Canadian infrastructure elements, determine their criticality, and assess the probability of their failure.[8] To determine the criticality, two criteria were used:

- The possible impact on four tenets (direct impact on individual Canadians);
  - No loss of life,
  - Basic community needs are met,
  - Business continues as usual,
  - Confidence in government is maintained.
- The degree of dependency (direct impact on Canadian government, industry, and business).[9]

Thirty-six infrastructure elements were agreed upon, ranging from physical systems (such as electricity, telecommunications, or airports) to services (such as health or finances). An expert panel was assembled

8 Charters, David. *The Future of Canada's Security and Defence Policy: Critical Infrastructure Protection and DND Policy and Strategy.* Research Paper of the Council for Canadian Security in the 21st Century. http://www.ccs21.org/ccspapers/papers/charters-CSDP.htm.

9 National Contingency Planning Group. *Canadian Infrastructures and their Dependencies.* (March 2000), preface.

to rank the criticality of the infrastructure elements against each of the criteria.[10]

A group formed under the auspices of the NCPG, called the Infrastructure Analysis Group (IAG),[11] subsequently produced a number of →*Infrastructure Profiles (IPs)*. Fifteen are collected in a compendium entitled "Canadian Infrastructure and Their Dependencies". The profiles include a description of the infrastructure, statistics, maps, contacts, references, and jurisdictions, as well as a detailed analysis of the interdependencies.

Infrastructure Protection Process

In spring 2000, the NCPG was converted into the Critical Infrastructure Protection Task Force (CIPTF). The Task Force, which was established within the Department of National Defence, developed an extensive process to review critical infrastructures in Canada (Figure 3).

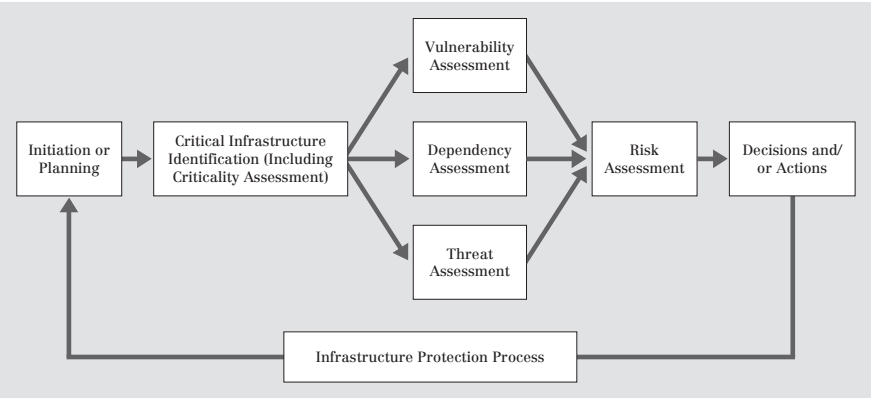

Figure 3: Canadian Infrastructure Protection Process (Source: Presentation by J. Grenier)

10 National Contingency Planning Group. Canadian Infrastructures and their Dependencies.

11 The IAG's mandate was to predict potential impacts on the Canadian infrastructure and critical government functions resulting from any year 2000 failures.

One of the main aims of this process was to understand and picture interdependencies.[12] Important steps within this approach are discussed below.

Canadian Layer Model

Based on six sectors identified as crucial,[13] the CIPTF developed a multi-dimensional →*Layer Model* that takes into consideration the responsibilities of five sectors: the international, federal, provincial, municipal, and the private level. Each of these areas of responsibility consists of three vertical sector-specific layers (operations layer, technical application layer, and control layer), which in turn rest on two "Common foundation layers":

- A "Terrain layer" that considers components such as vegetation, hydrography, geology, etc.,
- A "Feature layer" that considers components such as cities, buildings, roads, tunnels, airports, harbors, etc.

Figure 4 shows the layer model at an initial phase. At this step, only the specific layer of the international sector has been added onto the common foundation layers. With each additional step, the federal, provincial, municipal, and private-sector layers are added.

The CIPTF used this model to draw up a detailed dependency analysis based on input from approximately sixty experts (Figure 5). It became obvious that there was an immense number of interdependencies, which could not be plotted concisely this way.

12 Canada has not officially moved forward with this model and so far, there is no final model in Canada: see speech by Jacques Grenier: "The Challenge of CIP Interdependencies." *Conference on the Future of European Crisis Management.* (Uppsala, Sweden, 19–21 March 2001). http://www.ntia.doc.gov/osmhome/cip/workshop/ciptf_files/frame.htm.

13 These six sectors are: Governments, Energy and Utilities; Services; Transportation; Safety; Communications.

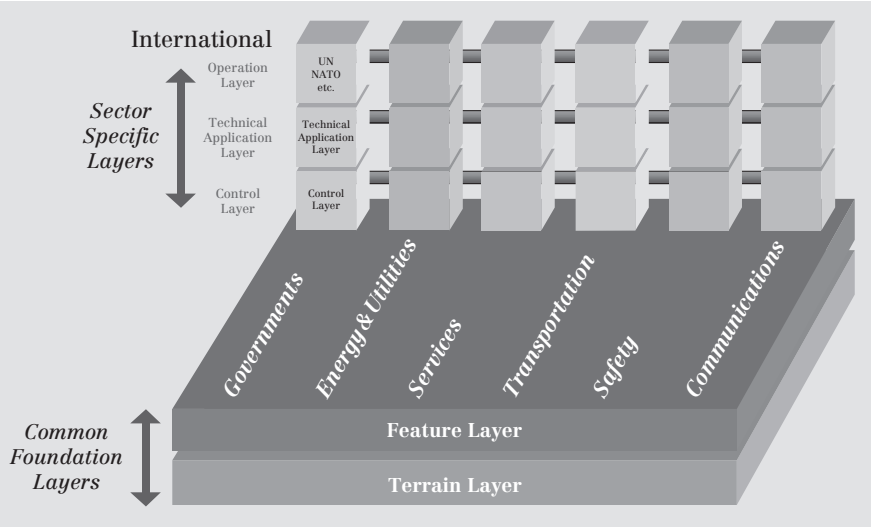

Figure 4: Canadian Critical Infrastructure Model (Source: Presentation by J. Grenier)

