



Critical Infrastructure Protection in the National Capital Region

**Risk-Based Foundations for Resilience and
Sustainability**

**Final Report, Volume II:
Criteria and Evaluation of Vulnerability
Assessment and Risk Management Tools and
Procedures**

September 2005

University Consortium for Infrastructure Protection

Managed by the
Critical Infrastructure Protection Program
School of Law
George Mason University

This Page Intentionally Blank

Critical Infrastructure Protection in the National Capital Region

Risk-Based Foundations for Resilience and Sustainability

Final Report, Volume II: Criteria and Evaluation of Vulnerability Assessment and Risk Management Tools and Procedures

Submitted in fulfillment of:

Department of Homeland Security Urban Areas Security Initiative (UASI) Grant 03-TU-03; and
Department Justice Office of Community Oriented Policing Services (COPS) Grant 2003CKWX0199

September 2005

Terrence P. Ryan, Christine Pommerening, and Jerry P. Brashear

University Consortium for Infrastructure Protection

Managed by the
Critical Infrastructure Protection Program
School of Law
George Mason University



– **Notice** –

This research was conducted as part of the National Capital Region Critical Infrastructure Project, carried out by the University Consortium for Infrastructure Protection, managed by the Critical Infrastructure Protection Program, George Mason University, John A. McCarthy, Director and Principal Investigator.

It was sponsored by the U.S. Department of Homeland Security's Urban Area Security Initiative grant #03-TU-03, and by the U.S. Department of Justice Community Oriented Policing Services Program grant #2003CKWX0199, under the direction of the Senior Policy Group of the National Capital Region.

The views expressed are those of the authors, and do not necessarily reflect the views of the Department of Homeland Security, the Department of Justice, or the Senior Policy Group of the National Capital Region.

Copyright © 2005 by George Mason University

Published in 2006 by George Mason University

National Capital Region
Critical Infrastructure Protection Project

Criteria and Evaluation of Vulnerability Assessment and Risk
Management Tools and Procedures

September 2005

Terrence P. Ryan

Christine Pommerening, PhD

Jerry P. Brashear, PhD

This Page Intentionally Blank

Table of Contents

Acknowledgements	3
1. Criteria and Evaluation of Vulnerability Assessment and Risk Management Tools and Procedures	4
1.1. General Discussion	4
1.2. Establishing criteria	4
1.3. Identifying vulnerability and risk management tools	7
1.4. Analyzing the nature of the available tools	7
1.4.1. Major Findings	8
1.4.2. Recommendations	9
1.5. Conclusions	11
Endnotes	12
Appendix A: Critical Infrastructure Analysis Matrix	32
Appendix B: Assessment Tool Analysis Matrix Summary	35
Appendix C: Assessment Tool Analysis Matrix	41
Appendix D: Bibliography	91

List of Tables

Table 1. Characterization of Types of Critical Infrastructure Vulnerability Assessment and Risk Management Tools	6
--	---

Table of Figures

Figure 1: What are the primary subjects of the tool?	13
Figure 2: Assessment Subject: Type of Asset Assessed?	14
Figure 3: Does the system address the interaction of multiple assets within a system?	15

Figure 4 Interdependencies: Which upstream or down stream sectors are included systematically?	16
Figure 5: Consequence Metric: What types of consequence or loss are measured?	17
Figure 6: Tool Design: Principle elements that make up the core of the tool.	18
Figure 7: Tool Design: Type of data input required by the tool.	19
Figure 8: Tool Design: Output from execution of the tool.	20
Figure 9: Tool Design: Estimated time frame for completion or implementation of the tool.	21
Figure 10: Tool Design: Estimated cost of completing or implementing the tool.	22
Figure 11: Tool Design: Who can the tool be used by?	23
Figure 12: Level of maturity of the tool in its sector	24
Figure 13: Is there a process for screening out low priority assets from further assessment?	25
Figure 14: What type of Threats / Hazards does the tool address?	26
Figure 15: How are threats / hazards are quantified?	27
Figure 16: Does the analysis include contextual standards and from a systemic perspective?	28
Figure 17: How are vulnerabilities quantified?	29
Figure 18: How are critical structures and functions identified?	30
Figure 19: How are risk reduction and cost benefits determined?	31

Acknowledgements

This research was conducted as part of the National Capital Region Critical Infrastructure Protection Project, carried out by the University Consortium for Infrastructure Protection, managed by the Critical Infrastructure Protection Program, George Mason University, John A. McCarthy, Director and Principal Investigator. It was sponsored by the U.S. Department of Homeland Security's Urban Area Security Initiative grant #03-TU-03 under the direction of the Senior Policy Group of the National Capital Region. The views expressed are those of the authors, and do not necessarily reflect the views of the Department of Homeland Security or the Senior Policy Group.

1. Criteria and Evaluation of Vulnerability Assessment and Risk Management Tools and Procedures

1. 1 General Discussion

There are literally hundreds of tools and methods for conducting vulnerability assessments and risk management of critical infrastructures. They differ widely in terms of approach, scale, and scope. Selecting the most appropriate and relevant one for a particular sector, asset, and system is necessary, however, to assure adequate protection of a critical service, facility or function. This report is intended to give an overview of the nature and completeness of the most widely used tools for those individuals in the public and private sector that are tasked with risk management for their organizations. The report provides an analysis that characterizes a number of the most prominent tools relative to a standard list of criteria. The process consisted of the following steps:

- Establishing criteria
- Identifying a broad set of vulnerability and risk management tools
- Determining the small subset of tools in the studied sectors that are widely used and accepted by the Critical Infrastructure owner / operators. These are referred to as “Good Practice” tools.
- Analyzing the nature of the available tools. This includes comparing / contrasting the traits of all tools analyzed with the traits of the “Good Practice” subset of the tool list

In conjunction with the Tool Database¹ this analysis serves as a means to improve the quality of the risk management process by giving users a quick way of comparing and contrasting different tools, and specifically selecting parts or all of them according to their needs.

1.2 Establishing criteria

First, an initial characterization of vulnerability and risk management tools was devised to group the available tools along a continuum from broad, general policy guidance to highly quantitative engineering / economic risk estimation (Table 1). Placing the tools into one of these four categories organizes the analysis and provides an indicator of the level of sophistication of the sectors' state of risk management.

A list of criteria was developed based on this risk management categorization and three other sources: The Office of Domestic Preparedness (ODP),² The Congressional Research Service (CRS),³ and the present NCR-CIP project.⁴ The criteria were designed to identify similarities in design as well as differences in the scope of tools. This enables the analyst to make an informed decision on what tool or tools might be relevant, applicable, and practical for a particular critical infrastructure asset or system.

The criteria were organized into two sections: the first section is descriptive, the second analytic. The full analysis questionnaire is attached in Appendix-A, Critical Infrastructure Analysis Matrix.

- **Descriptive Section:** The descriptive section of the matrix describes the assessment tools by subject, metric, and design.

- **Analytic Section:** The analytical section of the matrix characterizes the assessment tools by Maturity, Threat / Hazard, Consequence, Vulnerability, and Cost benefit.

They follow a continuum from a level of simple compliance, through a level of basic analytical risk reduction, to the final level of risk reduction by full economic optimization considering potential threat probabilities and consequences.

Table 1. Characterization of Types of Critical Infrastructure Vulnerability Assessment and Risk Management Tools

Sophistication Level	Pros	Cons	Aggregation Level		
			Asset/Function Examples	System/Sector	Multi-Sector Region
General Policy Guidance	Broadly stated requirements with maximum of flexibility in implementation	Lacks standards of compliance; difficult to audit	Sarbanes-Oxley	Sarbanes-Oxley	None available; not recommended
Detailed Procedures	Consensus-based, qualitative or %-compliance; on/off priority lists; requires little or no professional training or expertise	No estimates of relative or absolute value, only gross rank comparisons and only with like assets and methods	ANSI	NCR-CIP Minimum: Assure sector guidance as extension of asset governance	NCR-CIP: Guidance to SPG: promote as minimum, standard-based
Relative Risk Management (Risk Management Lite)	Standard analytics; can compare results with others, possibly in different sectors using same method	Limited cross-comparisons; only relative values – no absolute values (cannot compare benefits to costs); requires moderate level of professional training/expertise	FEMA 426 Series; Sandia’s RAM-W™; RAM-D™; Department of Veteran Affairs Guide; Current ODP Special Needs Tool Kit; ASME RAM-CAP™	NCR-CIP: recommendations for sector tools, incentives, guidance – as generalized to systems	NCR-CIP objective: First approximation resource allocation tool; rough prototype expected from NCR-CIP Phase I
Full Risk Management	Standard analytics can be directly compared across assets and sectors; estimates absolute values of benefits	Requires high level of professional training/expertise	Nuclear/NASA risk engineering	NCR-CIP: specs for extension of ASME to systems; DHS-National Labs’ CIPP/DSS	DHS-National Labs’ CIPP/DSS NCR-CIP objective.: specs as phase II RIPP Long Term Target

1.3 Identifying vulnerability and risk management tools

As part of the project, several research teams were examining the state of risk management in their respective sectors in the NCR. These sector teams identified a broad range of risk and vulnerability assessment methodologies generally available to critical infrastructure owners and operators. These consisted of assessment tools useful at the asset, firm, system, and sector level. The non-proprietary tools were also collected for inclusion into the NCR toolkit and library. After screening, a total of 62 tools were identified for study.

Additionally, the sector teams identified a small subset from this list of nineteen tools that are widely used and accepted by the CI owner / operators. These were established as the “Good Practice” subset of tools.

1.4 Analyzing the nature of the available tools.

The project team conducted an extensive literature review and numerous interviews engaging representatives from eight different critical infrastructure sectors. These activities found that the tools varied widely in their design and relative to their approach to the application of risk management. Tools were found throughout the continuum from a level of simple checklist compliance, through a level of basic analytical risk reduction, to the final level of risk reduction by full economic optimization considering potential threat probabilities and consequences. The tools ranged from several pages of yes-no questions, to sophisticated software systems that require significant amounts of data, and experts to run them. The study also found significant differences between the general focus and design of available tools and focus of the “Good

Practice” subset of the tool list. A summary of the major findings and recommendations are listed below. A full compellation of the characterization results and their related charts are found in Figures 1-19, Appendix B, Assessment Tool Analysis Matrix Summary, and Appendix C: Assessment Tool Analysis Matrix.

1.4.1 Major Findings

- The majority of tools reviewed are at the lower end of the risk management continuum. This includes simple compliance, through a level of basic analytical risk reduction. This was found true for both the general list of tools and the “Good practice” subset of tools. (See figures 7, 8, 12, 15-17, 19) Two of the few high end risk management tools that include relative risk reduction and relative economic optimization while considering potential threat probabilities and consequences were:
 - Office for Domestic Preparedness, State Homeland Security Assessment and Strategy Program, Special Needs Jurisdiction Tool Kit
 - Risk Analysis and Management for Critical Asset Protection (RAMCAP™), ASME Innovative Technologies Institute, LLC

- The topic of interdependencies is systematically included in many assessment tools, but is addressed on a rather superficial level. The checklist for interdependencies within the tools is mostly a simple review of dependent utilities and communication lines. The tools give little guidance for understanding the levels of interdependencies

and where vulnerabilities may lurk, which is the underlying intention for this guidance. (See figures 1, 4)

- Most of the assessments address protecting buildings, facilities and operation, but less than half consider protecting “people”. However, most of the “Good Practice” tools systematically include “people” as assets in their calculations. (See figures 2, 5)
- A majority of the tools address or measure financial and capacity impacts in their analysis of the consequences of loss. However, environmental degradation is considered in less than a quarter of the cases. (See figure 5)
- 75% of tools surveyed and 89% of the “Good Practice” tools use qualitative data (expert assessment and relative ranking scales) rather than quantitative data (a cost benefit analysis). The associated scale for the threat, consequence and vulnerability factors varied widely across the studied tools and were not readily comparable. (See figures 7, 8, 12-19)
- Very few tools have a wide spread use. Even among the “Good Practice” tool subset, only a 33% were accepted as a standard practice in the sector. (See figure 12)
- Most of the assessment tools do not take an all threat / hazard approach, but most of the “Good Practice” tools systematically include both man made and natural threats in their calculations. (See figures 14,15)
- Assigning relative and absolute probabilities or likelihoods based on failure analysis is conducted in only about 20% of the assessment tools. This was found in quantifying threats, vulnerabilities, and also assigning consequences of loss. (See figures 15-19)

1.4.2 Recommendations

From these findings, the following recommendations were developed to foster and enhance security of the critical infrastructure in the NCR.

- Encourage the evolution of business practices that are currently simple compliance based assessment processes towards using a risk based methodology.
- Establish a common “Consequence of Loss” reference table. The majority of current assessment tools use qualitative data (expert assessment and relative ranking scales) rather than quantitative data (a cost benefit analysis). A common relative scale is required to use these results to compare disparate assets in a region wide risk management program.
- Establish a regional assessment process that can accept and harmonize data from the many different asset level assessment tools. There are so many different assessment tools used on so many different types of assets that it would be cost prohibitive to require each to conduct a new assessment with a new tool. The private owner / operators have also stated strong opposition to assessment tools developed outside of their trade associations or even their control. A regional assessment processes that can accept and normalize the basic data (threat, consequence, vulnerability, risk, and risk reduction) from assessments is required.
- Request and encourage professional organizations (e.g. American Water Works Association, Association of American Society of Civil Engineers), and government laboratories and agencies (e.g. Sandia National Laboratory, US Environmental Protection Agency) to develop Good Practices in assigning relative and absolute probabilities or likelihoods based on failure analysis.

- Require assessment methods and tools to assess inter-sectoral dependencies.
- Give priority to infrastructure security strategies and measures that both enhance infrastructure safety and security as well as support or enhance normal operations.

1.5 Conclusion

This analysis of publicly available tools, procedures, and assessment processes for critical infrastructures in the National Capital Region and beyond, together with other such efforts, indicate a less than consistent approach to, and application of, vulnerability assessment and risk management methods. Research and development in support of a more resilient region must encourage the evolution of business practices from a simple compliance based assessment toward a risk based methodology. These methods and analytics must also better address issues of interdependencies and costs-benefit concerns of the private sector.

Endnotes

¹ The database is another deliverable of project and has been developed as a stand-alone application that can be hosted on UNIX servers. It is described in detail in another report in this series.

² Moteff, J. (2004). *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences* (No. RL32561). Washington, DC: Congressional Research Service.

³U.S. Department of Homeland Security. (2003). *Vulnerability Assessment Methodologies Report. Phase I Final Report*. Washington, DC: Office for Domestic Preparedness.

⁴McCarthy, J.A. et al. (2005). *Foundations for Risk Based Critical Infrastructure Protection in the National Capital Region*. Arlington, VA: George Mason University.

Figure 1

What are the primary subjects the tool refers or applies to?

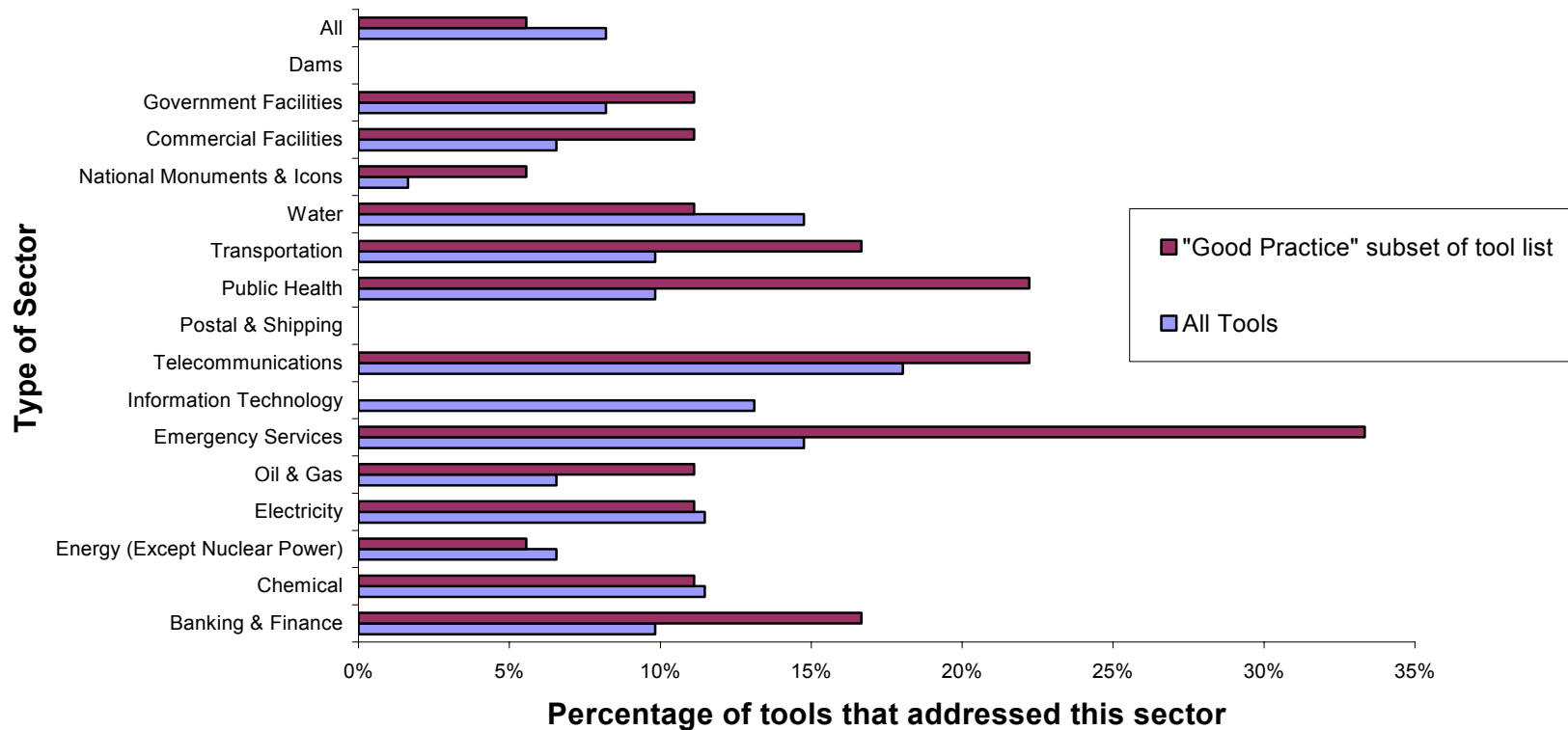


Figure 2

Assessment Subject: Type of Asset Assessed

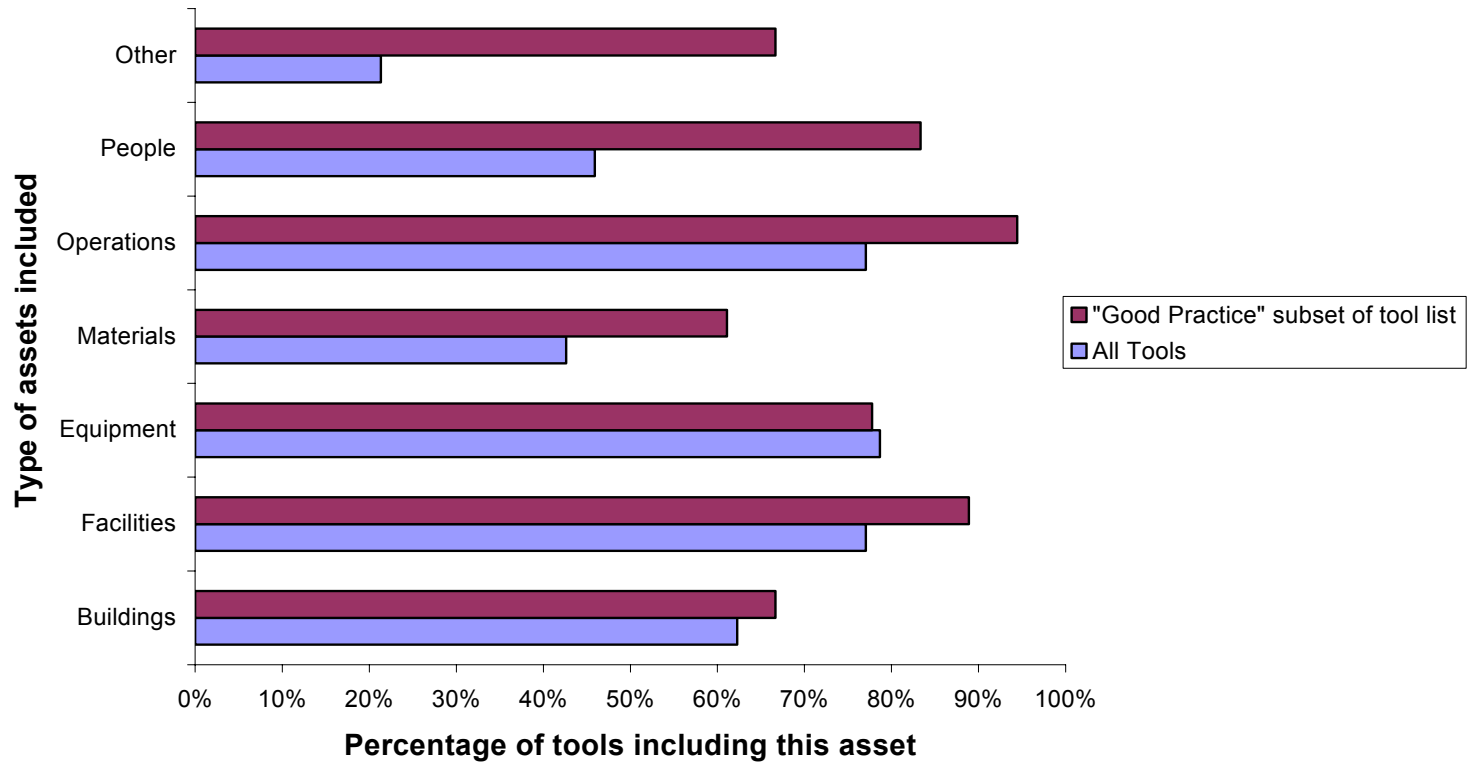


Figure 3

Does the system address the interaction of multiple assets within a system?