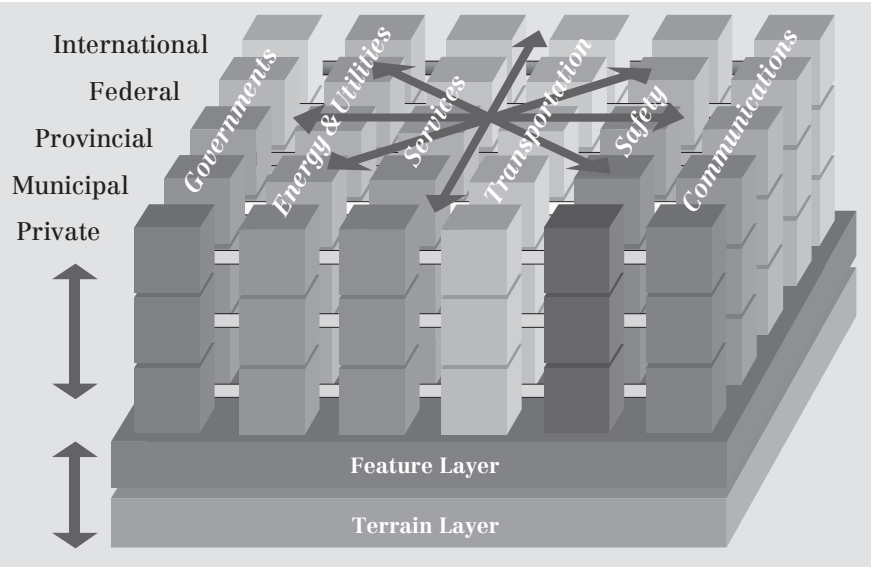

Figure 5: Canadian Critical Infrastructure Model: Dependencies (Source: Presentation by J. Grenier)

Sector	Element	Energy & Utilities					Services		
		Electrical Power	Water Purification	Sewage Treatment	Natural Gas	Oil Industry	Customs and Immigration	Hospital & Health Care Services	Food Industry
Energy & Utilities	Electrical Power		L			M			
	Water Purification	H				M			
	Sewage Treatment	M	H			H			
	Natural Gas	L				L			
	Oil Industry	H	L						
Services	Customs & Immigration	H	L	L	L	L		L	
	Hospital & Health Care Services	H	H	L	H	H	M		H
	Food Industry	H	H	H	L	M	M	L	

Key: H High M Medium L Low

Figure 6: Portion of the Indefinite Matrix (Source: Presentation by J. Grenier)

To better show and evaluate the level of interdependency between the different infrastructure elements, a →*Dependency Matrix* was developed (Figure 6). The extent of direct dependency between infrastructure elements is assigned the →*Values* "high", "medium", "low", and "none".

An application called *Relational Analysis For Linked Systems (RAFLS)* was developed to measure and model the ripple effects of these direct dependencies.[14]

Further Steps in the Infrastructure Protection Process

The Canadian Infrastructure Protection Process further evaluates threats and vulnerabilities in the physical dimension as well as in cyberspace for each component of an infrastructure element in all layers of the model. Risks can then be determined based on 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

14 RAFLS, which is based on an algorithm, uses scored interdependencies and iteratively determines the dependencies and impacts. It shows high and medium dependencies and can demonstrate second-, third-, fourth-, and fifth-level dependencies. It can help to trace linkages and potentially interdict a path in time of crisis. (See Grenier, The Challenge of CIP Interdependencies).

element, between layers in the infrastructure model, and between infrastructure elements, which are called specific risks.

It is noted that risks accumulate when the risks of dependencies are propagated. Therefore, the Canadian process conducts a →*Cumulative Risk Assessment* through dependencies. The assessment of impacts then can be done with the use of a →*Risk/Impact Scattergram*, which ultimately helps to propose a framework for future action in terms of protection.[15]

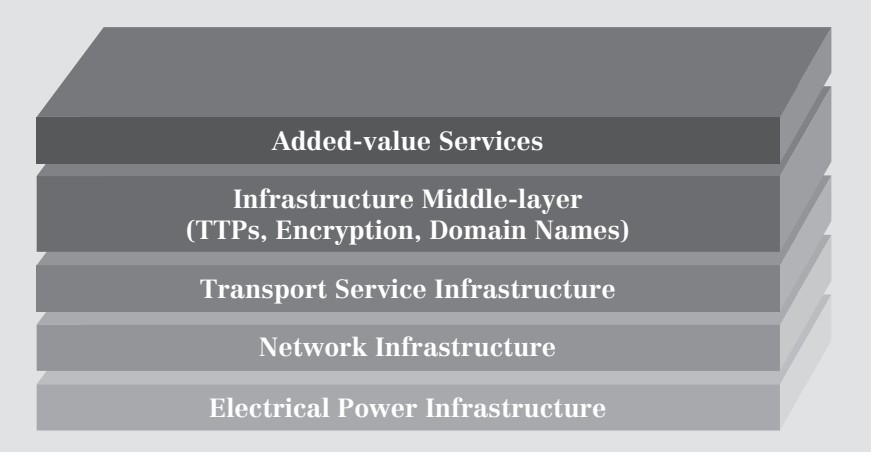

Figure 7: Bitbreuk Layer Model (Source: BITBREUK-Report)

15 Grenier, The Challenge of CIP Interdependencies, slide 25.

The Netherlands

In the Netherlands, the key studies on interdependency are *BITBREUK* ("In Bits and Pieces") by Infodrome[16] and a report on the vulnerability of the Internet by Stratix Consulting Group/TNO FEL. In both studies, qualitative models are described.[17]

BITBREUK Model

The model proposed by the BITBREUK report, which focuses on the Information and Communication Technologies (ICT) infrastructure, is a →*Layer Model* with vertically stacked elements of CII with focus on the IT sector (Figure 7).

Electrical power supply is considered the single factor underlying all ICT. Above this first layer are four more layers. The infrastructure middle layer is located on the fourth level. This layer provides added-value services such as domain name registration or Internet servers between different underlying national and international infrastructures. This middle layer is the basis for the provision of more advanced chains of services for government and the public and commercial organizations. These added-value services are dependent on the availability and integrity of the underlying infrastructure layers. This indicates vertical dependence on the one hand, and, on the other hand, also involves horizontal information flows and information service chains between the different public and private actors, individuals, and society as a whole.[18]

16 Luiijf, Eric., M. Klaver. *In Bits and Pieces: Vulnerability of the Netherlands ICT-Infrastructure and Consequences for the Information Society.* (Translation of he Dutch Infodrome essay "BITBREUK", de kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij). (Amsterdam, March 2000).

17 Luiijf, Eric., M. Klaver, J. Huizenga. *The Vulnerable Internet: A Study of the Critical Infrastructure of (the Netherlands Section of) the Internet.* (The Hague, 2001). http://www.tno.nl/instit/fel/refs/pub2001/kwint_paper1048.pdf. (KWINT Paper).

18 Luiijf, Klaver, In Bits and Pieces, 8–10 and Luiijf, Eric. "Critical Info-Infrastructure Protection in the Netherlands". *ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead.* (Zurich, 8–10 November 2001). http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/luiijf/sld001.htm.

KWINT-Report by Stratix Consulting Group / TNO FEL

The aim of the study was to analyze the current vulnerabilities of the Dutch section of the Internet,[19] to identify possible consequences of threats, and to determine appropriate measures to reduce the vulnerabilities.[20]

The Four Models of the KWINT-Report

In order to address and clarify the roles of various actors, as well as the diversity, interdependencies, and vulnerabilities, four models with different orthogonal points of view were proposed (Figure 8).

- The social level model was used to discuss the motives and economics behind developments in the Internet,
- The functional level model was used as an intermediate between the functions experienced by the user of ICT and the more abstract and technical processes that form the basis for the functioning of the Internet (Figure 9).
- The structural level model was used to investigate the market environment of service providers and of product suppliers,
- The physical level model takes into account that the physical location of the operational facilities is of importance when analyzing vulnerabilities.[21]

Vulnerability Analysis

The vulnerability analysis was conducted for each of the four layers in Figure 8 and for two additional layers (interaction layer for infrastructures; physical environment). For each of the six layers, the weaknesses, the threat probability, and the possible impact were evaluated using three →*Values (*"high", "medium", and "low"). The vulnerabilities were investigated with respect to four →*IT-Security Objectives*, and with respect to natural causes, deliberate attacks by insiders, and deliberate attacks by outsiders.

19 'Internet' was defined end-to-end in this study, to include workstations, private and public IP networks, and information systems on servers.

20 Luiijf, Klaver, Huizenga, The Vulnerable Internet.

21 Luiijf, Klaver, Huizenga, The Vulnerable Internet, 3–5.

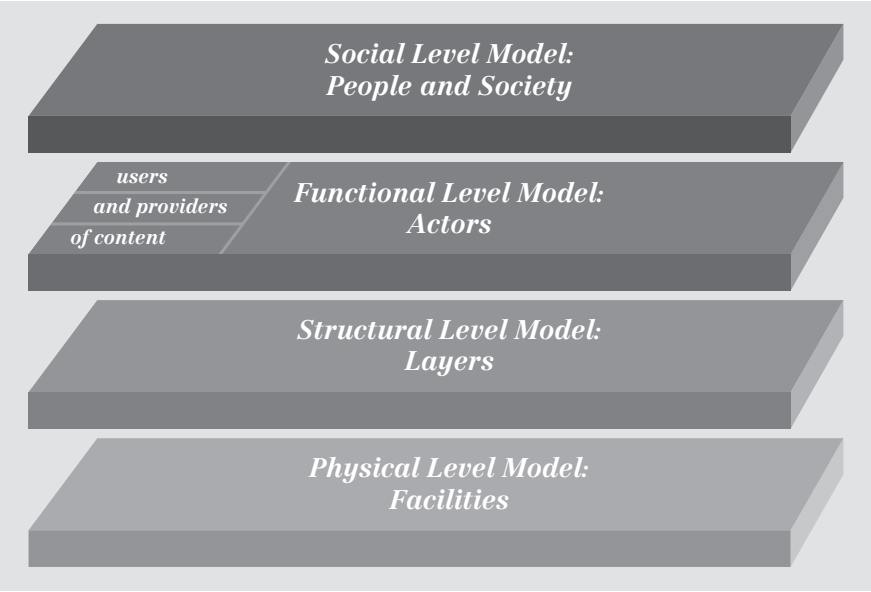

Figure 8: Four Levels of Models (Source: KWINT-Report)