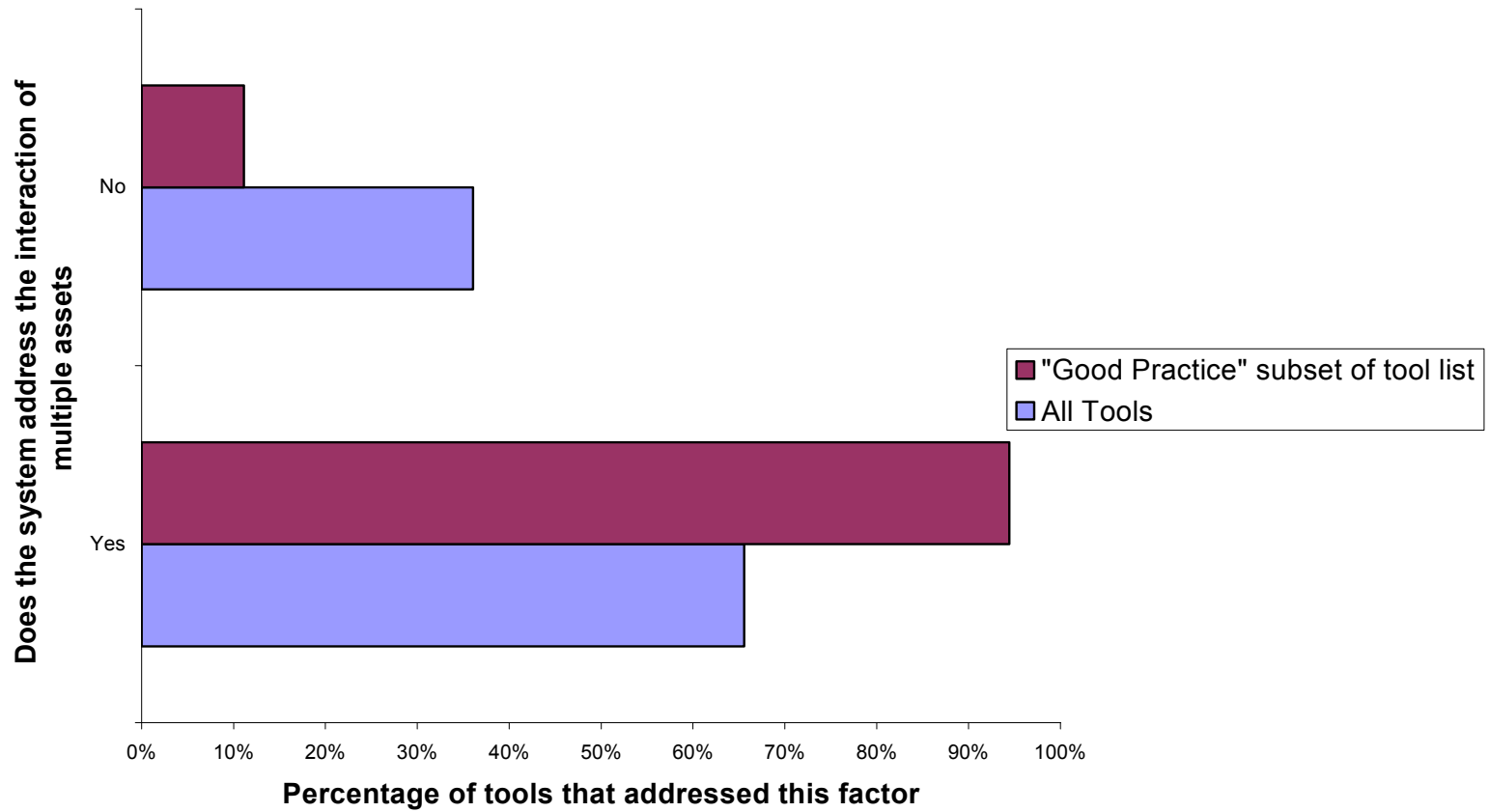


Figure 4

Interdependencies: Which upstream or down stream sectors are included systematically?

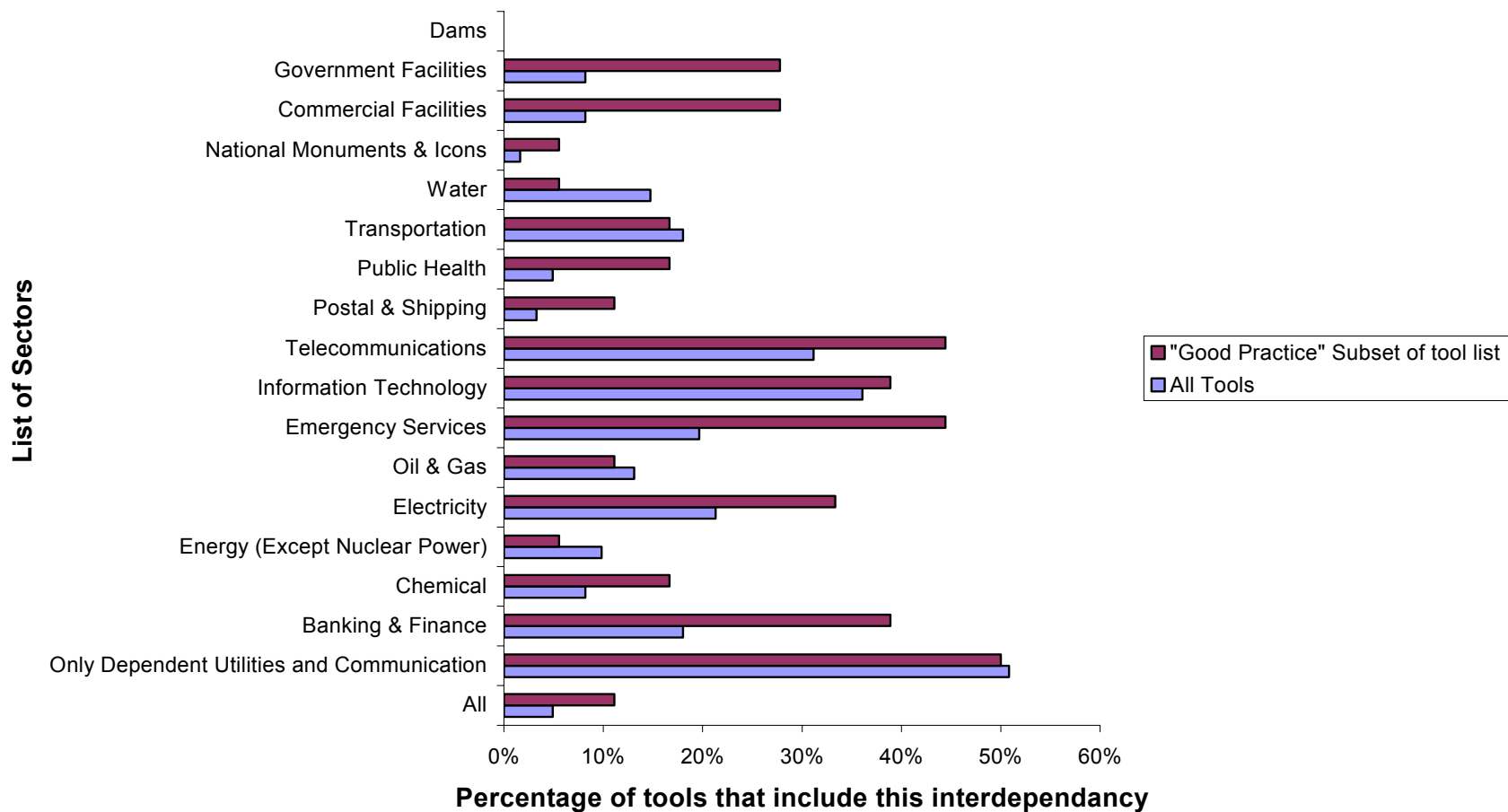


Figure 5

Consequence Metric: What types of consequence or loss are measured?

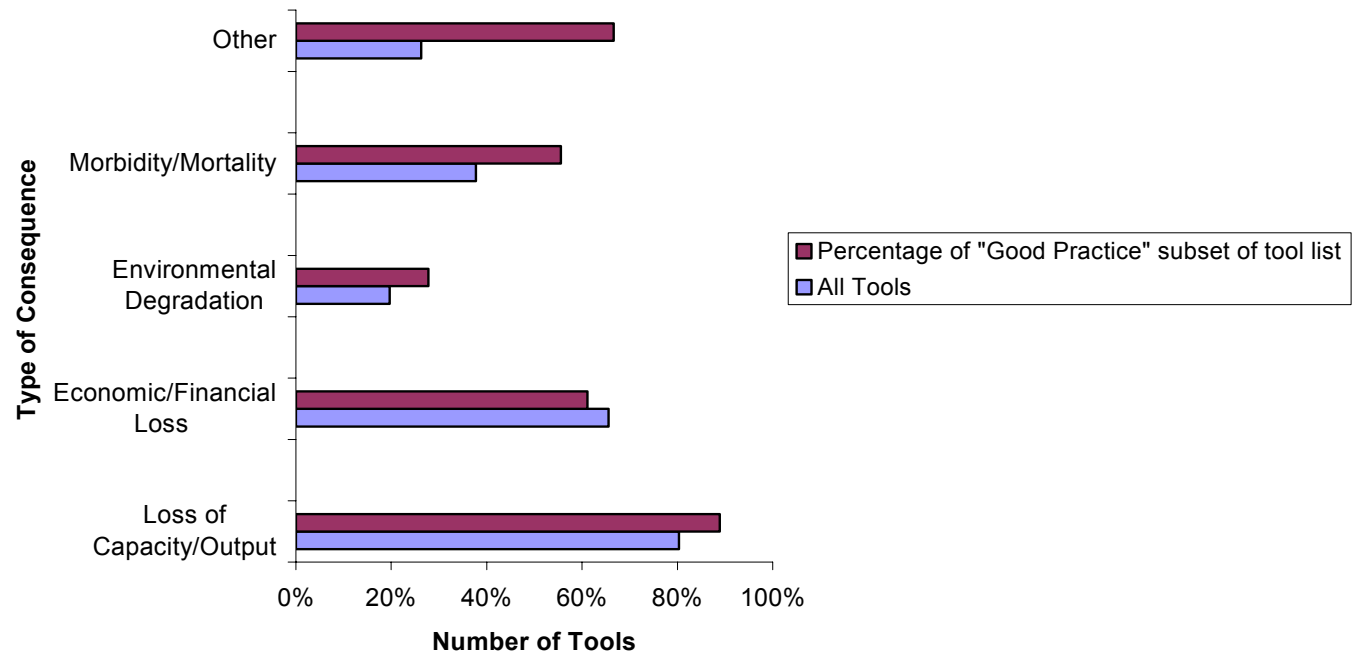


Figure 6

Tool Design: Principle elements that make up the core of the tool.

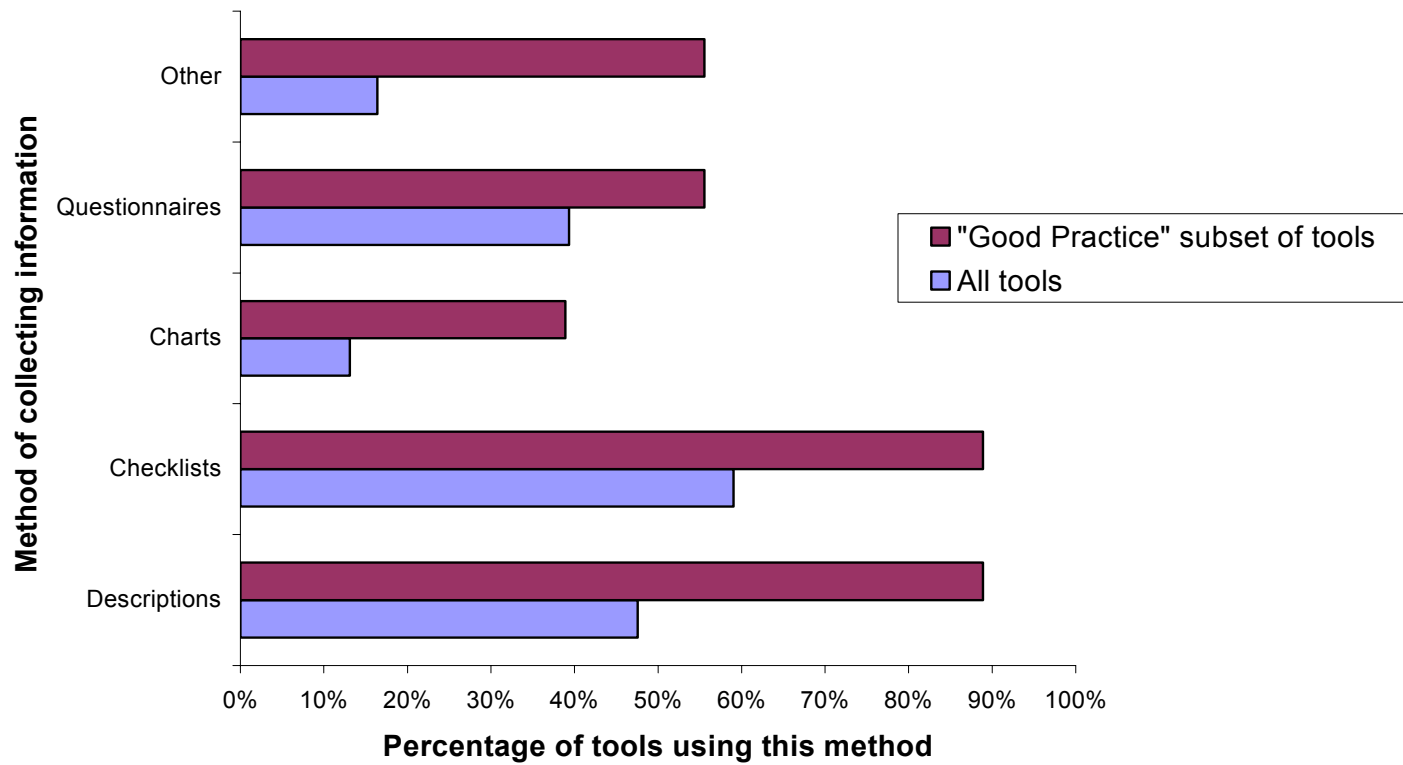


Figure 7

Tool Design: Type of data input required by the tool.

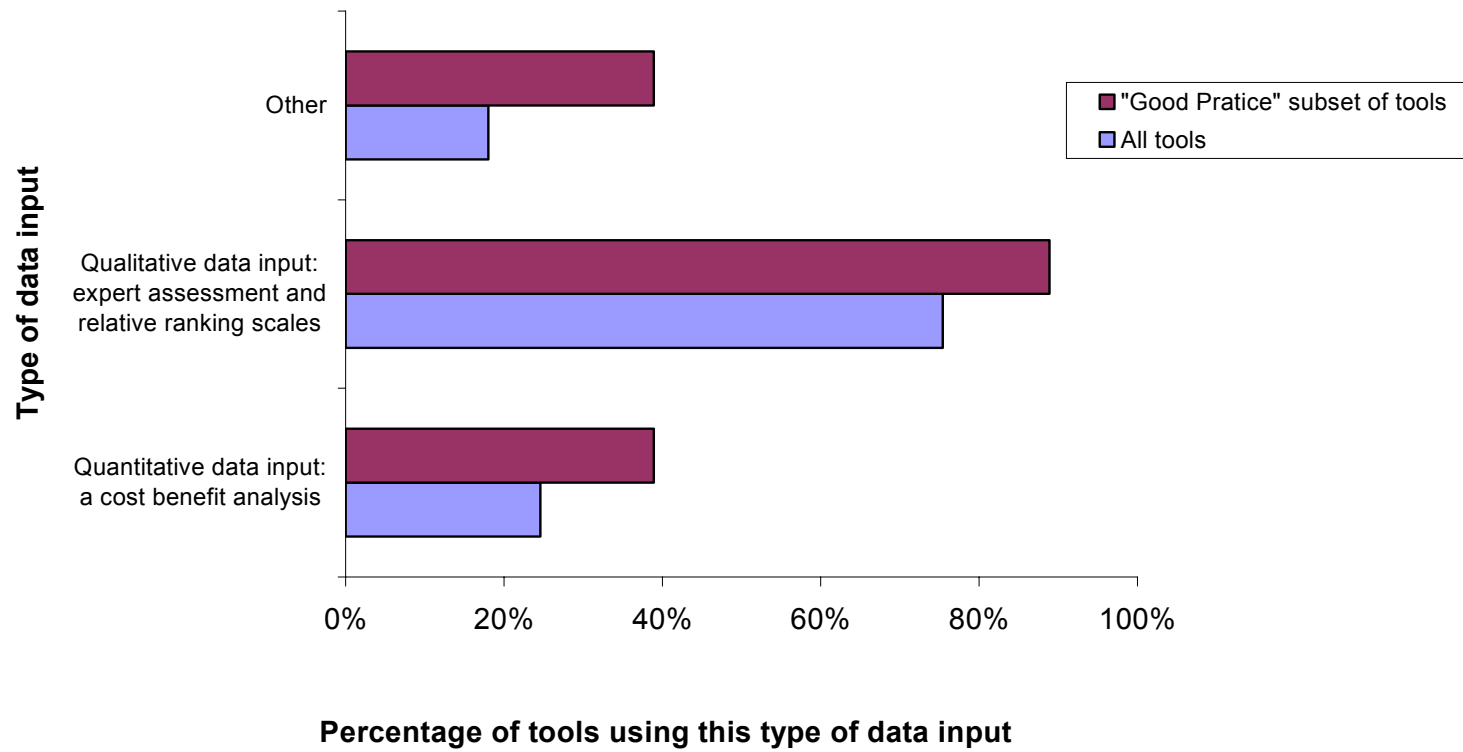


Figure 8

Tool Design: Output from execution of the tool.