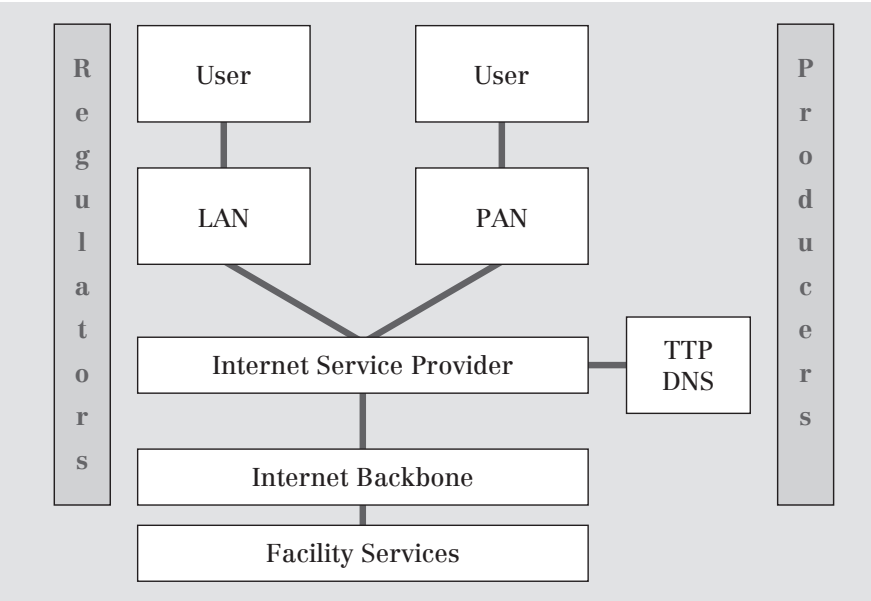

Figure 9: Functional Model with Types of Actors (Source: KWINT-Report)

This resulted in six tables that were aggregated and condensed. The final outcome is a table showing the most important vulnerabilities of the (Netherlands' section of the) Internet (Figure 10). In this table, the impact of selected vulnerabilities on citizens, enterprises, the nation, and society were assessed, as were vulnerabilities with global impact (geographical impact area). These results were used to devise a number of measures that were subsequently proposed to the Dutch government.

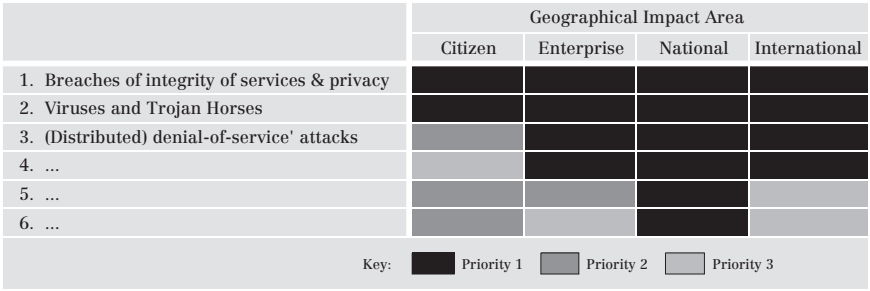

Figure 10: Geographical Impact Area Matrix (Source: KWINT-Report)

Norway

According to Norwegian experts, the BAS matrix is the only available model for analysis of Norwegian CII. However, the need to return to research agendas is well known in Norway and additional efforts can be expected.[22]

Multi-Criteria Model of the "Protection of Society" Projects (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).[23] 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 proceeded in four interlinked steps (Figure 11).

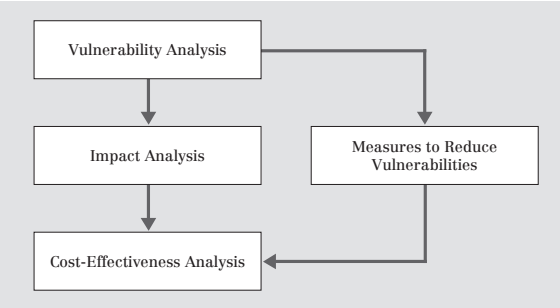

Figure 11: Steps of the Norwegian Vulnerability Analysis (Source: Hagen, Fridheim)

22 Interview with representative of the Norwegian Commission on the Vulnerability of Society.

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

At first, a →*Vulnerability Analysis* was conducted. By using →*Seminar Games*, BAS2 mapped the dependency of modern society upon telecommunication services in crisis and war-like situations. Secondly, an impact analysis was conducted. Next, measures that might reduce the vulnerabilities were evaluated. Lastly, the actual cost-effectiveness analysis was undertaken.

Because no single method was able to handle all the problems BAS2 had to analyze, a combination of several techniques and methods was employed to calculate the most cost-effective protection strategy for the telecommunication system. These other approaches include seminar games; use of →*Scenarios*, →*Causal Mapping*, →*Fault Tree Analysis*, and Probabilistic Cost Estimation, as well as a →*Multi-Criteria Model*.

The Multi-Criteria Model

Calculating the effectiveness of measures to reduce the vulnerabilities proved to be a challenge. Rather than applying mathematical simulation models, the BAS2 study used the →*Multi-Criteria Decision Approach*. This approach systematically maps out subjective expert evaluations and combines them into a quantitative measure of effectiveness.

The multi-criteria 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 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 to each other, so that the top criteria in the technical sub-system are identical to the bottom criteria in the societal sub-system. (Figure 12).

The ultimate goal is to maximize the protection of society. This goal can be distilled into three sub-criteria, which are:

- to minimize loss of life,
- to minimize economic losses, and
- to minimize the danger of a loss of sovereignty.

These criteria can be further divided into more specialized criteria. Figure 13 shows parts of the social hierarchy. The relationships between the criteria on different levels are then quantified by experts. The experts weigh the different criteria in the model relative to each other. These preferences serve as a measure of the effectiveness of one criterion compared to the others on the same level.

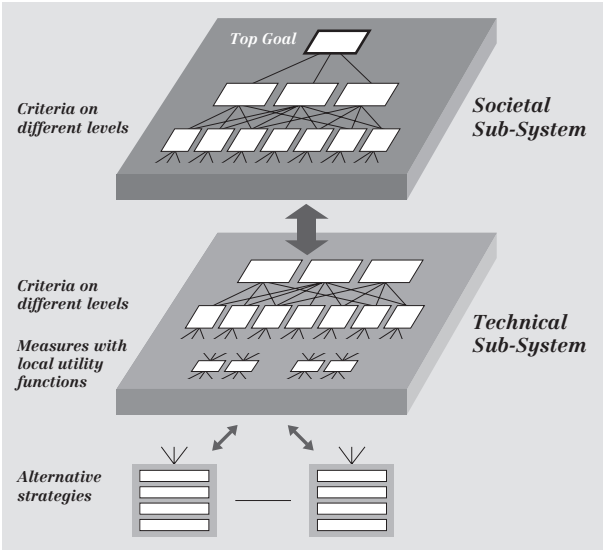

Figure 12: Multi-criteria Hierarchy (Source: Hagen, Fridheim)

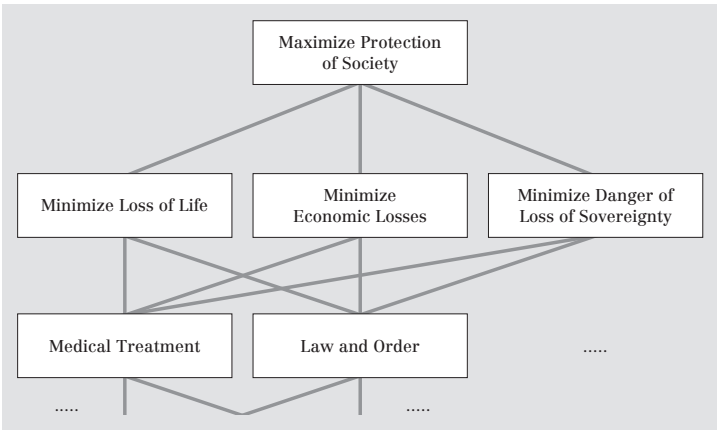

Figure 13: Parts of the Social Hierarchy for the Multi-Criteria Analysis (Source: Hagen, Fridheim)

Switzerland

Although Switzerland's authorities recognize the increasing vulnerability of Swiss CII, appropriate measures for gathering, structuring, and managing the emerging risks are yet to be accomplished. There are few attempts to model the dependencies of critical infrastructures on the information infrastructure, or on the interdependencies between CII. Existing models are predominantly qualitative. One model is described: The InfoSurance Sector Model. Overall, there is a great need to return to the research agenda.

InfoSurance Sector Model and CIIP Framework

Representatives of the InfoSurance foundation defined fourteen infrastructure sectors as being critical to Switzerland, and explored possible interdependencies between these sectors. The resulting picture shows the crucial sectors on a circle and the expected one-way or two-way interdependencies between them. At the center of the model are the two main recipients of the services provided by these critical sectors: enterprises and the individual inhabitants of Switzerland (Figure 14).

The InfoSurance →*Sector Model* is only the starting point for a more comprehensive CIIP framework that encompasses seven methodological elements (Figure 15).[24] The combined analysis in a step-by-step procedure provides a rough picture of interdependencies between CII sectors, impacts, threat patterns, and risk management procedures. To a large extent, this model is still theoretical.

- Element 1: *Sector Model:* Switzerland is defined as a complex of fourteen interdependent sectors.
- Element 2: →*Process and Technology Analysis:* This element identifies the interdependencies within a single sector by assessing different layers of a sector. Figure 16 shows a process and technology analysis for the telecommunications sector.
- Element 3: *Dependability Analysis:* The next element identifies the interdependencies between two and more sectors, using the results of the →*Process and Technological Analysis*. The degree of depen-

24 InfoSurance, Ernst Basler + Partner AG. *Einflussfaktoren und Abhängigkeiten im Umgang und Einsatz von Informationssicherheit* (Zollikon, 2000). http://www.infosurance.ch/de/ppt/Krisenverstaendnis.ppt.