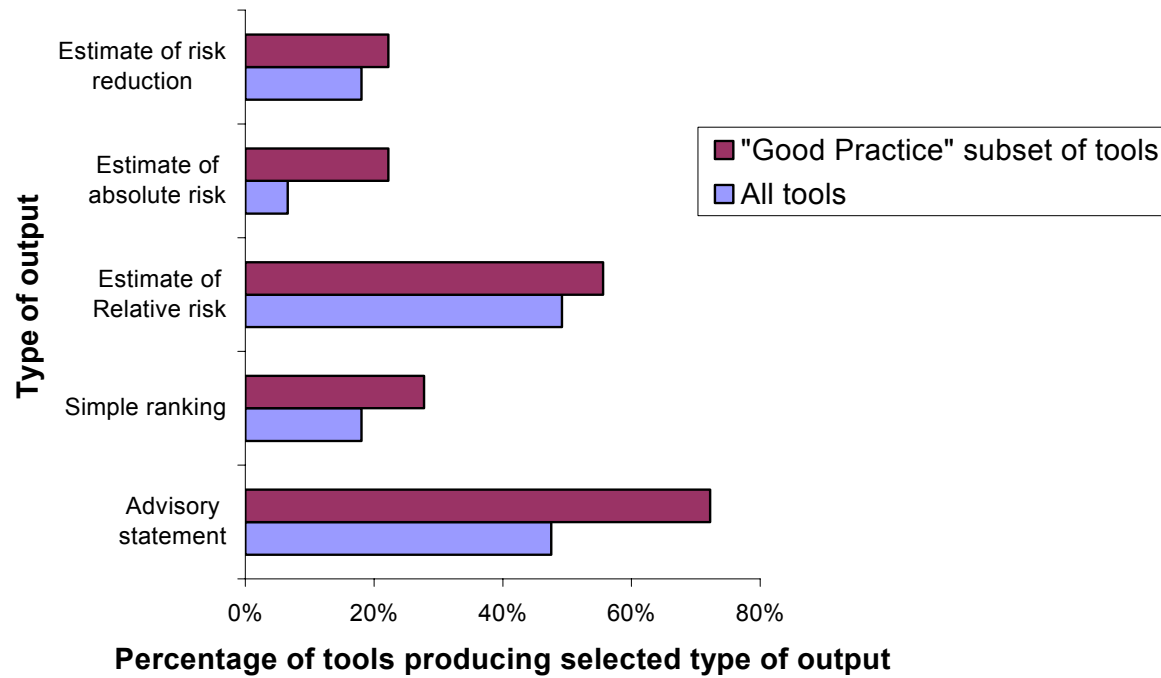


Figure 9

Tool Design: Estimated time frame for completion or implementation of the tool

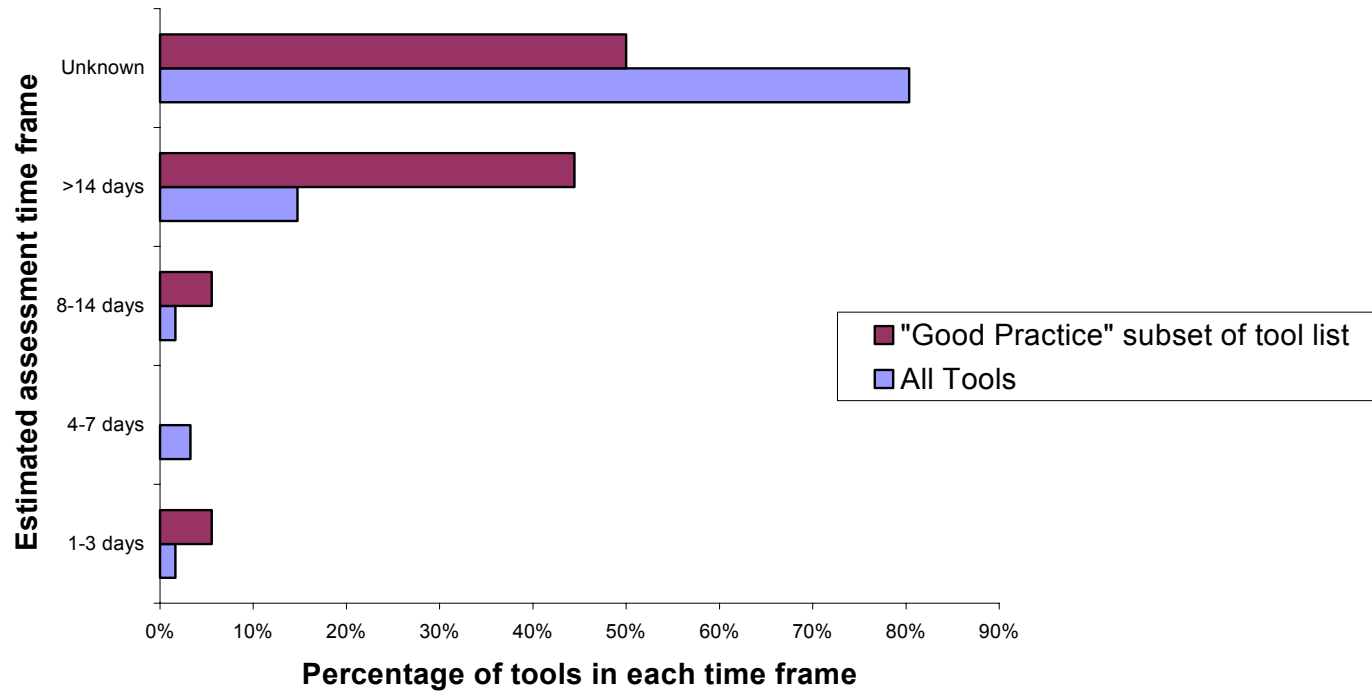


Figure 10

Tool Design: Estimated cost of completing or implementing the tool

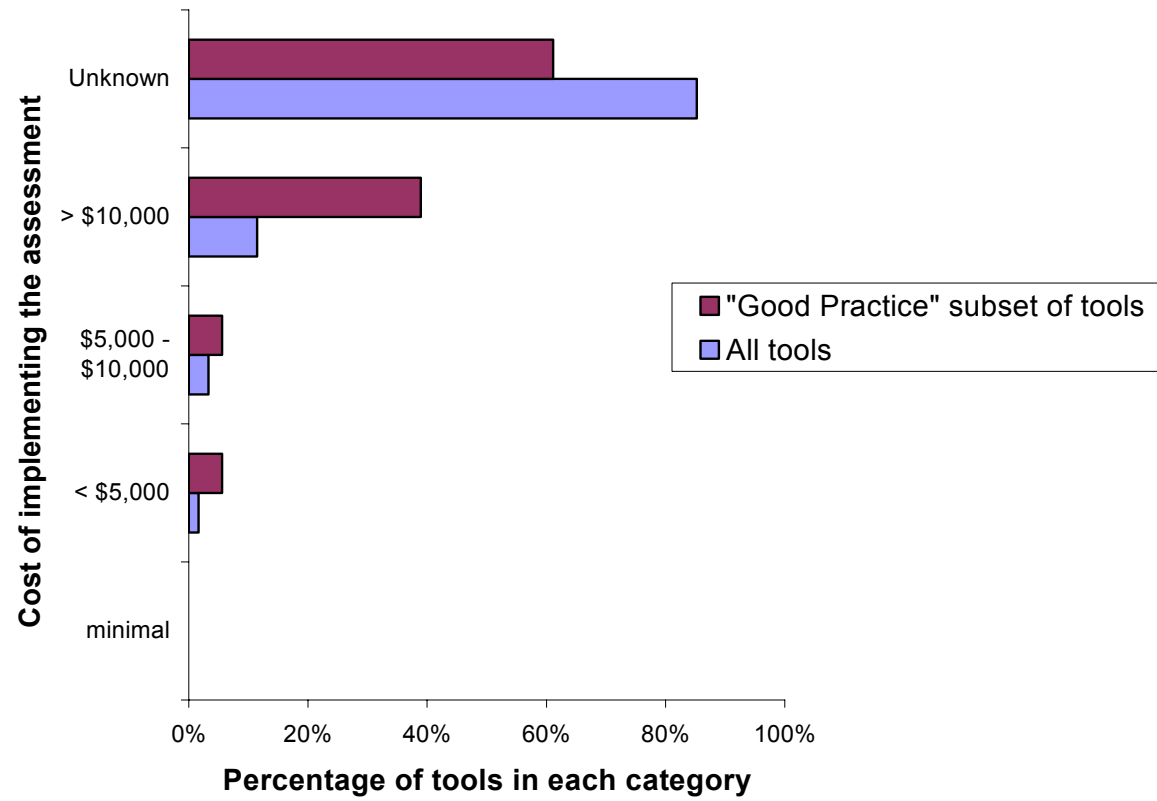


Figure 11

Tool Design: Who can the tool be used by?

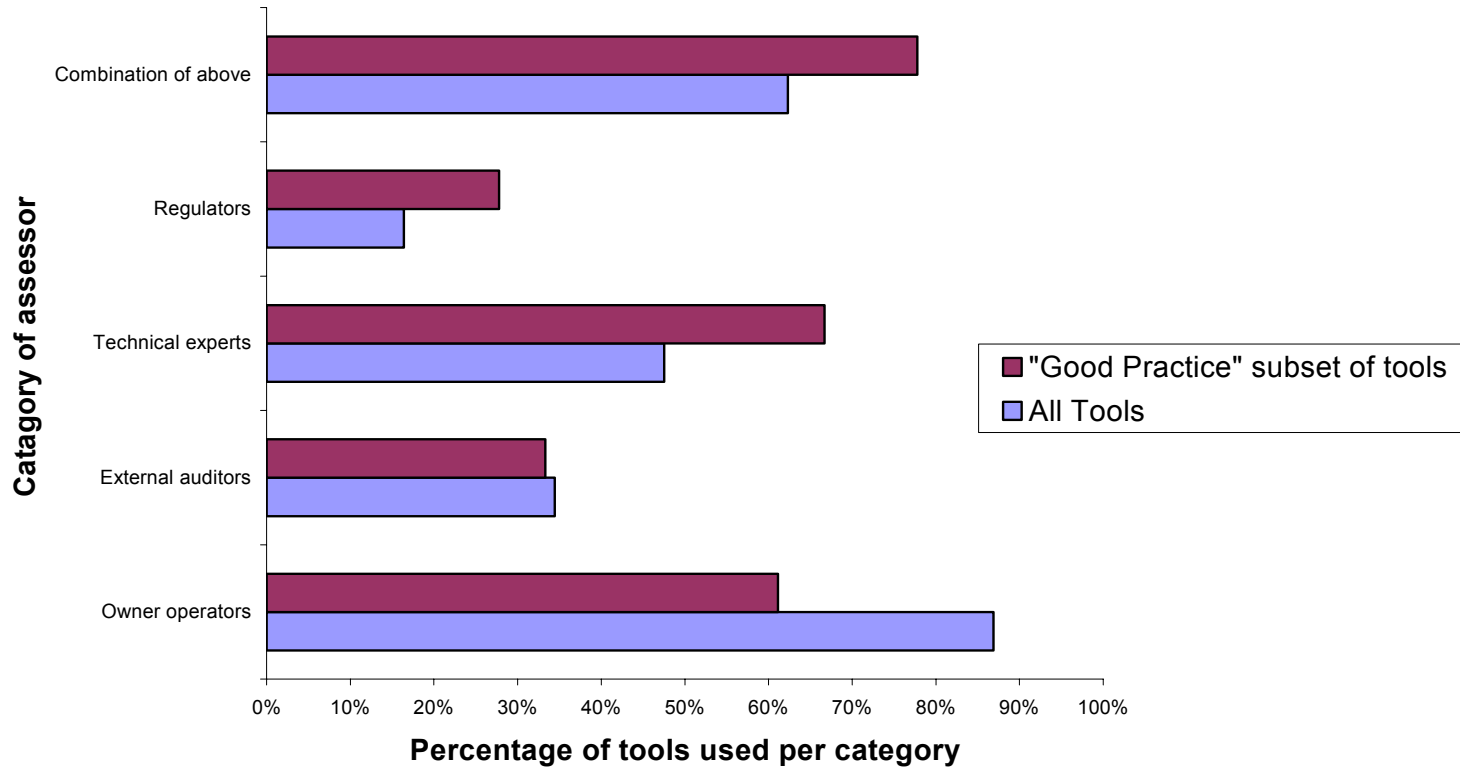


Figure 12

Level of maturity of the tool in its sector

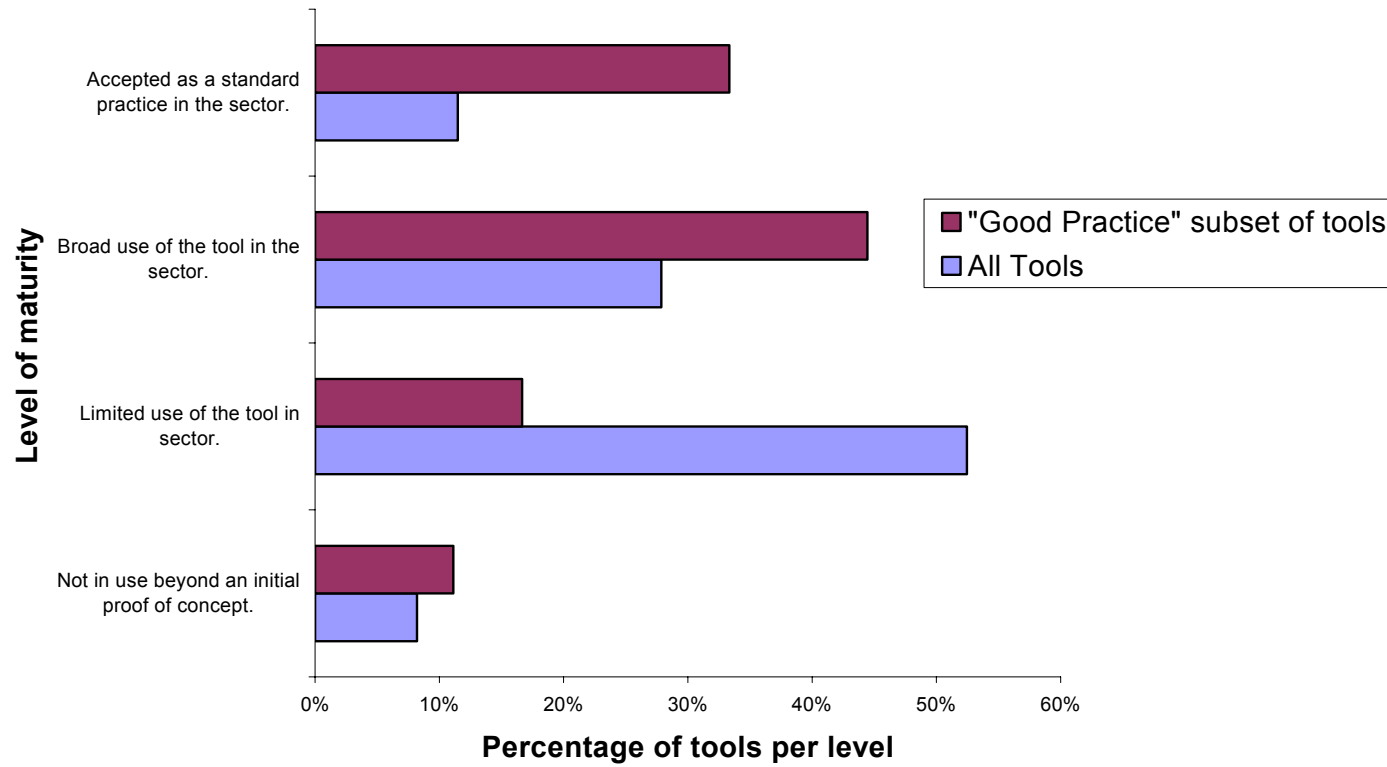


Figure 13

Is there a process for screening out low priority assets from further assessment?

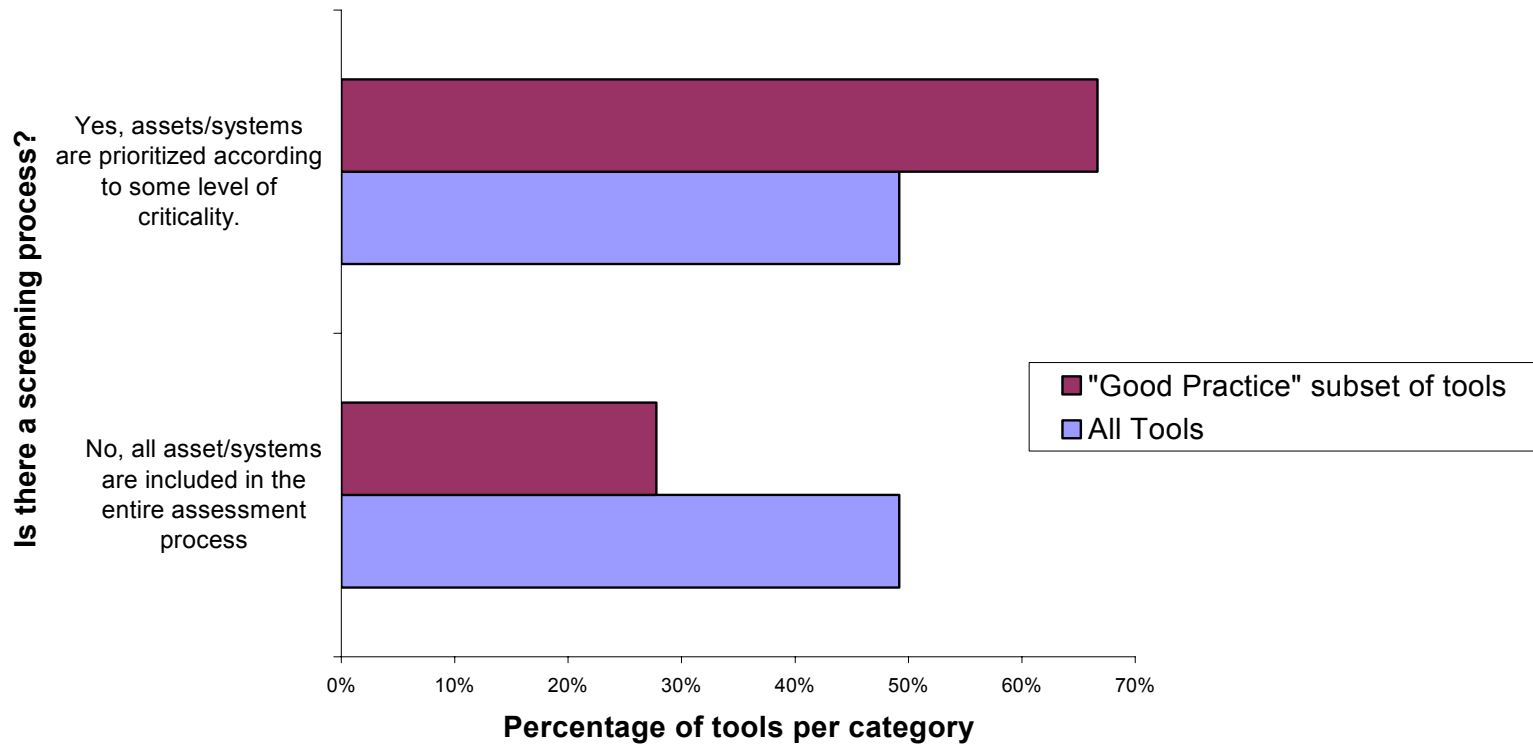


Figure 14

What type of Threats / Hazards does the tool address?