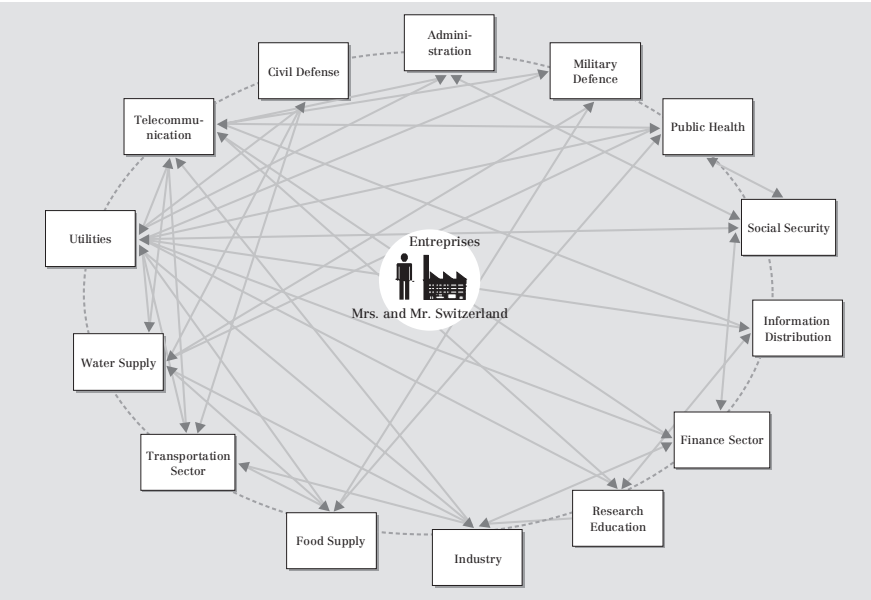

Figure 14: InfoSurance Sector Model (Source: InfoSurance/ Ernst Basler + Partner AG)

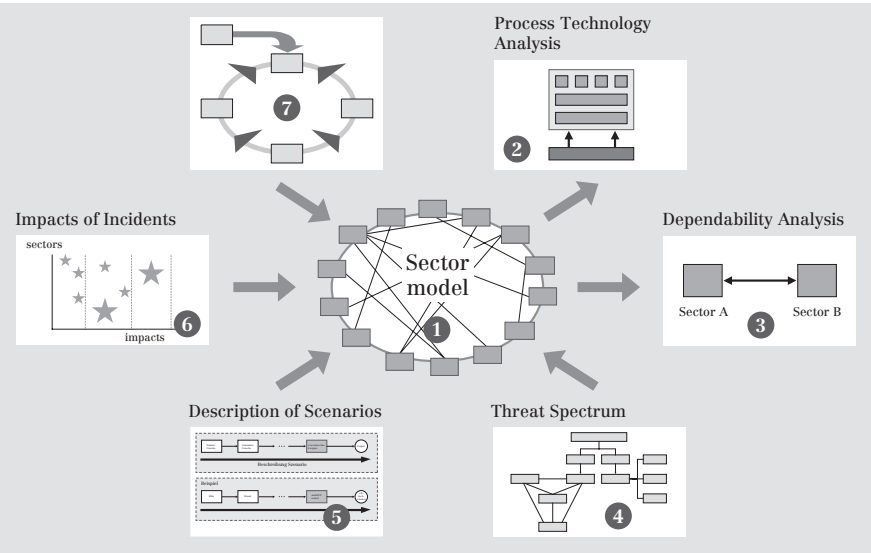

Figure 15: The CIIP Framework Switzerland (Source: InfoSurance/ Ernst Basler + Partner AG)

dency may be determined by identifying the nodes and linkages between sectors.

- Element 4: *Spectrum of Possible Threats:* This element structures the threat spectrum, and also includes an analysis of possible actors and their motives.
- Element 5: *Description of Scenarios:* Possible scenarios are described using →*Scenario Technique* or scenario software.
- Element 6: *Impacts of a Single Event:* A risk analysis approach identifies the impact of incidents within critical infrastructure sectors.
- Element 7: *Risk Management Process:* The risk management process helps to analyze and assess risks and is useful in the planning, implementation, and control of measures.

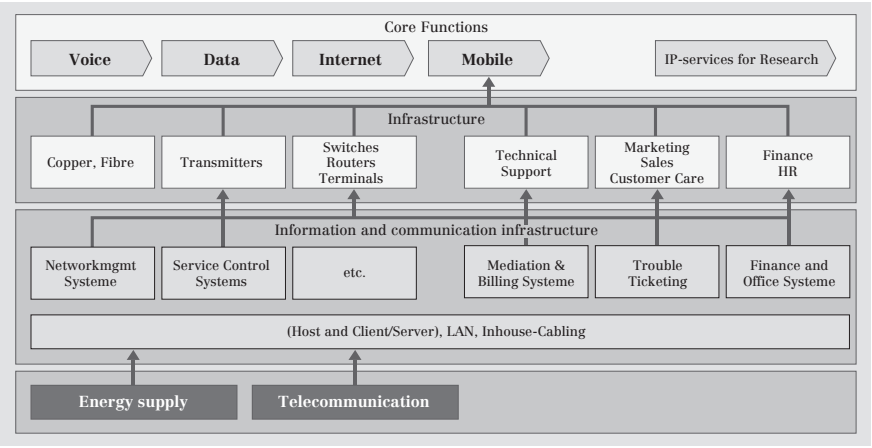

Figure 16: Process and Technology Analysis for the Telecommunication (Source: InfoSurance/ Ernst Basler + Partner AG)

United States

Even though many official US papers discuss the concept and importance of interdependencies,[25] none of them provides a methodological guideline for analyzing this phenomenon. However, over the years, the US has consistently focused on interdependency research. For example, efforts are underway to model and simulate complex interdependencies. One modeling approach, currently developed at the Sandia National Laboratories, utilizes an agent-based methodology to predict interactions among critical infrastructure elements.[26] Also, a comprehensive toolset for interdependence analysis is being developed by the Department of Energy (DoE), which is very active due to the extensive experience its Argonne National Laboratory has accumulated in the field. Below, a →*Layer Model* as developed by the DoE is presented together with the →*Vulnerability Assessment* Process designed by the Critical Infrastructure Assurance Office (CIAO).