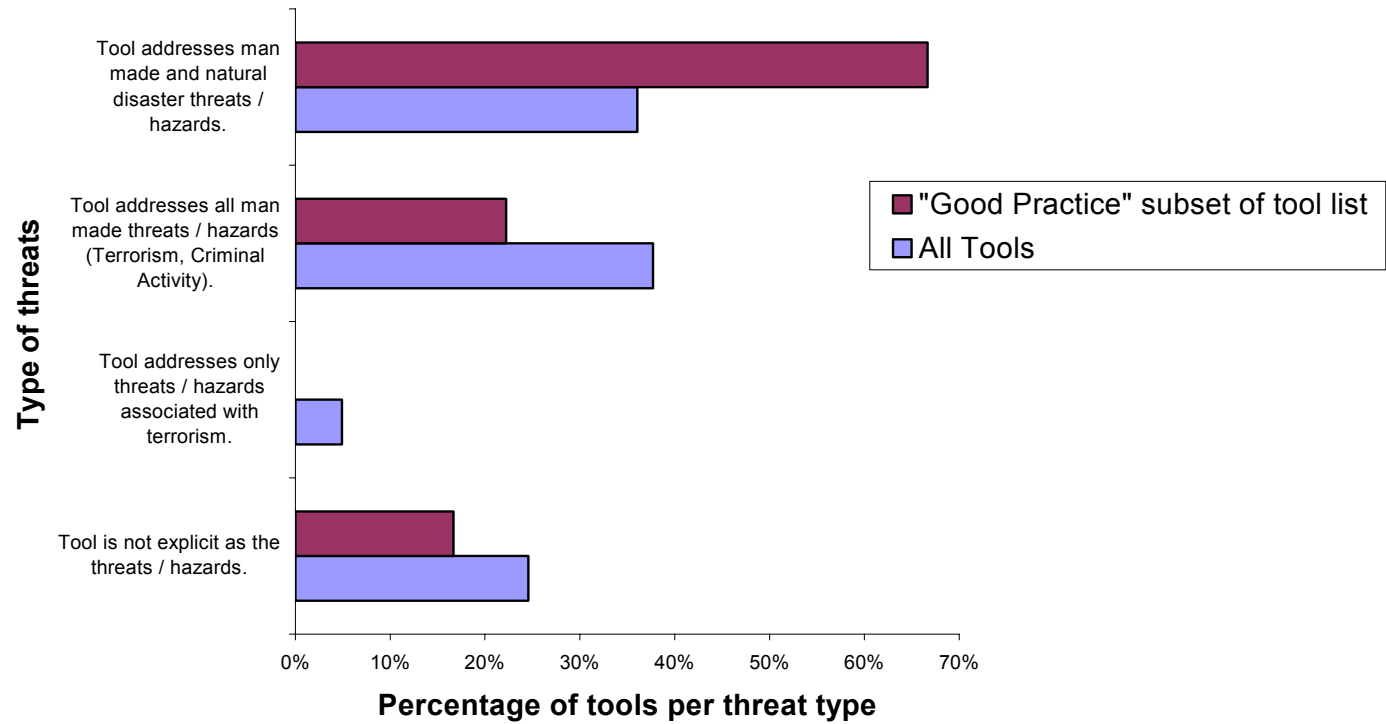


Figure 15

How are threats / hazards are quantified?

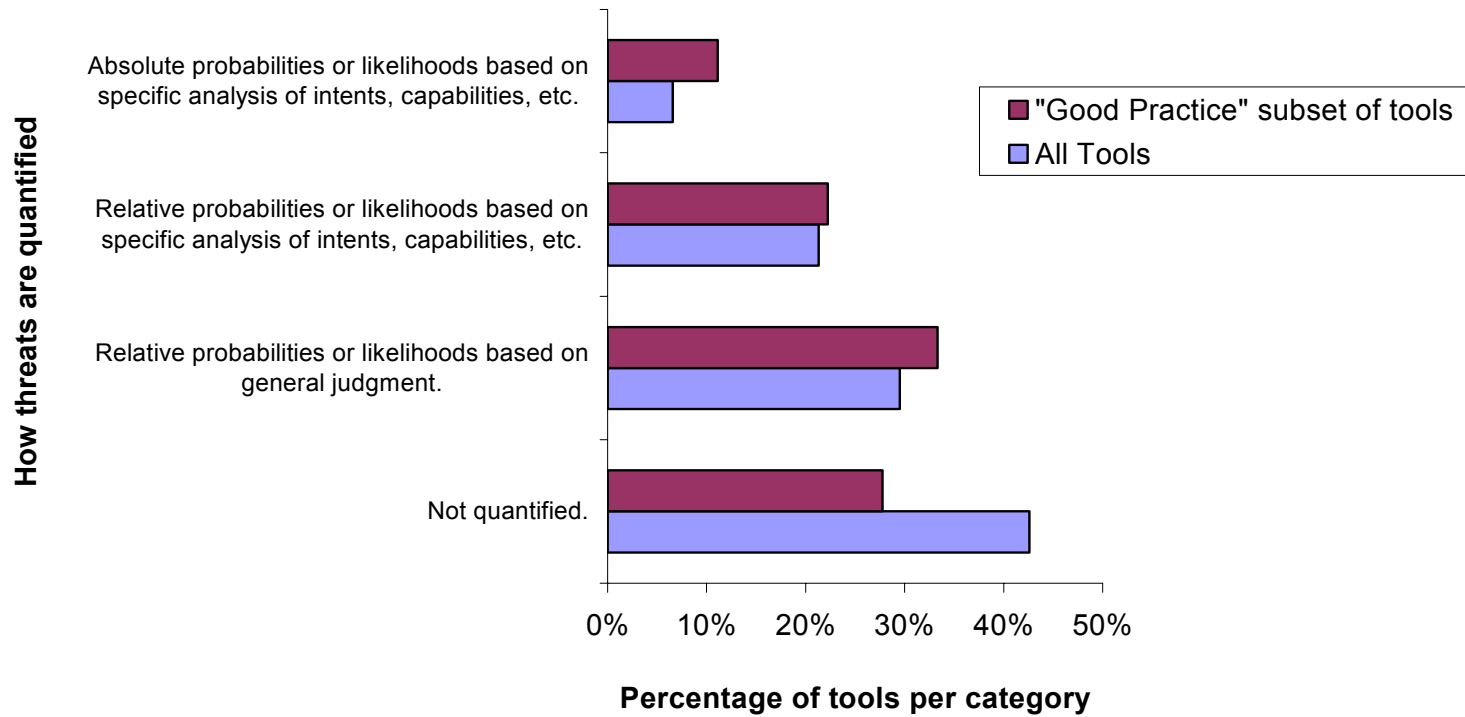


Figure 16

Does the analysis include contextual standards and from a systemic perspective?

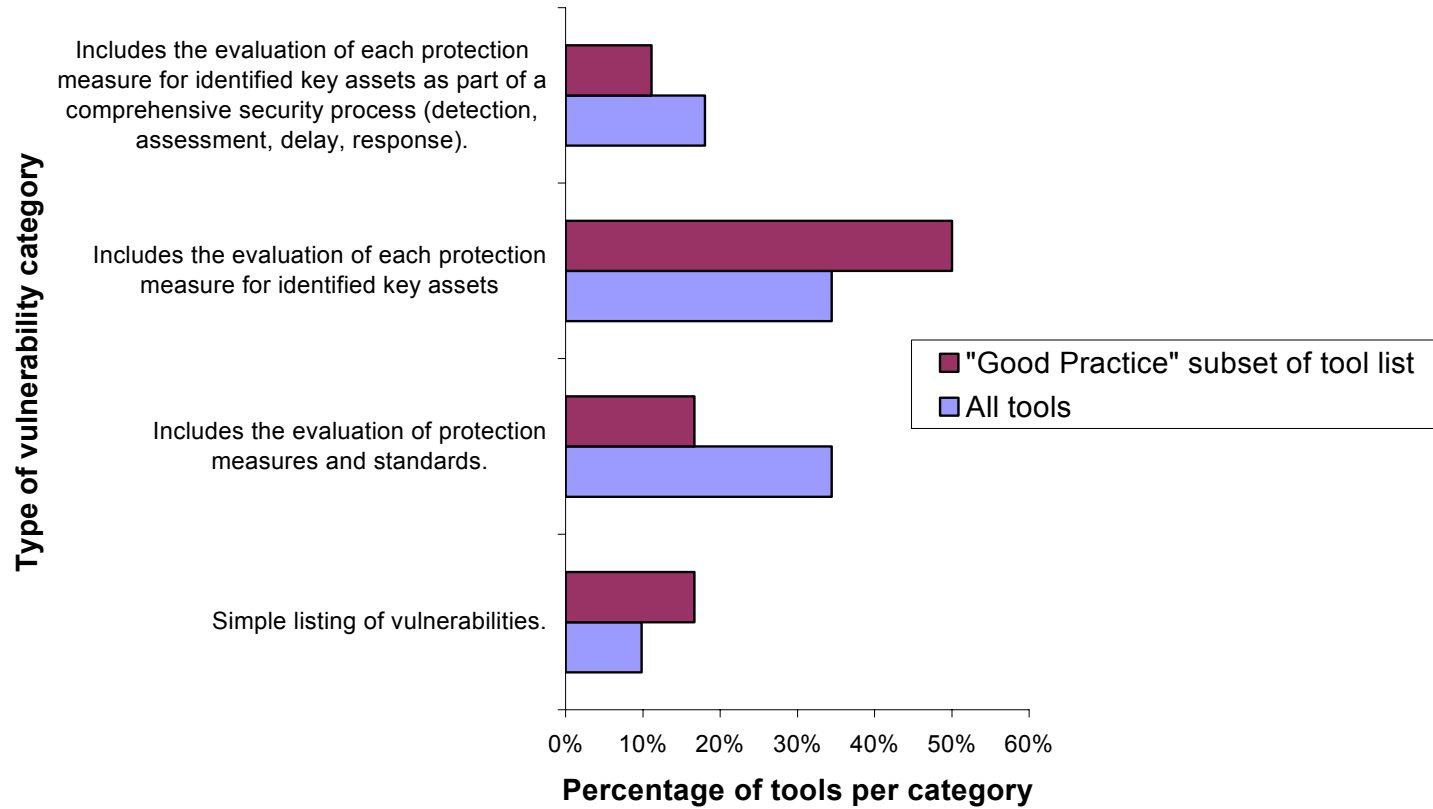


Figure 17

How are vulnerabilities quantified?

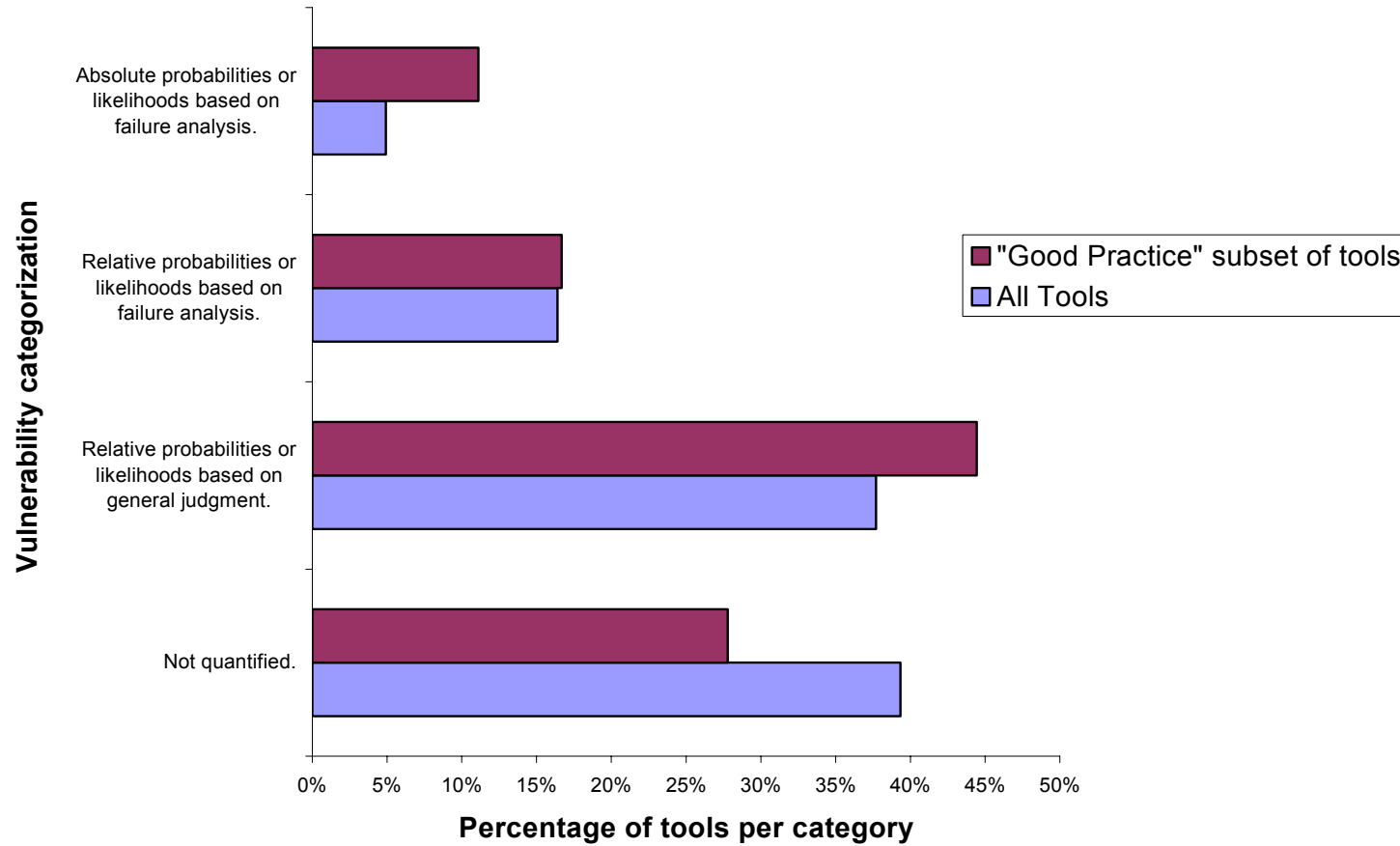


Figure 18

How are critical structures and functions identified?

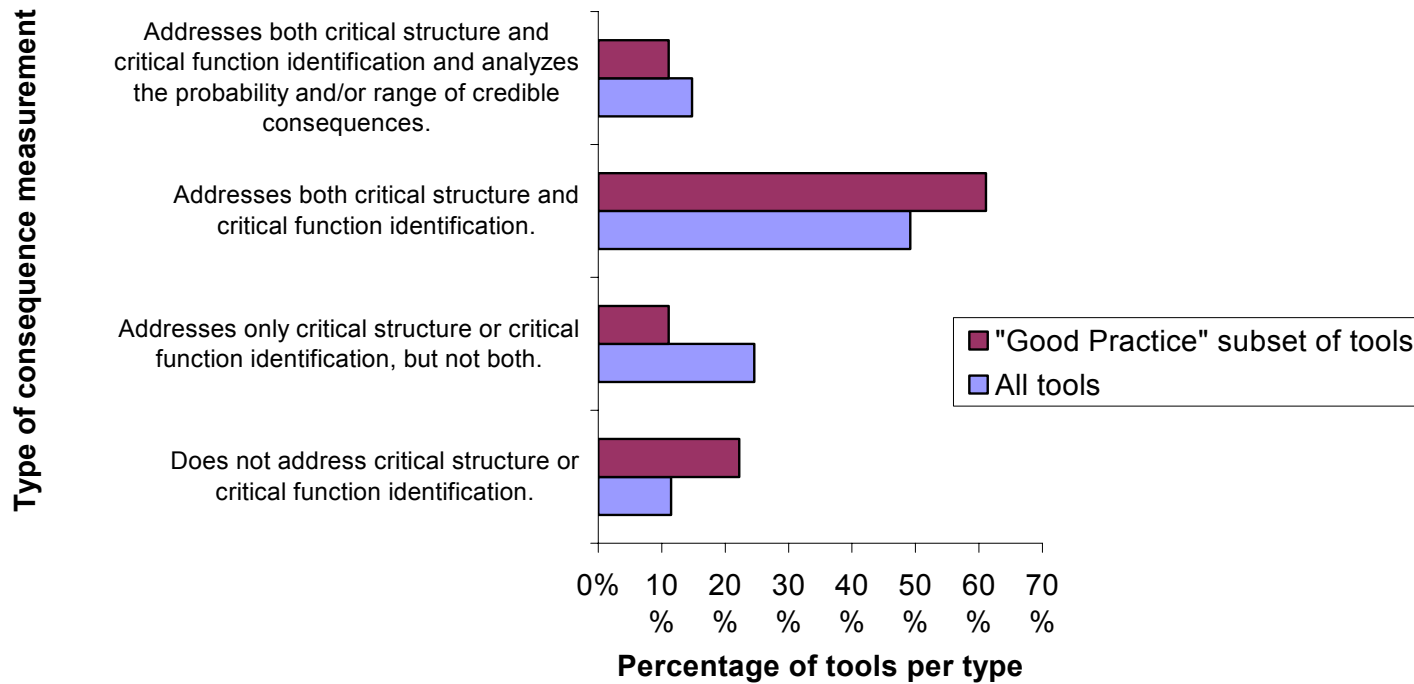
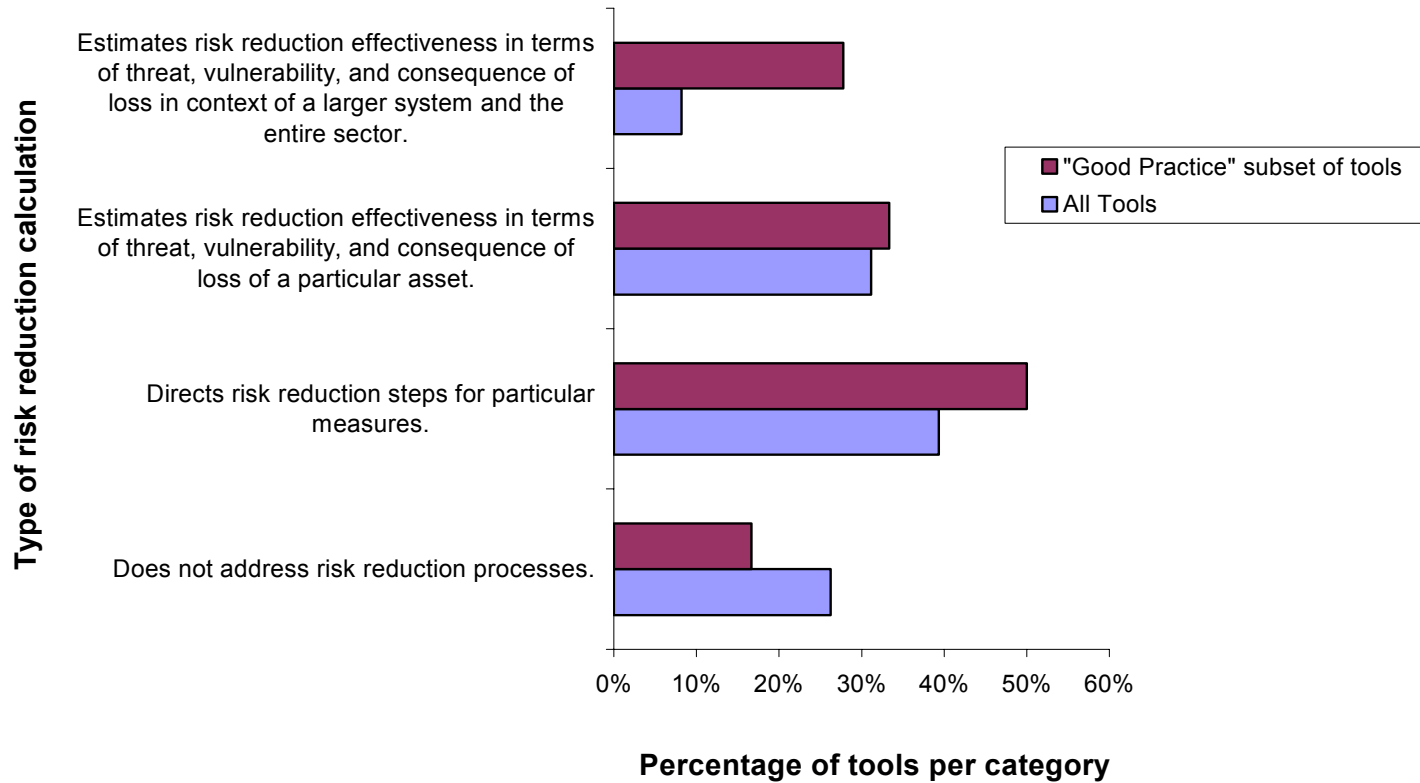


Figure 19

How are risk reduction and cost benefits determined?