The Department of Energy (DoE) Layer Model

The Department of Energy (DoE) uses a →*Layer Model* for the energy sector that shows interdependencies with other sectors and sector components (Figure 17).

Each sector is pictured as a grid on which the individual critical system components are located. Each component must be mapped in detail. The aim is to define critical system components and attendant vulnerabilities, interdependence propagation pathways and the degree of coupling, spatial and temporal system behavior, and the evaluation of protection, mitigation, response, and recovery options.[27]

In addition, a comprehensive toolset for interdependence analysis is being developed by the DoE. It is composed of early alert screening tools, interdependency simulation tools, and a broad range of supporting analytic tools. Its aim is to model the interaction among system components and analyze how disruptions to one infrastructure can affect or propa-

25 Cf. The President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Protecting America's Infrastructures.* (Washington, D.C., October 1997).

26 See http://www.sandia.gov/Surety/Facts/Modeling.htm.

27 Scalingi, Paula. *Critical Infrastructure Protection Activities. Department of Energy.* (March 2001). http://www.naseo.org/events/outlook/2001/presentations/scalingi.pdf.

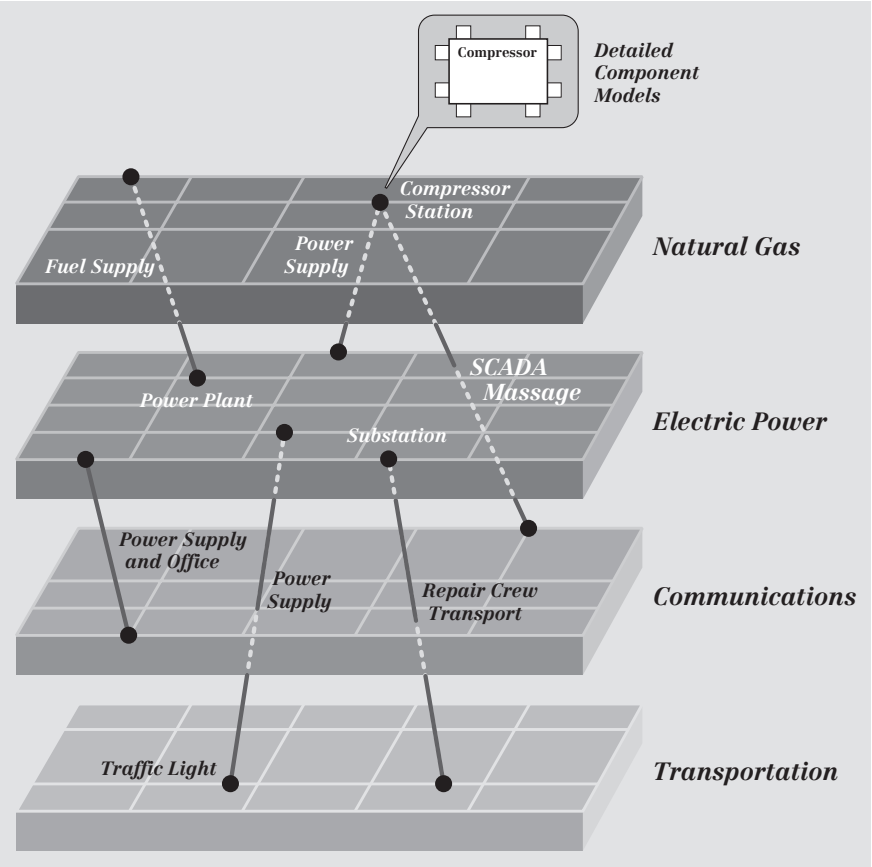

Figure 17: DoE Layer Model (Source: Buehring, Argonne National Laboratory) [28]

gate to other infrastructures. These tools also help to examine protection, mitigation, response, and recovery strategies.[29] The DoE has also developed a three-step →*Vulnerability Assessment* Process.[30]

28 Buehring, Bill. *Natural Gas Security Issues Related to Electric Power Systems*. (28 November 2001). http://wpweb2k.gsia.cmu.edu/ceic/presentations/Buehring.pdf, slide 19.

29 Buehring, Natural Gas Security Issues Related to Electric Power Systems.

30 Scalingi, Critical Infrastructure Protection Activities.

CIAO Vulnerability Assessment Process/Project Matrix

On the basis of Presidential Decision Directive (PDD) 63 and the National Plan 1.0, CIAO developed "Project Matrix™", a program designed to identify and characterize the assets and associated infrastructure dependencies and interdependencies that the US government requires to fulfill its most critical responsibilities to the nation. Project Matrix™ involves a three-step process in which each civilian federal department and agency identifies (1) its critical assets; (2) other federal government assets, systems, and networks on which those critical assets depend to operate; and (3) all associated dependencies on privately owned and operated critical infrastructure elements.[31] The exact methodology is confidential, but the similar approach of the "Vulnerability Assessment Framework" (VAF) developed for CIAO is publicly available.[32] The methodology consists of three main steps, as shown in Figure 18.

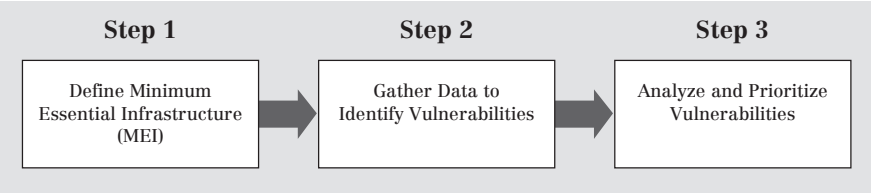

Figure 18: Steps of the VAF Evaluation Process (Source: KPMG/ Marwick)

Step 1: Define Minimum Essential Infrastructure (MEI)

In step 1, the assessment team will define the so-called "Minimum Essential Infrastructure" (MEI) for the organization, with focus on the specific infrastructure components that support essential processes. It is recommended that this first step consist of a broad, department- or agency-level macro vulnerability assessment of both the internal agency MEI and the agency's relationship to, and connection with, the national MEI.

31 Critical Infrastructure Assurance Office, Project Matrix: http://www.ciao.gov/federal/.

32 KPMG, Peat Marwick. *Vulnerability Assessment Framework 1.1. Prepared under contract for the Critical Infrastructure Assurance Office*. (October 1998). http://www.ciao.gov/resource/vulassessframework.pdf. The VAF methodology has drawn heavily on other processes for measuring information technology (IT) system controls, such as: the Control Objectives for Information Technology (COBIT) process of the Information Systems Audit and Control Foundation (ISACF); the May 1998 publication "Executive Guide Information Security Management" of the US General Accounting Office (GAO); and the GAO's standards for auditing federal information systems (Federal Information Systems Control Audit Manual (FISCAM)).

Step 2: Gather Data to Identify Vulnerabilities

The objective of step 2 is to identify the vulnerabilities in the organization related specifically to the MEI. The outcome will be the identification and reporting of flaws or omissions in controls that may affect the integrity, confidentiality, accountability, and/or availability of resources that are essential for achieving the organization's core mission(s). The criteria used to identify these vulnerabilities are depicted in Figure 19, showing the so-called "VAF Cube".

Step 3: Analyze and Prioritize Vulnerabilities

In step 3, vulnerabilities identified in step 2 are defined and analyzed. This allows a first order of prioritization for purposes of remediation or minimization. Figure 20 shows the activities conducted under step 3.
Step 3 includes four sub-steps: (1) Each vulnerability is examined to determine if it has an impact on more than one MEI core process; (2) vulnerabilities are sorted by core process; (3) a graphical summary of

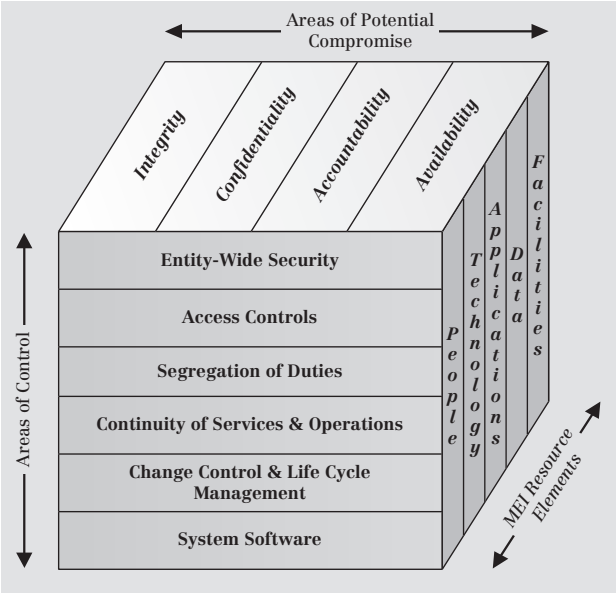

Figure 19: The VAF Cube (Source: KPMG/ Marwick)

the number of vulnerabilities by core process is generated; (4) an analysis of the likelihood that a vulnerability will be exploited is conducted, taking into consideration the potential threats to the agency. Using these four parameters, priorities are assigned for vulnerability remediation or minimization.

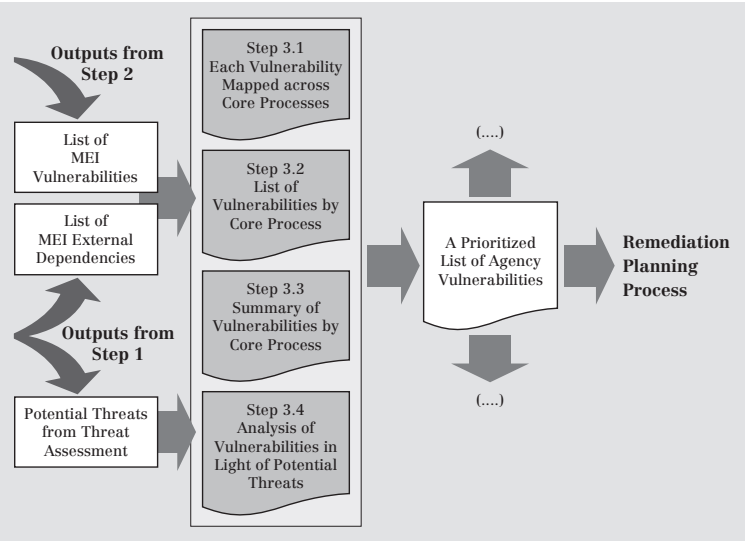

Figure 20: Step 3 Activities (Source: KPMG/ Marwick)