Appendix A: Critical Infrastructure Analysis Matrix

Descriptive Section: The descriptive section of the matrix describes the assessment tools by subject, metric, and design:

1. Assessment Subject: What are the primary subjects the tool refers or applies to?

Sector: Check the specific sector(s) or industries the tool refers to, or if it is cross-sector

Asset: Check the types of assets included, e.g. facilities, equipment, materials, operations, or people

System: Does the tool address the interaction of multiple assets within a system?

Interdependencies: Check which, if any, upstream or downstream sectors are systematically included

2. Consequence Metric: What types of consequence or loss are addressed or measured?

Loss of Capacity/Output

Economic/Financial Loss

Environmental Degradation

Morbidity/Mortality

Other

3. Tool Design: What are the principle elements of the tool?

Format: The core of the tool mainly consists of e.g. descriptions, checklists, charts, or questionnaires

Input: Tool requires mainly quantitative or qualitative data input

Output: Tool execution results in e.g. probability assignment, ranking, or advisory

Time: Estimated time frame of completion or implementation of the tool

Cost: Estimated cost of completing or implementing the tool

Executor: Tool can be used by e.g. owners/operators, external auditors, technical experts, regulators

Analytic Section: The analytical section of the matrix characterizes the assessment tools by Maturity, Threat / Hazard, Consequence, Vulnerability, and Cost Benefit. The criteria range for each of these categories is listed below. They follow a continuum from a level of simple compliance, through a level of basic analytical risk reduction, to the final level of risk reduction by full economic optimization considering potential threat probabilities and consequences.

1. Maturity: What is the level of maturity of the CI-VA / RM Tool in its sector?

Type 1: Not in use beyond an initial proof of concept.

Type 2: Limited use of the tool in sector.

Type 3: Broad use of the tool in the sector.

Type 4: Accepted as a standard practice in the sector.

2. Criticality Screen: Is there a process of screening out low priority assets from further assessment?

Type 1: NO, all asset/systems are included in the entire assessment process

Type 2: YES, assets/systems are prioritized according to some level of criticality.

3a Threat / Hazard Types: What is the CI-VA / RM Tool Threats / Hazard approach?

Type 1: Tool is not explicit as the threats / hazards.

Type 2: Tool addresses only threats / hazards associated with terrorism.

Type 3: Tool addresses all man made threats / hazards (Terrorism, Criminal Activity).

Type 4: Tool addresses man made and natural disaster threats / hazards.

3b. Threat / Hazard Quantification: Are threats / hazards quantified?

Type 1: Not quantified.

Type 2: Relative probabilities or likelihoods based on general judgment.

Type 3: Relative probabilities or likelihoods based on specific analysis of intents, capabilities, etc.

Type 4: Absolute probabilities or likelihoods based on specific analysis of intents, capabilities, etc.

4a. Vulnerability Types: Does CI-VA / RM Tool conduct a Vulnerability Analysis with contextual standards and from a systemic perspective?

Type 1: Not specific as to vulnerabilities.

Type 2: Simple listing of vulnerabilities.

Type 3: Includes the evaluation of protection measures and standards.

Type 4: Includes the evaluation of each protection measure for identified key assets as part of a comprehensive security process (detection, assessment, delay, response).

4b. Vulnerability Quantification: Are vulnerabilities quantified?

Type 1: Not quantified.

Type 2: Relative probabilities or likelihoods based on general judgment.

Type 3: Relative probabilities or likelihoods based on failure analysis.

Type 4: Absolute probabilities or likelihoods based on failure analysis.

5. Consequence: Does the CI-VA / RM Tool identify *critical structures* (such as utility systems, mechanical systems, fire alarm system, wall& window design, roofing system, structural system, security systems and site layout) and/or *critical functions* (i.e., primary services or outputs and the critical activities that take place at the site)

Type 1: Tool does not address critical structure or critical function identification.
Type 2: Tool addresses only critical structure or critical function identification, but not both.
Type 3: Tool addresses both critical structure and critical function identification.
Type 4: Tool addresses both critical structure and critical function identification and analyzes the probability, uncertainty, and/or range of credible consequences.

6. Risk Reduction: Does the CI-VA / RM Tool determine risk reduction and cost benefit of mitigation?

Type 1: Tool does not address risk reduction processes.
Type 2: Tool directs risk reduction steps for particular measures.
Type 3: Tool estimates risk reduction effectiveness in terms of threat, vulnerability, and consequence of loss of a particular asset.
Type 4: Tool estimates risk reduction effectiveness in terms of threat, vulnerability, and consequence of loss in context of a larger system and the entire sector.

Appendix B: Assessment Tool Analysis Matrix Summary

Assessment Tool

Question	Range of Replies	Total number of tools evaluated	Percentage of All tools	Number of "Good Practice" subset of tools evaluated	Percentage of "Good Practice" subset of tool list
Descriptive Section		61		18	
1. Assessment Subject: What are the primary subjects the tool refers or applies to?		<u>Sum</u>	%	<u>Sum</u>	%
1.a. Sector: Check the specific sector(s) or industries the tool is designed to assess.					
	Banking & Finance	6	10%	3	17%
	Chemical	7	11%	2	11%
	Energy (Except Nuclear Power)	4	7%	1	6%
	Electricity	7	11%	2	11%
	Oil & Gas	4	7%	2	11%
	Emergency Services	9	15%	6	33%
	Information Technology	8	13%	0	0%
	Telecommunications	11	18%	4	22%
	Postal & Shipping	0	0%	0	0%
	Public Health	6	10%	4	22%
	Transportation	6	10%	3	17%
	Water	9	15%	2	11%
	National Monuments & Icons	1	2%	1	6%
	Commercial Facilities	4	7%	2	11%
	Government Facilities	5	8%	2	11%
	Dams	0	0%	0	0%
	All	5	8%	1	6%
1.b. Asset: Check the types of assets included					
	Buildings	38	62%	12	67%
	Facilities	47	77%	16	89%
	Equipment	48	79%	14	78%
	Materials	26	43%	11	61%
	Operations	47	77%	17	94%
	People	28	46%	15	83%
	Other	13	21%	12	67%
1.c. System: Does the tool address the interaction of multiple assets within a system?			0%		
	Yes	40	66%	17	94%
	No	22	36%	2	11%
1.d. Interdependencies: Check which, if any, upstream or downstream sectors are included systematically					
	All	3	5%	2	11%
	Only Dependent Utilities and Communication	31	51%	9	50%
	Banking & Finance	11	18%	7	39%
	Chemical	5	8%	3	17%
	Energy (Except Nuclear Power)	6	10%	1	6%
	Electricity	13	21%	6	33%
	Oil & Gas	8	13%	2	11%

Assessment Tool

Question	Range of Replies	Total number of tools evaluated	Percentage of All tools	Number of "Good Practice" subset of tools evaluated	Percentage of "Good Practice" subset of tool list
Descriptive Section		61		18	
	Emergency Services	12	20%	8	44%
	Information Technology	22	36%	7	39%
	Telecommunications	19	31%	8	44%
	Postal & Shipping	2	3%	2	11%
	Public Health	3	5%	3	17%
	Transportation	11	18%	3	17%
	Water	9	15%	1	6%
	National Monuments & Icons	1	2%	1	6%
	Commercial Facilities	5	8%	5	28%
	Government Facilities	5	8%	5	28%
	Dams	0	0%	0	0%
2. Consequence Metric: What types of consequence or loss are addressed or measured?					
2.a Loss of Capacity/Output (not in financial terms)					
	Check if yes, blank if no	49	80%	16	89%
2.b Economic/Financial Loss					
	Check if yes, blank if no	40	66%	11	61%
2.c. Environmental Degradation					
	Check if yes, blank if no	12	20%	5	28%
2.d. Morbidity/Mortality					
	Check if yes, blank if no	23	38%	10	56%
2.e. Other					
	Check if yes, blank if no	16	26%	12	67%
3. Tool Design: What are the principle elements of the tool?					
3.a. Format: Check the item(s) that make up the core of the tool.					
	Descriptions	29	48%	16	89%
	Checklists	36	59%	16	89%
	Charts	8	13%	7	39%
	Questionnaires	24	39%	10	56%
	Other	10	16%	10	56%
3.b. Input: Indicate the main type of data input					
	Quantitative data input: a cost benefit analysis	15	25%	7	39%
	Qualitative data input: expert assessment and relative ranking scales	46	75%	16	89%
	Other	11	18%	7	39%
3.c. Output: Indicate the output from the execution of the tool.					
	Advisory statement	29	48%	13	72%
	Simple ranking	11	18%	5	28%
	Estimate of Relative risk	30	49%	10	56%
	Estimate of absolute risk	4	7%	4	22%
	Estimate of risk reduction	11	18%	4	22%

Assessment Tool

Question	Range of Replies	Total number of tools evaluated	Percentage of All tools	Number of "Good Practice" subset of tools evaluated	Percentage of "Good Practice" subset of tool list
<u>Descriptive Section</u>		61		18	
3.e. Cost: Estimated cost of completing or implementing the tool					
	1-3 days	1	2%	1	6%
	4-7 days	2	3%	0	0%
	8-14 days	1	2%	1	6%
	>14 days	9	15%	8	44%
	Unknown	49	80%	9	50%
3.e. Cost: Estimated cost of completing or implementing the tool					
	minimal	0	0%	0	0%
	< \$5,000	1	2%	1	6%
	\$5,000 - \$10,000	2	3%	1	6%
	> \$10,000	7	11%	7	39%
	Unknown	52	85%	11	61%
3.f. Executor: Tool can be used by e.g. owners/operators, external auditors, technical experts, regulators					
	Owner operators	53	87%	11	61%
	External auditors	21	34%	6	33%
	Technical experts	29	48%	12	67%
	Regulators	10	16%	5	28%
	Combination of above	38	62%	14	78%
<u>Analytic Section</u>					
1. Maturity: What is the level of maturity of the CI-VA / RM Tool in its sector?					
	Not in use beyond an initial proof of concept.	5	8%	2	11%
	Limited use of the tool in sector.	32	52%	3	17%
	Broad use of the tool in the sector.	17	28%	8	44%
	Accepted as a standard practice in the sector.	7	11%	6	33%
2. Criticality Screen: Is there a process of screening out low priority assets from further assessment?					
	No, all asset/systems are included in the entire assessment process	30	49%	5	28%
	Yes, assets/systems are prioritized according to some level of criticality.	30	49%	12	67%
3a Threat / Hazard Types:					
3.a. What is the CI-VA / RM Tool Threats / Hazard approach?					
	Tool is not explicit as the threats / hazards.	15	25%	3	17%
	Tool addresses only threats / hazards associated with	3	5%	0	0%
	Tool addresses all man made threats / hazards (Terrorism, Criminal Activity).	23	38%	4	22%

Assessment Tool

Question	Range of Replies	Total number of tools evaluated	Percentage of All tools	Number of "Good Practice" subset of tools evaluated	Percentage of "Good Practice" subset of tool list
Descriptive Section		61		18	
	Tool addresses man made and natural disaster threats /	22	36%	12	67%
3b. Threat / Hazard Quantification: Are threats / hazards					
	Not quantified.	26	43%	5	28%
	Relative probabilities or likelihoods based on general	18	30%	6	33%
	Relative probabilities or likelihoods based on specific analysis of intents, capabilities, etc.	13	21%	4	22%
	Absolute probabilities or likelihoods based on specific analysis of intents, capabilities, etc.	4	7%	2	11%
4a. Vulnerability Types:					
4a. Does CI-VA / RM Tool conduct a Vulnerability Analysis with contextual standards and from a systemic perspective?					
	Simple listing of vulnerabilities.	6	10%	3	17%
	Includes the evaluation of protection measures and standards.	21	34%	3	17%
	Includes the evaluation of each protection measure for identified key assets	21	34%	9	50%
	Includes the evaluation of each protection measure for identified key assets as part of a comprehensive security process (detection, assessment, delay, response).	11	18%	2	11%
4b. Vulnerability Quantification: Are vulnerabilities quantified?					
	Not quantified.	24	39%	5	28%
	Relative probabilities or likelihoods based on general	23	38%	8	44%
	Relative probabilities or likelihoods based on failure analysis.	10	16%	3	17%
	Absolute probabilities or likelihoods based on failure analysis.	3	5%	2	11%
5. Consequence: Does the CI-VA / RM Tool identify critical structures (such as utility systems, mechanical systems, fire alarm system, wall& window design, roofing system, structural system, security systems and site layout) and/or critical functions (i.e., primary services or outputs and the critical activities that take place at the site)					
	Does not address critical structure or critical function identification.	7	11%	4	22%
	Addresses only critical structure or critical function identification, but not both.	15	25%	2	11%

Assessment Tool

Question	Range of Replies
----------	------------------

Descriptive Section	
Addresses both critical structure and critical function identification.	
Addresses both critical structure and critical function identification and analyzes the probability and/or range of credible consequences.	

6. Risk Reduction: Does the CI-VA / RM Tool determine risk reduction and cost benefit of mitigation?

Does not address risk reduction processes.	
Directs risk reduction steps for particular measures.	
Estimates risk reduction effectiveness in terms of threat, vulnerability, and consequence of loss of a particular asset.	
Estimates risk reduction effectiveness in terms of threat, vulnerability, and consequence of loss in context of a larger system and the entire sector.	

Total number of tools evaluated	Percentage of All tools	Number of "Good Practice" subset of tools evaluated	Percentage of "Good Practice" subset of tool list
61		18	
30	49%	11	61%
9	15%	2	11%
16	26%	3	17%
24	39%	9	50%
19	31%	6	33%
5	8%	5	28%

Appendix C: Assessment Tool Analysis Matrix

Question	Range of Replies
Assessment Tool	USCG, Outer Continental Shelf Facility Security Plans Review DOJ, Department of Justice Standards for Protection of Federal Facilities AMSA, Asset Based Vulnerability Checklist for Wastewater Utilities DOJ, NIJ Special report: A Method to Assess the Vulnerability of U.S. Chemical Facilities National Environmental Training Center, Protecting Your Community's Assets: A Guide for Small Wastewater Systems EPA, Protect Your Water For Life: Vulnerability Assessment Fact sheet DOE, Vulnerability Assessment Methodology, Electric Power Infrastructure Dept. of Veterans Affairs, Physical Security Assessment for Department of Veterans Affairs Facilities NERC, Security Guidelines for the Electricity Sector

Descriptive Section

1. Assessment Subject: What are the primary subjects the tool refers or applies to?

1.a. Sector: Check the specific sector(s) or industries the tool is designed to assess.

Banking & Finance									
Chemical				x					
Energy (Except Nuclear Power)	x								
Electricity							x		x
Oil & Gas									
Emergency Services									
Information Technology									
Telecommunications									
Postal & Shipping									
Public Health								x	
Transportation									
Water			x		x	x			
National Monuments & Icons									
Commercial Facilities									
Government Facilities		x							
Dams									
All									

1.b. Asset: Check the types of assets included

Buildings		x	x	x	x	x	x	x	x
Facilities	x	x	x	x	x	x	x	x	x
Equipment	x		x	x	x	x	x	x	x
Materials				x	x			x	
Operations	x	x	x	x			x	x	
People	x	x	x					x	
Other									

Question	Range of Replies
Assessment Tool	American Chemistry Council, Transportation Security Guidelines for the US Chemical Industry AASHTO, A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection American Chemistry Council, Site Security Guidelines for the US NIST, Pub 800-26 Security Self-Assessment Guide for Information Technology Systems DOJ, Assessment and Strategy Development Tool Kit CIAO, Vulnerability Assessment Framework 1.1 DoD, Physical Security Evaluation Guide NPRA, Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries BITS, Framework for Managing Technology Risk for IT Service Provider Relationships BITS, Calculator: BITS Key Risk Measurement Tool for Information Security Operational Risks

Descriptive Section

1. Assessment Subject: What are the primary subjects the tool refers or applies to?

1.a. Sector: Check the specific sector(s) or industries the tool is designed to assess.

Banking & Finance					X					
Chemical	X		X		X			X		
Energy (Except Nuclear Power)					X					
Electricity					X					
Oil & Gas					X					
Emergency Services					X					
Information Technology					X					
Telecommunications				X	X				X	X
Postal & Shipping										
Public Health					X					
Transportation		X			X					
Water					X					
National Monuments & Icons										
Commercial Facilities					X					
Government Facilities							X			
Dams										
All						X				

1.b. Asset: Check the types of assets included

Buildings		X	X		X	X	X	X		
Facilities		X	X		X	X	X	X		
Equipment		X	X	X		X		X	X	X
Materials	X		X				X	X		
Operations						X		X	X	X
People		X	X		X	X		X		
Other				X						

Assessment Tool	FEMA, Emergency Management Guide for Business and Industry	NFPA 1600, Standard on Disaster / Emergency Management and Business Continuity Programs, 2004 Edition	FFIEC, Operations, IT Examination Handbook	FFIEC, Information Security, IT Examination Handbook	FFIEC, Management, IT Examination Handbook	NCS, Public Switched Network Assessment Guidelines	NCS, The Electronic intrusion threat to national Security and Emergency Preparedness (NS/EP) Internet Communications	NISCC, Good Practice Guide, Telecommunications Resilience	DOE, Energy Infrastructures Risk Management Checklists for Small and Medium Sized Energy Facilities	AWWA, Interim Voluntary Security Guidance for Water Utilities, December 9, 2004
-----------------	--	---	--	--	--	--	--	---	---	---

Question Range of Replies

Descriptive Section

1. Assessment Subject: What are the primary subjects the tool refers or applies to?

1.a. Sector: Check the specific sector(s) or industries the tool is designed to assess.

Banking & Finance										
Chemical										
Energy (Except Nuclear Power)										
Electricity									x	
Oil & Gas										
Emergency Services	x	x								
Information Technology			x	x	x		x			
Telecommunications						x		x		
Postal & Shipping										
Public Health										
Transportation										
Water										x
National Monuments & Icons										
Commercial Facilities										
Government Facilities										
Dams										
All										

1.b. Asset: Check the types of assets included

Buildings	x	x							x	x
Facilities		x							x	x
Equipment			x	x		x	x	x	x	x
Materials										x
Operations			x	x	x	x	x	x	x	
People										
Other										

Question	Range of Replies	Assessment Tool							
		AWWA, Interim Voluntary Security Guidance for Wastewater / Storm water Utilities, December 9, 2004							
		ASDWA/NRWA, Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems Serving Populations Between 3,300 and 10,000, November 13, 2002							
		ASIS, Business Continuity Guideline, 01 2005							
		BITS, BITS Guide to Business-Critical Telecommunications Services, November 2004							
		Compendium of Supporting Documents to the National Strategy for Critical Infrastructure Assurance Version 1.0, May 13, 2002.							
		DOE, Energy Infrastructures Risk Assessment Checklists for State Governments, December 4, 2001							
		EOC Checklist							
		NIST SP800-53, Recommended Security Controls for Federal Information Systems, February 2005							
		USCG, Navigation and Vessel Inspection Circular NO. 05 03, December 15, 2003							

Descriptive Section

1. Assessment Subject: What are the primary subjects the tool refers or applies to?

1.a. Sector: Check the specific sector(s) or industries the tool is designed to assess.

Banking & Finance					X				
Chemical									
Energy (Except Nuclear Power)						X			
Electricity						X			
Oil & Gas						X			
Emergency Services									
Information Technology								X	
Telecommunications					X				
Postal & Shipping									
Public Health									
Transportation									X
Water	X	X							
National Monuments & Icons									
Commercial Facilities								X	
Government Facilities								X	
Dams									
All				X					

1.b. Asset: Check the types of assets included

Buildings	X	X		X					
Facilities	X	X		X	X	X	X	X	X
Equipment	X	X		X	X	X	X	X	X
Materials					X	X	X		X
Operations	X	X	X	X	X	X	X	X	X
People					X	X			X
Other									

Question	Range of Replies
Assessment Tool	RAND, Finding and Fixing Vulnerabilities in Information Systems, The Vulnerability Assessment and Mitigation Methodology, 2003
	Securities Industry Association, Business Continuity Planning Committee Critical Infrastructure Guide
	BITS ITSP Expectations Matrix
	ODP, State Homeland Security Assessment and Strategy Program, Special Needs Jurisdiction Tool Kit
	Risk Analysis and management for Critical Asset Protection (RAMCAP™)
	DHS, Target Capability List
	Commission on Accreditation for Law Enforcement Agencies (CALEA)
	Emergency Management Accreditation Program (EMAP)
	National Incident Management System (NIMS)
	Sandia National Labs, Risk Assessment Methodology for Water (RAM-W)

Descriptive Section

1. Assessment Subject: What are the primary subjects the tool refers or applies to?

1.a. Sector: Check the specific sector(s) or industries the tool is designed to assess.

Banking & Finance		x								
Chemical										
Energy (Except Nuclear Power)										
Electricity										
Oil & Gas										
Emergency Services						x	x	x	x	
Information Technology	x			x						
Telecommunications						x				
Postal & Shipping										
Public Health						x				
Transportation										
Water										x
National Monuments & Icons						x				
Commercial Facilities						x				
Government Facilities						x				
Dams										
All					x	x				

1.b. Asset: Check the types of assets included

Buildings	x	x	x	x	x	x				x
Facilities	x	x	x	x	x	x		x	x	x
Equipment		x	x	x	x	x			x	x
Materials			x	x	x	x		x	x	x
Operations	x	x	x		x	x	x	x	x	x
People					x	x	x		x	x
Other						x	x	x	x	x

Question	Range of Replies	The Vulnerability Self Assessment Tool™ (VSAT) for Water & Wastewater Utilities	FEMA, Reference Manual to Mitigate Terrorist Attacks Against Buildings	Kaiser Center Hazard and Vulnerability Analysis	NCR Healthcare Organization Guided Vulnerabilities Assessment and Preparedness Planning	Media Security and Reliability Council (MSRC) Adopted Best Practices Recommendations	NRIC Best Practice	National Security Telecommunications Advisory Committee (NSTAC) Reports	FFIEC Guidelines, BITS studies and recommendations for IT security	Banking and Financial Regulatory and Supervisory Oversight	General Industry Practices - Trade Associations National, State, Regional	Loudon County: Hazard Identification and Risk Analysis
		<i>"Good Practice" tools</i>										

Descriptive Section

1. Assessment Subject: What are the primary subjects the tool refers or applies to?

1.a. Sector: Check the specific sector(s) or industries the tool is designed to assess.

Banking & Finance									X	X	X	
Chemical												X
Energy (Except Nuclear Power)											X	
Electricity											X	X
Oil & Gas												X
Emergency Services											X	X
Information Technology												
Telecommunications						X	X	X				
Postal & Shipping												
Public Health				X	X							X
Transportation												X
Water	X											
National Monuments & Icons												
Commercial Facilities												X
Government Facilities												X
Dams												
All			X									

1.b. Asset: Check the types of assets included

Buildings	X	X	X				X		X	X	X	X
Facilities	X	X	X				X	X	X	X	X	X
Equipment	X	X	X			X	X		X	X	X	
Materials	X		X						X	X	X	
Operations	X		X	X	X	X	X	X	X	X	X	
People	X		X	X			X		X	X	X	X
Other	X					X	X	X	X	X	X	

Assessment Tool	American Petroleum Industries: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries ODP: Special Needs Jurisdiction Tool Kit Ohio DOT: Guide to conducting Critical Asset Protection Self Assessments
Question	Range of Replies

Descriptive Section

1. Assessment Subject: What are the primary subjects the tool refers or applies to?

1.a. Sector: Check the specific sector(s) or industries the tool is designed to assess.

Banking & Finance			
Chemical	x		
Energy (Except Nuclear Power)			
Electricity			
Oil & Gas	x		
Emergency Services			
Information Technology			
Telecommunications			
Postal & Shipping			
Public Health			
Transportation		x	x
Water			
National Monuments & Icons			
Commercial Facilities			
Government Facilities			
Dams			
All			

1.b. Asset: Check the types of assets included

Buildings		x	x
Facilities	x	x	x
Equipment	x	x	x
Materials	x		x
Operations	x	x	x
People	x	x	x
Other			

Question	Range of Replies	Assessment Tool								
<u>Descriptive Section</u>										
		USCG, Outer Continental Shelf Facility Security Plans Review	DOJ, Department of Justice Standards for Protection of Federal Facilities	AMSA, Asset Based Vulnerability Checklist for Wastewater Utilities	DOJ, NIJ Special report: A Method to Assess the Vulnerability of U.S. Chemical Facilities	National Environmental Training Center, Protecting Your Community's Assets: A Guide for Small Wastewater Systems	EPA, Protect Your Water For Life: Vulnerability Assessment Fact sheet	DOE, Vulnerability Assessment Methodology, Electric Power Infrastructure	Dept. of Veterans Affairs, Physical Security Assessment for Department of Veterans Affairs Facilities	NERC, Security Guidelines for the Electricity Sector

1.c. System: Does the tool address the interaction of multiple assets within a system?

Yes	x		x				x		
No		x		x	x	x		x	x

1.d. Interdependencies: Check which, if any, upstream or downstream sectors are included systematically

All						x			
Only Dependent Utilities and Communication	x	x		x	x		x	x	x
Banking & Finance							x		x
Chemical							x		x
Energy (Except Nuclear Power)							x		x
Electricity							x		x
Oil & Gas							x		x
Emergency Services									
Information Technology							x		x
Telecommunications							x		x
Postal & Shipping									
Public Health									
Transportation							x		x
Water			x				x		x
National Monuments & Icons									
Commercial Facilities									
Government Facilities									
Dams									

2. Consequence Metric: What types of consequence or loss are addressed or measured?

2.a Loss of Capacity/Output (not in financial terms)

Assessment Tool	American Chemistry Council, Transportation Security Guidelines for the US Chemical Industry	AASHTO, A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection	American Chemistry Council, Site Security Guidelines for the US	NIST, Pub 800-26 Security Self-Assessment Guide for Information Technology Systems	DOJ, Assessment and Strategy Development Tool Kit	CIAO, Vulnerability Assessment Framework 1.1	DoD, Physical Security Evaluation Guide	NPRA, Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries	BITS, Framework for Managing Technology Risk for IT Service Provider Relationships	BITS, Calculator: BITS Key Risk Measurement Tool for Information Security Operational Risks
-----------------	---	--	---	--	---	--	---	--	--	---

Question **Range of Replies**

Descriptive Section

1.c. System: Does the tool address the interaction of multiple assets within a system?

Yes		X				X		X		
No	X		X	X	X		X		X	X

1.d. Interdependencies: Check which, if any, upstream or downstream sectors are included systematically

All										
Only Dependent Utilities and Communication		X	X	X	X	X		X		X
Banking & Finance										
Chemical										
Energy (Except Nuclear Power)										
Electricity								X		
Oil & Gas								X		
Emergency Services										
Information Technology	X							X	X	X
Telecommunications								X		
Postal & Shipping										
Public Health										
Transportation	X							X		
Water								X		
National Monuments & Icons										
Commercial Facilities										
Government Facilities										
Dams										

2. Consequence Metric: What types of consequence or loss are addressed or measured?

2.a Loss of Capacity/Output (not in financial terms)

Assessment Tool	FEMA, Emergency Management Guide for Business and Industry	NFPA 1600, Standard on Disaster / Emergency Management and Business Continuity Programs, 2004 Edition	FFIEC, Operations, IT Examination Handbook	FFIEC, Information Security, IT Examination Handbook	FFIEC, Management, IT Examination Handbook	NCS, Public Switched Network Assessment Guidelines	NCS, The Electronic intrusion threat to national Security and Emergency Preparedness (NS/EP) Internet Communications	NISCC, Good Practice Guide, Telecommunications Resilience	DOE, Energy Infrastructures Risk Management Checklists for Small and Medium Sized Energy Facilities	AWWA, Interim Voluntary Security Guidance for Water Utilities, December 9, 2004
-----------------	--	---	--	--	--	--	--	---	---	---

Question Range of Replies

Descriptive Section

1.c. System: Does the tool address the interaction of multiple assets within a system?

Yes	x		x	x	x	x		x	x	x
No		x					x			

1.d. Interdependencies: Check which, if any, upstream or downstream sectors are included systematically

All										
Only Dependent Utilities and Communication			x						x	x
Banking & Finance										
Chemical										
Energy (Except Nuclear Power)									x	
Electricity									x	
Oil & Gas									x	
Emergency Services	x								x	
Information Technology			x			x	x	x	x	
Telecommunications			x			x		x	x	
Postal & Shipping										
Public Health										
Transportation									x	
Water									x	
National Monuments & Icons										
Commercial Facilities										
Government Facilities										
Dams										

2. Consequence Metric: What types of consequence or loss are addressed or measured?

2.a Loss of Capacity/Output (not in financial terms)

Assessment Tool	AWWA, Interim Voluntary Security Guidance for Wastewater / Storm water Utilities, December 9, 2004	ASDWA/NRWA, Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems Serving Populations Between 3,300 and 10,000, November 13, 2002	ASIS, Business Continuity Guideline, 01 2005	BITS, BITS Guide to Business-Critical Telecommunications Services, November 2004	Compendium of Supporting Documents to the National Strategy for Critical Infrastructure Assurance Version 1.0, May 13, 2002	DOE, Energy Infrastructures Risk Assessment Checklists for State Governments, December 4, 2001	EOC Checklist	NIST SP800-53, Recommended Security Controls for Federal Information Systems, February 2005	USCG, Navigation and Vessel Inspection Circular NO. 05 03, December 15, 2003
-----------------	--	---	--	--	---	--	---------------	---	--

Question Range of Replies

Descriptive Section

1.c. System: Does the tool address the interaction of multiple assets within a system?

Yes	x		x	x		x		x	
No		x			x		x		x

1.d. Interdependencies: Check which, if any, upstream or downstream sectors are included systematically

All									
Only Dependent Utilities and Communication	x								
Banking & Finance				x					
Chemical									
Energy (Except Nuclear Power)									
Electricity				x					
Oil & Gas									
Emergency Services									
Information Technology				x				x	
Telecommunications				x				x	
Postal & Shipping									
Public Health									
Transportation									x
Water		x							
National Monuments & Icons									
Commercial Facilities									
Government Facilities									
Dams									

2. Consequence Metric: What types of consequence or loss are addressed or measured?

2.a Loss of Capacity/Output (not in financial terms)

Question	Range of Replies										
<u>Descriptive Section</u>											
Assessment Tool		RAND, Finding and Fixing Vulnerabilities in Information Systems, The Vulnerability Assessment and Mitigation Methodology, 2003	Securities Industry Association, Business Continuity Planning Committee Critical Infrastructure Guide	BITS ITSP Expectations Matrix	ODP, State Homeland Security Assessment and Strategy Program, Special Needs Jurisdiction Tool Kit	Risk Analysis and management for Critical Asset Protection (RAMCAP™)	DHS, Target Capability List	Commission on Accreditation for Law Enforcement Agencies (CALEA)	Emergency Management Accreditation Program (EMAP)	National Incident Management System (NIMS)	Sandia National Labs, Risk Assessment Methodology for Water (RAM-W)

1.c. System: Does the tool address the interaction of multiple assets within a system?

Yes	x	x	x		x	x		x	x	x
No				x			x			

1.d. Interdependencies: Check which, if any, upstream or downstream sectors are included systematically

All										x
Only Dependent Utilities and Communication	x	x	x	x					x	
Banking & Finance		x						x	x	
Chemical						x				
Energy (Except Nuclear Power)		x			x					
Electricity		x			x					
Oil & Gas		x			x					
Emergency Services		x			x	x	x	x	x	
Information Technology		x			x				x	
Telecommunications		x			x	x		x		
Postal & Shipping										
Public Health						x			x	
Transportation		x			x				x	
Water		x			x					
National Monuments & Icons							x			
Commercial Facilities							x			
Government Facilities							x			
Dams										

2. Consequence Metric: What types of consequence or loss are addressed or measured?

2.a Loss of Capacity/Output (not in financial terms)

Question	Range of Replies	The Vulnerability Self Assessment Tool™ (VSAT) for Water & Wastewater Utilities	FEMA, Reference Manual to Mitigate Terrorist Attacks Against Buildings	Kaiser Center Hazard and Vulnerability Analysis	NCR Healthcare Organization Guided Vulnerabilities Assessment and Preparedness Planning	Media Security and Reliability Council (MSRC) Adopted Best Practices Recommendations	NRIC Best Practice	National Security Telecommunications Advisory Committee (NSTAC) Reports	FFIEC Guidelines, BITS studies and recommendations for IT security	Banking and Financial Regulatory and Supervisory Oversight	General Industry Practices - Trade Associations National, State, Regional	Loudon County: Hazard Identification and Risk Analysis
Assessment Tool		<i>"Good Practice" tools</i>										
Descriptive Section												

1.c. System: Does the tool address the interaction of multiple assets within a system?

Yes	X	X	X	X	X	X	X	X	X	X	X	
No												X

1.d. Interdependencies: Check which, if any, upstream or downstream sectors are included systematically

All	X											
Only Dependent Utilities and Communication		X	X	X	X			X	X	X		
Banking & Finance							X	X	X	X		
Chemical												X
Energy (Except Nuclear Power)												
Electricity								X	X	X		X
Oil & Gas												X
Emergency Services									X			X
Information Technology							X	X	X	X		
Telecommunications							X	X	X	X		
Postal & Shipping									X	X		
Public Health												X
Transportation												X
Water												
National Monuments & Icons												
Commercial Facilities								X	X	X		X
Government Facilities								X	X	X		X
Dams												

2. Consequence Metric: What types of consequence or loss are addressed or measured?

2.a Loss of Capacity/Output (not in financial terms)

Assessment Tool	American Petroleum Industries: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries	ODP: Special Needs Jurisdiction Tool Kit	Ohio DOT: Guide to conducting Critical Asset Protection Self Assessments
Question	Range of Replies		
<u>Descriptive Section</u>			

1.c. System: Does the tool address the interaction of multiple assets within a system?

Yes	x	x	x
No			

1.d. Interdependencies: Check which, if any, upstream or downstream sectors are included systematically

All			
Only Dependent Utilities and Communication	x		
Banking & Finance	x		
Chemical	x		
Energy (Except Nuclear Power)	x		
Electricity	x		x
Oil & Gas	x		
Emergency Services	x		x
Information Technology	x		x
Telecommunications	x		x
Postal & Shipping			
Public Health			
Transportation	x		
Water	x		
National Monuments & Icons			
Commercial Facilities			
Government Facilities			
Dams			

2. Consequence Metric: What types of consequence or loss are addressed or measured?

2.a Loss of Capacity/Output (not in financial terms)

Assessment Tool	USCG, Outer Continental Shelf Facility Security Plans Review	DOJ, Department of Justice Standards for Protection of Federal Facilities	AMSA, Asset Based Vulnerability Checklist for Wastewater Utilities	DOJ, NIJ Special report: A Method to Assess the Vulnerability of U.S. Chemical Facilities	National Environmental Training Center, Protecting Your Community's Assets: A Guide for Small Wastewater Systems	EPA, Protect Your Water For Life: Vulnerability Assessment Fact sheet	DOE, Vulnerability Assessment Methodology, Electric Power Infrastructure	Dept. of Veterans Affairs, Physical Security Assessment for Department of Veterans Affairs Facilities	NERC, Security Guidelines for the Electricity Sector
-----------------	--	---	--	---	--	---	--	---	--

Question	Range of Replies									
Descriptive Section										
2.b Economic/Financial Loss	Check if yes, blank if no	X	X	X	X	X	X	X	X	X
2.c Environmental Degradation	Check if yes, blank if no	X		X	X	X	X	X		X
2.d Morbidity/Mortality	Check if yes, blank if no									
2.e Other	Check if yes, blank if no				X	X	X		X	
	Check if yes, blank if no									

3. Tool Design: What are the principle elements of the tool?

3.a. Format: Check the item(s) that make up the core of the tool.

Descriptions	X								
Checklists		X	X	X	X	X	X	X	X
Charts									
Questionnaires									
Other									

3.b. Input: Indicate the main type of data input

Quantitative data input: a cost benefit analysis									
Qualitative data input: expert assessment and relative ranking scales	X	X	X	X	X	X	X	X	X
Other									

3.c. Output: Indicate the output from the execution of the tool.

Advisory statement	X								
Simple ranking		X						X	
Estimate of Relative risk	X		X	X	X	X		X	X
Estimate of absolute risk									
Estimate of risk reduction			X				X		X

3.e. Cost: Estimated cost of completing or implementing the tool

Assessment Tool	American Chemistry Council, Transportation Security Guidelines for the US Chemical Industry	AASHTO, A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection	American Chemistry Council, Site Security Guidelines for the US	NIST, Pub 800-26 Security Self-Assessment Guide for Information Technology Systems	DOJ, Assessment and Strategy Development Tool Kit	CIAO, Vulnerability Assessment Framework 1.1	DoD, Physical Security Evaluation Guide	NIPRA, Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries	BITS, Framework for Managing Technology Risk for IT Service Provider Relationships	BITS, Calculator: BITS Key Risk Measurement Tool for Information Security Operational Risks
-----------------	---	--	---	--	---	--	---	---	--	---

Question	Range of Replies									
Descriptive Section										
2.b Economic/Financial Loss	Check if yes, blank if no		X		X	X	X		X	X
2.c Environmental Degradation	Check if yes, blank if no		X	X	X	X	X		X	X
2.d Morbidity/Mortality	Check if yes, blank if no	X		X					X	
2.e Other	Check if yes, blank if no	X	X	X					X	
	Check if yes, blank if no	X								

3. Tool Design: What are the principle elements of the tool?

3.a. Format: Check the item(s) that make up the core of the tool.

Descriptions							X			
Checklists		X		X	X	X		X		
Charts										
Questionnaires	X		X	X					X	
Other										

3.b. Input: Indicate the main type of data input

Quantitative data input: a cost benefit analysis				X					X	
Qualitative data input: expert assessment and relative ranking scales	X	X	X		X	X	X	X		
Other										

3.c. Output: Indicate the output from the execution of the tool.

Advisory statement	X		X	X			X			
Simple ranking					X				X	
Estimate of Relative risk		X				X		X		X
Estimate of absolute risk										
Estimate of risk reduction		X						X		

3.e. Cost: Estimated cost of completing or implementing the tool

Assessment Tool	FEMA, Emergency Management Guide for Business and Industry	NFPA 1600, Standard on Disaster / Emergency Management and Business Continuity Programs, 2004 Edition	FFIEC, Operations, IT Examination Handbook	FFIEC, Information Security, IT Examination Handbook	FFIEC, Management, IT Examination Handbook	NCS, Public Switched Network Assessment Guidelines	NCS, The Electronic intrusion threat to national Security and Emergency Preparedness (NS/EP) Internet Communications	NISCC, Good Practice Guide, Telecommunications Resilience	DOE, Energy Infrastructures Risk Management Checklists for Small and Medium Sized Energy Facilities	AWWA, Interim Voluntary Security Guidance for Water Utilities, December 9, 2004
-----------------	--	---	--	--	--	--	--	---	---	---

Question	Range of Replies									
Descriptive Section										
2.b Economic/Financial Loss	Check if yes, blank if no		X	X	X		X	X	X	X
2.c Environmental Degradation	Check if yes, blank if no	X	X	X		X	X	X		X
2.d Morbidity/Mortality	Check if yes, blank if no	X			X					
2.e Other	Check if yes, blank if no	X							X	
	Check if yes, blank if no									

3. Tool Design: What are the principle elements of the tool?

3.a. Format: Check the item(s) that make up the core of the tool.

Descriptions	X		X	X	X		X			X
Checklists		X				X			X	
Charts										
Questionnaires								X		
Other										

3.b. Input: Indicate the main type of data input

Quantitative data input: a cost benefit analysis			X	X	X					
Qualitative data input: expert assessment and relative ranking scales	X					X	X		X	X
Other		X						X		

3.c. Output: Indicate the output from the execution of the tool.

Advisory statement		X	X	X			X	X		
Simple ranking	X									
Estimate of Relative risk					X	X			X	X
Estimate of absolute risk										
Estimate of risk reduction										

3.e. Cost: Estimated cost of completing or implementing the tool

Assessment Tool	AWWA, Interim Voluntary Security Guidance for Wastewater / Storm water Utilities, December 9, 2004	ASDWA/NRWA, Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems Serving Populations Between 3,300 and 10,000, November 13, 2002	ASIS, Business Continuity Guideline, 01 2005	BITS, BITS Guide to Business-Critical Telecommunications Services, November 2004	Compendium of Supporting Documents to the National Strategy for Critical Infrastructure Assurance Version 1.0, May 13, 2002	DOE, Energy Infrastructures Risk Assessment Checklists for State Governments, December 4, 2001	EOC Checklist	NIST SP800-53, Recommended Security Controls for Federal Information Systems, February 2005	USCG, Navigation and Vessel Inspection Circular NO. 05 03, December 15, 2003
-----------------	--	---	--	--	---	--	---------------	---	--

Question	Range of Replies								
Descriptive Section									
2.b Economic/Financial Loss	Check if yes, blank if no	x	x	x	x			x	
2.c Environmental Degradation	Check if yes, blank if no	x		x		x	x		
2.d Morbidity/Mortality	Check if yes, blank if no								
2.e Other	Check if yes, blank if no			x					
	Check if yes, blank if no						x		x

3. Tool Design: What are the principle elements of the tool?

3.a. Format: Check the item(s) that make up the core of the tool.

Descriptions	x			x		x		x	
Checklists				x			x		x
Charts									
Questionnaires		x		x	x			x	
Other									

3.b. Input: Indicate the main type of data input

Quantitative data input: a cost benefit analysis				x					x
Qualitative data input: expert assessment and relative ranking scales	x			x		x	x	x	
Other		x					x		

3.c. Output: Indicate the output from the execution of the tool.

Advisory statement				x			x	x	x
Simple ranking		x							
Estimate of Relative risk	x			x		x	x		
Estimate of absolute risk									
Estimate of risk reduction									

3.e. Cost: Estimated cost of completing or implementing the tool

Question	Range of Replies	Assessment Tool									
		RAND, Finding and Fixing Vulnerabilities in Information Systems, The Vulnerability Assessment and Mitigation Methodology, 2003	Securities Industry Association, Business Continuity Planning Committee Critical Infrastructure Guide	BITS ITSP Expectations Matrix	ODP, State Homeland Security Assessment and Strategy Program, Special Needs Jurisdiction Tool Kit	Risk Analysis and management for Critical Asset Protection (RAMCAP™)	DHS, Target Capability List	Commission on Accreditation for Law Enforcement Agencies (CALEA)	Emergency Management Accreditation Program (EMAP)	National Incident Management System (NIMS)	Sandia National Labs, Risk Assessment Methodology for Water (RAM-W)

Descriptive Section											
2.b Economic/Financial Loss	Check if yes, blank if no	X	X		X	X	X		X		X
2.c Environmental Degradation	Check if yes, blank if no	X	X		X	X		X	X	X	
2.d Morbidity/Mortality	Check if yes, blank if no				X	X	X		X		
2.e Other	Check if yes, blank if no				X	X	X		X		
	Check if yes, blank if no				X		X	X	X		

3. Tool Design: What are the principle elements of the tool?

3.a. Format: Check the item(s) that make up the core of the tool.

Descriptions				X		X	X	X		X
Checklists				X		X	X	X		X
Charts				X						X
Questionnaires	X	X	X	X	X	X	X	X		X
Other						X	X		X	

3.b. Input: Indicate the main type of data input

Quantitative data input: a cost benefit analysis			X					X		X
Qualitative data input: expert assessment and relative ranking scales	X	X		X	X	X	X	X	X	X
Other										

3.c. Output: Indicate the output from the execution of the tool.

Advisory statement		X	X				X	X	X	X
Simple ranking										
Estimate of Relative risk	X					X				X
Estimate of absolute risk										
Estimate of risk reduction				X	X					

3.e. Cost: Estimated cost of completing or implementing the tool

Question	Range of Replies	The Vulnerability Self Assessment Tool™ (VSAT) for Water & Wastewater Utilities	FEMA, Reference Manual to Mitigate Terrorist Attacks Against Buildings	Kaiser Center Hazard and Vulnerability Analysis	NCR Healthcare Organization Guided Vulnerabilities Assessment and Preparedness Planning	Media Security and Reliability Council (MSRC) Adopted Best Practices Recommendations	NRIC Best Practice	National Security Telecommunications Advisory Committee (NSTAC) Reports	FFIEC Guidelines, BITS studies and recommendations for IT security	Banking and Financial Regulatory and Supervisory Oversight	General Industry Practices - Trade Associations National, State, Regional	Loudon County: Hazard Identification and Risk Analysis
		<i>"Good Practice" tools</i>										

Descriptive Section

2.a. Economic/Financial Loss	Check if yes, blank if no	X	X	X	X	X	X	X	X	X	X	
2.b. Environmental Degradation	Check if yes, blank if no		X	X					X	X	X	
2.c. Morbidity/Mortality	Check if yes, blank if no											
2.d. Other	Check if yes, blank if no		X	X					X	X	X	
2.e. Other	Check if yes, blank if no					X	X	X	X	X	X	

3. Tool Design: What are the principle elements of the tool?

3.a. Format: Check the item(s) that make up the core of the tool.

Descriptions	X	X		X	X	X	X	X	X	X	X	X
Checklists	X	X	X	X	X	X			X	X	X	X
Charts	X			X					X	X	X	
Questionnaires	X								X	X	X	
Other					X	X	X	X	X	X	X	

3.b. Input: Indicate the main type of data input

Quantitative data input: a cost benefit analysis	X								X	X	X	
Qualitative data input: expert assessment and relative ranking scales	X	X	X	X					X	X	X	X
Other					X	X	X	X	X	X	X	

3.c. Output: Indicate the output from the execution of the tool.

Advisory statement	X	X			X	X			X	X	X	
Simple ranking		X		X								X
Estimate of Relative risk	X	X	X						X	X	X	X
Estimate of absolute risk									X	X	X	
Estimate of risk reduction									X	X	X	

3.e. Cost: Estimated cost of completing or implementing the tool

Assessment Tool	American Petroleum Industries: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries	ODP: Special Needs Jurisdiction Tool Kit	Ohio DOT: Guide to conducting Critical Asset Protection Self Assessments
Question	Range of Replies		

Descriptive Section

Check if yes, blank if no	x	x	x
2.b Economic/Financial Loss			
Check if yes, blank if no	x	x	x
2.c. Environmental Degradation			
Check if yes, blank if no	x	x	x
2.d. Morbidity/Mortality			
Check if yes, blank if no	x	x	x
2.e. Other			
Check if yes, blank if no	x	x	x

3. Tool Design: What are the principle elements of the tool?

3.a. Format: Check the item(s) that make up the core of the tool.

Descriptions		x	x
Checklists	x	x	
Charts		x	
Questionnaires	x	x	
Other			x

3.b. Input: Indicate the main type of data input

Quantitative data input: a cost benefit analysis		x	
Qualitative data input: expert assessment and relative ranking scales	x	x	x
Other	x		

3.c. Output: Indicate the output from the execution of the tool.

Advisory statement		x	x
Simple ranking		x	x
Estimate of Relative risk		x	
Estimate of absolute risk	x		
Estimate of risk reduction	x		

3.e. Cost: Estimated cost of completing or implementing the tool

Assessment Tool	USCG, Outer Continental Shelf Facility Security Plans Review	DOJ, Department of Justice Standards for Protection of Federal Facilities	AMSA, Asset Based Vulnerability Checklist for Wastewater Utilities	DOJ, NIJ Special report: A Method to Assess the Vulnerability of U.S. Chemical Facilities	National Environmental Training Center, Protecting Your Community's Assets: A Guide for Small Wastewater Systems	EPA, Protect Your Water For Life: Vulnerability Assessment Fact sheet	DOE, Vulnerability Assessment Methodology, Electric Power Infrastructure	Dept. of Veterans Affairs, Physical Security Assessment for Department of Veterans Affairs Facilities	NERC, Security Guidelines for the Electricity Sector
-----------------	--	---	--	---	--	---	--	---	--

Question Range of Replies

Descriptive Section

1-3 days									
4-7 days	X							X	
8-14 days									
>14 days									
Unknown		X	X	X	X	X	X		X

3.e. Cost: Estimated cost of completing or implementing the tool

minimal									
< \$5,000									
\$5,000 - \$10,000								X	
> \$10,000									
Unknown	X	X	X	X	X	X	X		X

3.f. Executor: Tool can be used by e.g. owners/operators, external auditors, technical experts, regulators

Owner operators	X	X	X	X	X	X	X	X	X
External auditors		X						X	
Technical experts		X	X				X	X	X
Regulators		X						X	
Combination of above		X		X	X	X	X	X	X

Analytic Section

1. Maturity: What is the level of maturity of the CI-VA / RM Tool in its sector?

Not in use beyond an initial proof of concept.									
Limited use of the tool in sector.			X	X	X	X	X	X	X
Broad use of the tool in the sector.	X	X							
Accepted as a standard practice in the sector.									

Assessment Tool	American Chemistry Council, Transportation Security Guidelines for the US Chemical Industry	AASHTO, A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection	American Chemistry Council, Site Security Guidelines for the US	NIST, Pub 800-26 Security Self-Assessment Guide for Information Technology Systems	DOJ, Assessment and Strategy Development Tool Kit	CIAO, Vulnerability Assessment Framework 1.1	DoD, Physical Security Evaluation Guide	NPR, Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries	BITS, Framework for Managing Technology Risk for IT Service Provider Relationships	BITS, Calculator: BITS Key Risk Measurement Tool for Information Security Operational Risks
-----------------	---	--	---	--	---	--	---	---	--	---

Question Range of Replies

Descriptive Section

1-3 days										
4-7 days										
8-14 days										
>14 days		X								
Unknown	X		X	X	X	X	X	X	X	X

3.e. Cost: Estimated cost of completing or implementing the tool

minimal										
< \$5,000										
\$5,000 - \$10,000										
> \$10,000										
Unknown	X	X	X	X	X	X	X	X	X	X

3.f. Executor: Tool can be used by e.g. owners/operators, external auditors, technical experts, regulators

Owner operators	X	X	X	X	X	X	X		X	X
External auditors		X		X	X	X	X			
Technical experts		X		X	X	X	X			
Regulators						X				
Combination of above		X		X	X	X	X	X		X

Analytic Section

1. Maturity: What is the level of maturity of the CI-VA / RM Tool in its sector?

Not in use beyond an initial proof of concept.										
Limited use of the tool in sector.	X	X	X		X	X		X	X	X
Broad use of the tool in the sector.				X			X			
Accepted as a standard practice in the sector.										

Assessment Tool	FEMA, Emergency Management Guide for Business and Industry	NFPA 1600, Standard on Disaster / Emergency Management and Business Continuity Programs, 2004 Edition	FFIEC, Operations, IT Examination Handbook	FFIEC, Information Security, IT Examination Handbook	FFIEC, Management, IT Examination Handbook	NCS, Public Switched Network Assessment Guidelines	NCS, The Electronic intrusion threat to national Security and Emergency Preparedness (NS/EP) Internet Communications	NISCC, Good Practice Guide, Telecommunications Resilience	DOE, Energy Infrastructures Risk Management Checklists for Small and Medium Sized Energy Facilities	AWWA, Interim Voluntary Security Guidance for Water Utilities, December 9, 2004
-----------------	--	---	--	--	--	--	--	---	---	---

Question Range of Replies

Descriptive Section

1-3 days										
4-7 days										
8-14 days										
>14 days										
Unknown	X	X	X	X	X	X	X	X	X	X

3.e. Cost: Estimated cost of completing or implementing the tool

minimal										
< \$5,000										
\$5,000 - \$10,000										
> \$10,000										
Unknown	X	X	X	X	X	X	X	X	X	X

3.f. Executor: Tool can be used by e.g. owners/operators, external auditors, technical experts, regulators

Owner operators	X	X	X	X	X	X	X	X	X	X
External auditors			X	X	X		X			
Technical experts						X		X		
Regulators										
Combination of above			X	X	X	X	X	X		

Analytic Section

1. Maturity: What is the level of maturity of the CI-VA / RM Tool in its sector?

Not in use beyond an initial proof of concept.										
Limited use of the tool in sector.				X	X	X	X	X	X	X
Broad use of the tool in the sector.	X	X	X							
Accepted as a standard practice in the sector.										

Assessment Tool	AWWA, Interim Voluntary Security Guidance for Wastewater / Storm water Utilities, December 9, 2004	ASDWA/NRWA, Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems Serving Populations Between 3,300 and 10,000, November 13, 2002	ASIS, Business Continuity Guideline, 01 2005	BITS, BITS Guide to Business-Critical Telecommunications Services, November 2004	Compendium of Supporting Documents to the National Strategy for Critical Infrastructure Assurance Version 1.0, May 13, 2002	DOE, Energy Infrastructures Risk Assessment Checklists for State Governments, December 4, 2001	EOC Checklist	NIST SP800-53, Recommended Security Controls for Federal Information Systems, February 2005	USCG, Navigation and Vessel Inspection Circular NO. 05 03, December 15, 2003
-----------------	--	---	--	--	---	--	---------------	---	--

Question Range of Replies

Descriptive Section

1-3 days									
4-7 days									
8-14 days									
>14 days									
Unknown	X	X	X	X	X	X	X	X	X

3.e. Cost: Estimated cost of completing or implementing the tool

minimal									
< \$5,000									
\$5,000 - \$10,000									
> \$10,000									
Unknown	X	X	X	X		X	X	X	X

3.f. Executor: Tool can be used by e.g. owners/operators, external auditors, technical experts, regulators

Owner operators	X	X	X	X	X	X	X	X	X
External auditors			X					X	
Technical experts			X		X	X			
Regulators								X	
Combination of above			X					X	

Analytic Section

1. Maturity: What is the level of maturity of the CI-VA / RM Tool in its sector?

Not in use beyond an initial proof of concept.					X	X			
Limited use of the tool in sector.	X	X	X	X				X	
Broad use of the tool in the sector.									
Accepted as a standard practice in the sector.									X

Question	Range of Replies	Assessment Tool											
		RAND, Finding and Fixing Vulnerabilities in Information Systems, The Vulnerability Assessment and Mitigation Methodology, 2003	Securities Industry Association, Business Continuity Planning Committee Critical Infrastructure Guide	BITS ITSP Expectations Matrix	ODP, State Homeland Security Assessment and Strategy Program, Special Needs Jurisdiction Tool Kit	Risk Analysis and management for Critical Asset Protection (RAMCAP™)	DHS, Target Capability List	Commission on Accreditation for Law Enforcement Agencies (CALEA)	Emergency Management Accreditation Program (EMAP)	National Incident Management System (NIMS)	Sandia National Labs, Risk Assessment Methodology for Water (RAM-W)		

Descriptive Section

1-3 days													
4-7 days													
8-14 days													
>14 days							X	X			X		
Unknown	X	X	X	X	X	X	X			X			

3.e. Cost: Estimated cost of completing or implementing the tool

minimal													
< \$5,000													
\$5,000 - \$10,000								X					
> \$10,000								X				X	
Unknown	X	X	X	X	X	X	X		X	X			

3.f. Executor: Tool can be used by e.g. owners/operators, external auditors, technical experts, regulators

Owner operators	X	X	X	X	X	X							
External auditors				X	X	X			X				
Technical experts				X	X	X			X				
Regulators				X									
Combination of above				X	X			X		X		X	

Analytic Section

1. Maturity: What is the level of maturity of the CI-VA / RM Tool in its sector?

Not in use beyond an initial proof of concept.					X	X							
Limited use of the tool in sector.	X	X								X			
Broad use of the tool in the sector.			X	X					X				
Accepted as a standard practice in the sector.								X				X	

Question	Range of Replies	The Vulnerability Self Assessment Tool™ (VSAT) for Water & Wastewater Utilities	FEMA, Reference Manual to Mitigate Terrorist Attacks Against Buildings	Kaiser Center Hazard and Vulnerability Analysis	NCR Healthcare Organization Guided Vulnerabilities Assessment and Preparedness Planning	Media Security and Reliability Council (MSRC) Adopted Best Practices Recommendations	NRIC Best Practice	National Security Telecommunications Advisory Committee (NSTAC) Reports	FFIEC Guidelines, BITS studies and recommendations for IT security	Banking and Financial Regulatory and Supervisory Oversight	General Industry Practices - Trade Associations National, State, Regional	Loudon County: Hazard Identification and Risk Analysis
		<i>"Good Practice" tools</i>										

Descriptive Section

1-3 days			X									
4-7 days					X							
8-14 days					X							
>14 days	X								X	X	X	
Unknown		X				X	X	X				X

3.e. Cost: Estimated cost of completing or implementing the tool

minimal												
< \$5,000			X									
\$5,000 - \$10,000												
> \$10,000	X				X				X	X	X	
Unknown		X				X	X	X				X

3.f. Executor: Tool can be used by e.g. owners/operators, external auditors, technical experts, regulators

Owner operators		X		X	X	X	X	X	X	X	X	
External auditors		X							X	X	X	
Technical experts		X		X	X	X	X	X	X	X	X	
Regulators					X	X			X	X	X	
Combination of above	X	X	X	X					X	X	X	X

Analytic Section

1. Maturity: What is the level of maturity of the CI-VA / RM Tool in its sector?

Not in use beyond an initial proof of concept.				X								
Limited use of the tool in sector.												
Broad use of the tool in the sector.	X	X	X		X	X	X					
Accepted as a standard practice in the sector.									X	X	X	X

Assessment Tool	American Petroleum Industries: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries	ODP: Special Needs Jurisdiction Tool Kit	Ohio DOT: Guide to conducting Critical Asset Protection Self Assessments
Question	Range of Replies		

Descriptive Section

1-3 days			
4-7 days			
8-14 days			
>14 days			x
Unknown	x	x	

3.e. Cost: Estimated cost of completing or implementing the tool

minimal			
< \$5,000			
\$5,000 - \$10,000			
> \$10,000			
Unknown	x	x	x

3.f. Executor: Tool can be used by e.g. owners/operators, external auditors, technical experts, regulators

Owner operators	x		x
External auditors			
Technical experts	x		x
Regulators			
Combination of above	x	x	x

Analytic Section

1. Maturity: What is the level of maturity of the CI-VA / RM Tool in its sector?

Not in use beyond an initial proof of concept.			
Limited use of the tool in sector.	x		x
Broad use of the tool in the sector.		x	
Accepted as a standard practice in the sector.			

Question	Range of Replies	USCG, Outer Continental Shelf Facility Security Plans Review	DOJ, Department of Justice Standards for Protection of Federal Facilities	AMSA, Asset Based Vulnerability Checklist for Wastewater Utilities	DOJ, NIJ Special report: A Method to Assess the Vulnerability of U.S. Chemical Facilities	National Environmental Training Center, Protecting Your Community's Assets: A Guide for Small Wastewater Systems	EPA, Protect Your Water For Life: Vulnerability Assessment Fact sheet	DOE, Vulnerability Assessment Methodology, Electric Power Infrastructure	Dept. of Veterans Affairs, Physical Security Assessment for Department of Veterans Affairs Facilities	NERC, Security Guidelines for the Electricity Sector
----------	------------------	--	---	--	---	--	---	--	---	--

Descriptive Section

2. Criticality Screen: Is there a process of screening out low priority assets from further assessment?

No, all asset/systems are included in the entire assessment process							x			x
Yes, assets/systems are prioritized according to some level of criticality.	x	x	x	x	x	x		x	x	

3a Threat / Hazard Types:

3.a. What is the CI-VA / RM Tool Threats / Hazard approach?

Tool is not explicit as the threats / hazards.										
Tool addresses only threats / hazards associated with		x								
Tool addresses all man made threats / hazards (Terrorism, Criminal Activity).	x			x	x	x	x			x
Tool addresses man made and natural disaster threats /			x						x	

3b. Threat / Hazard Quantification: Are threats / hazards

Not quantified.			x							
Relative probabilities or likelihoods based on general	x	x					x			
Relative probabilities or likelihoods based on specific analysis of intents, capabilities, etc.				x	x			x	x	x
Absolute probabilities or likelihoods based on specific analysis of intents, capabilities, etc.										

4a. Vulnerability Types:

4a. Does CI-VA / RM Tool conduct a Vulnerability Analysis with contextual standards and from a systemic perspective?

Simple listing of vulnerabilities.										
------------------------------------	--	--	--	--	--	--	--	--	--	--

Question	Range of Replies	American Chemistry Council, Transportation Security Guidelines for the US Chemical Industry	AASHTO, A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection	American Chemistry Council, Site Security Guidelines for the US	NIST, Pub 800-26 Security Self-Assessment Guide for Information Technology Systems	DOJ, Assessment and Strategy Development Tool Kit	CIAO, Vulnerability Assessment Framework 1.1	DoD, Physical Security Evaluation Guide	NPRA, Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries	BITS, Framework for Managing Technology Risk for IT Service Provider Relationships	BITS, Calculator: BITS Key Risk Measurement Tool for Information Security Operational Risks
----------	------------------	---	--	---	--	---	--	---	--	--	---

Descriptive Section

2. Criticality Screen: Is there a process of screening out low priority assets from further assessment?

No, all asset/systems are included in the entire assessment process			x	x		x	x		x	x
Yes, assets/systems are prioritized according to some level of criticality.	x	x			x			x		

3a Threat / Hazard Types:

3.a. What is the CI-VA / RM Tool Threats / Hazard approach?

Tool is not explicit as the threats / hazards.							x			
Tool addresses only threats / hazards associated with					x					
Tool addresses all man made threats / hazards (Terrorism, Criminal Activity).	x	x	x			x		x	x	
Tool addresses man made and natural disaster threats /				x						x

3b. Threat / Hazard Quantification: Are threats / hazards

Not quantified.	x		x	x		x	x			
Relative probabilities or likelihoods based on general									x	x
Relative probabilities or likelihoods based on specific analysis of intents, capabilities, etc.		x			x			x		
Absolute probabilities or likelihoods based on specific analysis of intents, capabilities, etc.										

4a. Vulnerability Types:

4a. Does CI-VA / RM Tool conduct a Vulnerability Analysis with contextual standards and from a systemic perspective?

Simple listing of vulnerabilities.							x			
------------------------------------	--	--	--	--	--	--	---	--	--	--

Assessment Tool	FEMA, Emergency Management Guide for Business and Industry	NFPA 1600, Standard on Disaster / Emergency Management and Business Continuity Programs, 2004 Edition	FFIEC, Operations, IT Examination Handbook	FFIEC, Information Security, IT Examination Handbook	FFIEC, Management, IT Examination Handbook	NCS, Public Switched Network Assessment Guidelines	NCS, The Electronic intrusion threat to national Security and Emergency Preparedness (NS/EP) Internet Communications	NISCC, Good Practice Guide, Telecommunications Resilience	DOE, Energy Infrastructures Risk Management Checklists for Small and Medium Sized Energy Facilities	AWWA, Interim Voluntary Security Guidance for Water Utilities, December 9, 2004
Question	Range of Replies									

Descriptive Section

2. Criticality Screen: Is there a process of screening out low priority assets from further assessment?

No, all asset/systems are included in the entire assessment process	x	x	x	x	x		x	x	x	x
Yes, assets/systems are prioritized according to some level of criticality.						x				

3a Threat / Hazard Types:

3.a. What is the CI-VA / RM Tool Threats / Hazard approach?

Tool is not explicit as the threats / hazards.			x	x					x	
Tool addresses only threats / hazards associated with										
Tool addresses all man made threats / hazards (Terrorism, Criminal Activity).						x	x	x		x
Tool addresses man made and natural disaster threats /	x	x			x					

3b. Threat / Hazard Quantification: Are threats / hazards

Not quantified.	x	x	x	x			x	x		
Relative probabilities or likelihoods based on general					x	x			x	x
Relative probabilities or likelihoods based on specific analysis of intents, capabilities, etc.										
Absolute probabilities or likelihoods based on specific analysis of intents, capabilities, etc.										

4a. Vulnerability Types:

4a. Does CI-VA / RM Tool conduct a Vulnerability Analysis with contextual standards and from a systemic perspective?

Simple listing of vulnerabilities.		x								
------------------------------------	--	---	--	--	--	--	--	--	--	--

Question	Range of Replies	Assessment Tool	AWWA, Interim Voluntary Security Guidance for Wastewater / Storm water Utilities, December 9, 2004	ASDWA/NRWA, Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems Serving Populations Between 3,300 and 10,000, November 13, 2002	ASIS, Business Continuity Guideline, 01 2005	BITS, BITS Guide to Business-Critical Telecommunications Services, November 2004	Compendium of Supporting Documents to the National Strategy for Critical Infrastructure Assurance Version 1.0, May 13, 2002	DOE, Energy Infrastructures Risk Assessment Checklists for State Governments, December 4, 2001	EOC Checklist	NIST SP800-53, Recommended Security Controls for Federal Information Systems, February 2005	USCG, Navigation and Vessel Inspection Circular NO. 05 03, December 15, 2003
----------	------------------	-----------------	--	---	--	--	---	--	---------------	---	--

Descriptive Section

2. Criticality Screen: Is there a process of screening out low priority assets from further assessment?

No, all asset/systems are included in the entire assessment process	x	x		x			x	x	
Yes, assets/systems are prioritized according to some level of criticality.			x		x	x			x

3a Threat / Hazard Types:

3.a. What is the CI-VA / RM Tool Threats / Hazard approach?

Tool is not explicit as the threats / hazards.				x	x		x	x	x
Tool addresses only threats / hazards associated with							x		
Tool addresses all man made threats / hazards (Terrorism, Criminal Activity).	x	x							
Tool addresses man made and natural disaster threats /			x						

3b. Threat / Hazard Quantification: Are threats / hazards

Not quantified.		x		x			x	x	x
Relative probabilities or likelihoods based on general	x				x	x			
Relative probabilities or likelihoods based on specific analysis of intents, capabilities, etc.			x						
Absolute probabilities or likelihoods based on specific analysis of intents, capabilities, etc.									

4a. Vulnerability Types:

4a. Does CI-VA / RM Tool conduct a Vulnerability Analysis with contextual standards and from a systemic perspective?

Simple listing of vulnerabilities.							x		
------------------------------------	--	--	--	--	--	--	---	--	--

Question	Range of Replies
Assessment Tool	RAND, Finding and Fixing Vulnerabilities in Information Systems, The Vulnerability Assessment and Mitigation Methodology, 2003
	Securities Industry Association, Business Continuity Planning Committee Critical Infrastructure Guide
	BITS ITSP Expectations Matrix
	ODP, State Homeland Security Assessment and Strategy Program, Special Needs Jurisdiction Tool Kit
	Risk Analysis and management for Critical Asset Protection (RAMCAP™)
	DHS, Target Capability List
	Commission on Accreditation for Law Enforcement Agencies (CALEA)
	Emergency Management Accreditation Program (EMAP)
	National Incident Management System (NIMS)
	Sandia National Labs, Risk Assessment Methodology for Water (RAM-W)

Descriptive Section

2. Criticality Screen: Is there a process of screening out low priority assets from further assessment?

No, all asset/systems are included in the entire assessment process	x	x	x				x	x		
Yes, assets/systems are prioritized according to some level of criticality.				x	x	x			x	x

3a Threat / Hazard Types:

3.a. What is the CI-VA / RM Tool Threats / Hazard approach?

Tool is not explicit as the threats / hazards.		x	x				x			
Tool addresses only threats / hazards associated with										
Tool addresses all man made threats / hazards (Terrorism, Criminal Activity).	x									
Tool addresses man made and natural disaster threats /				x	x	x		x	x	x

3b. Threat / Hazard Quantification: Are threats / hazards

Not quantified.	x	x	x				x		x	
Relative probabilities or likelihoods based on general										x
Relative probabilities or likelihoods based on specific analysis of intents, capabilities, etc.						x		x		
Absolute probabilities or likelihoods based on specific analysis of intents, capabilities, etc.				x	x					

4a. Vulnerability Types:

4a. Does CI-VA / RM Tool conduct a Vulnerability Analysis with contextual standards and from a systemic perspective?

Simple listing of vulnerabilities.							x		x	
------------------------------------	--	--	--	--	--	--	---	--	---	--

Question	Range of Replies	The Vulnerability Self Assessment Tool™ (VSAT) for Water & Wastewater Utilities	FEMA, Reference Manual to Mitigate Terrorist Attacks Against Buildings	Kaiser Center Hazard and Vulnerability Analysis	NCR Healthcare Organization Guided Vulnerabilities Assessment and Preparedness Planning	Media Security and Reliability Council (MSRC) Adopted Best Practices Recommendations	NRIC Best Practice	National Security Telecommunications Advisory Committee (NSTAC) Reports	FFIEC Guidelines, BITS studies and recommendations for IT security	Banking and Financial Regulatory and Supervisory Oversight	General Industry Practices - Trade Associations National, State, Regional	Loudon County: Hazard Identification and Risk Analysis
		<i>"Good Practice" tools</i>										

Descriptive Section

2. Criticality Screen: Is there a process of screening out low priority assets from further assessment?

No, all asset/systems are included in the entire assessment process			X	X				X				
Yes, assets/systems are prioritized according to some level of criticality.	X	X							X	X	X	X

3a Threat / Hazard Types:

3.a. What is the CI-VA / RM Tool Threats / Hazard approach?

Tool is not explicit as the threats / hazards.				X								
Tool addresses only threats / hazards associated with												
Tool addresses all man made threats / hazards (Terrorism, Criminal Activity).									X	X		
Tool addresses man made and natural disaster threats /	X	X	X				X		X	X	X	X

3b. Threat / Hazard Quantification: Are threats / hazards

Not quantified.				X			X					
Relative probabilities or likelihoods based on general	X		X					X	X	X		
Relative probabilities or likelihoods based on specific analysis of intents, capabilities, etc.		X										
Absolute probabilities or likelihoods based on specific analysis of intents, capabilities, etc.												X

4a. Vulnerability Types:

4a. Does CI-VA / RM Tool conduct a Vulnerability Analysis with contextual standards and from a systemic perspective?

Simple listing of vulnerabilities.			X									
------------------------------------	--	--	---	--	--	--	--	--	--	--	--	--

Assessment Tool	American Petroleum Industries: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries ODP: Special Needs Jurisdiction Tool Kit Ohio DOT: Guide to conducting Critical Asset Protection Self Assessments
Question	Range of Replies

Descriptive Section

2. Criticality Screen: Is there a process of screening out low priority assets from further assessment?

No, all asset/systems are included in the entire assessment process			
Yes, assets/systems are prioritized according to some level of criticality.	x	x	x

3a Threat / Hazard Types:

3.a. What is the CI-VA / RM Tool Threats / Hazard approach?

Tool is not explicit as the threats / hazards.			x
Tool addresses only threats / hazards associated with			
Tool addresses all man made threats / hazards (Terrorism, Criminal Activity).	x	x	
Tool addresses man made and natural disaster threats /			

3b. Threat / Hazard Quantification: Are threats / hazards

Not quantified.			x
Relative probabilities or likelihoods based on general			
Relative probabilities or likelihoods based on specific analysis of intents, capabilities, etc.	x		
Absolute probabilities or likelihoods based on specific analysis of intents, capabilities, etc.		x	

4a. Vulnerability Types:

4a. Does CI-VA / RM Tool conduct a Vulnerability Analysis with contextual standards and from a systemic perspective?

Simple listing of vulnerabilities.			
------------------------------------	--	--	--

Question	Range of Replies	USCG, Outer Continental Shelf Facility Security Plans Review	DOJ, Department of Justice Standards for Protection of Federal Facilities	AMSA, Asset Based Vulnerability Checklist for Wastewater Utilities	DOJ, NIJ Special report: A Method to Assess the Vulnerability of U.S. Chemical Facilities	National Environmental Training Center, Protecting Your Community's Assets: A Guide for Small Wastewater Systems	EPA, Protect Your Water For Life: Vulnerability Assessment Fact sheet	DOE, Vulnerability Assessment Methodology, Electric Power Infrastructure	Dept. of Veterans Affairs, Physical Security Assessment for Department of Veterans Affairs Facilities	NERC, Security Guidelines for the Electricity Sector
----------	------------------	--	---	--	---	--	---	--	---	--

Descriptive Section										
Includes the evaluation of protection measures and standards.				X						
Includes the evaluation of each protection measure for identified key assets	X	X								X
Includes the evaluation of each protection measure for identified key assets as part of a comprehensive security process (detection, assessment, delay, response).				X	X	X	X	X		

4b. Vulnerability Quantification: Are vulnerabilities quantified?

Not quantified.	X									
Relative probabilities or likelihoods based on general		X	X	X	X				X	
Relative probabilities or likelihoods based on failure analysis.							X			X
Absolute probabilities or likelihoods based on failure analysis.										

5. Consequence: Does the CI-VA / RM Tool identify critical structures (such as utility systems, mechanical systems, fire alarm system, wall& window design, roofing system, structural system, security systems and site layout) and/or critical functions (i.e., primary services or outputs and the critical activities that take place at the site)

Does not address critical structure or critical function identification.										
Addresses only critical structure or critical function identification, but not both.										
Addresses both critical structure and critical function identification.	X	X	X	X	X				X	X

Assessment Tool	American Chemistry Council, Transportation Security Guidelines for the US Chemical Industry	AASHTO, A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection	American Chemistry Council, Site Security Guidelines for the US	NIST, Pub 800-26 Security Self-Assessment Guide for Information Technology Systems	DOJ, Assessment and Strategy Development Tool Kit	CIAO, Vulnerability Assessment Framework 1.1	DoD, Physical Security Evaluation Guide	NPRA, Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries	BITS, Framework for Managing Technology Risk for IT Service Provider Relationships	BITS, Calculator: BITS Key Risk Measurement Tool for Information Security Operational Risks
-----------------	---	--	---	--	---	--	---	--	--	---

Question Range of Replies

Descriptive Section

Includes the evaluation of protection measures and standards.	x		x	x					x	x
Includes the evaluation of each protection measure for identified key assets					x	x				
Includes the evaluation of each protection measure for identified key assets as part of a comprehensive security process (detection, assessment, delay, response).		x						x		

4b. Vulnerability Quantification: Are vulnerabilities quantified?

Not quantified.	x		x				x			
Relative probabilities or likelihoods based on general				x		x			x	x
Relative probabilities or likelihoods based on failure analysis.		x			x			x		
Absolute probabilities or likelihoods based on failure analysis.										

5. Consequence: Does the CI-VA / RM Tool identify critical structures (such as utility systems, mechanical systems, fire alarm system, wall& window design, roofing system, structural system, security systems and site layout) and/or critical functions (i.e., primary services or outputs and the critical activities that take place at the site)

Does not address critical structure or critical function identification.	x									
Addresses only critical structure or critical function identification, but not both.			x		x		x		x	
Addresses both critical structure and critical function identification.				x		x				x

Assessment Tool	FEMA, Emergency Management Guide for Business and Industry	NFPA 1600, Standard on Disaster / Emergency Management and Business Continuity Programs, 2004 Edition	FFIEC, Operations, IT Examination Handbook	FFIEC, Information Security, IT Examination Handbook	FFIEC, Management, IT Examination Handbook	NCS, Public Switched Network Assessment Guidelines	NCS, The Electronic intrusion threat to national Security and Emergency Preparedness (NS/EP) Internet Communications	NISCC, Good Practice Guide, Telecommunications Resilience	DOE, Energy Infrastructures Risk Management Checklists for Small and Medium Sized Energy Facilities	AWWA, Interim Voluntary Security Guidance for Water Utilities, December 9, 2004
-----------------	--	---	--	--	--	--	--	---	---	---

Question Range of Replies

Descriptive Section										
Includes the evaluation of protection measures and standards.	X		X	X			X	X		
Includes the evaluation of each protection measure for identified key assets					X	X			X	X
Includes the evaluation of each protection measure for identified key assets as part of a comprehensive security process (detection, assessment, delay, response).										

4b. Vulnerability Quantification: Are vulnerabilities quantified?

Not quantified.	X	X	X	X			X	X		
Relative probabilities or likelihoods based on general					X	X			X	X
Relative probabilities or likelihoods based on failure analysis.										
Absolute probabilities or likelihoods based on failure analysis.										

5. Consequence: Does the CI-VA / RM Tool identify critical structures (such as utility systems, mechanical systems, fire alarm system, wall& window design, roofing system, structural system, security systems and site layout) and/or critical functions (i.e., primary services or outputs and the critical activities that take place at the site)

Does not address critical structure or critical function identification.							X			
Addresses only critical structure or critical function identification, but not both.			X	X	X	X		X		
Addresses both critical structure and critical function identification.	X	X							X	X

Assessment Tool	AWWA, Interim Voluntary Security Guidance for Wastewater / Storm water Utilities, December 9, 2004	ASDWA/NRWA, Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems Serving Populations Between 3,300 and 10,000, November 13, 2002	ASIS, Business Continuity Guideline, 01 2005	BITS, BITS Guide to Business-Critical Telecommunications Services, November 2004	Compendium of Supporting Documents to the National Strategy for Critical Infrastructure Assurance Version 1.0, May 13, 2002	DOE, Energy Infrastructures Risk Assessment Checklists for State Governments, December 4, 2001	EOC Checklist	NIST SP800-53, Recommended Security Controls for Federal Information Systems, February 2005	USCG, Navigation and Vessel Inspection Circular NO. 05 03, December 15, 2003
-----------------	--	---	--	--	---	--	---------------	---	--

Question Range of Replies

Descriptive Section

Includes the evaluation of protection measures and standards.		X		X	X			X	X
Includes the evaluation of each protection measure for identified key assets	X		X						
Includes the evaluation of each protection measure for identified key assets as part of a comprehensive security process (detection, assessment, delay, response).									

4b. Vulnerability Quantification: Are vulnerabilities quantified?

Not quantified.	X	X		X			X	X	X
Relative probabilities or likelihoods based on general					X	X			
Relative probabilities or likelihoods based on failure analysis.			X						
Absolute probabilities or likelihoods based on failure analysis.									

5. Consequence: Does the CI-VA / RM Tool identify critical structures (such as utility systems, mechanical systems, fire alarm system, wall& window design, roofing system, structural system, security systems and site layout) and/or critical functions (i.e., primary services or outputs and the critical activities that take place at the site)

Does not address critical structure or critical function identification.									X
Addresses only critical structure or critical function identification, but not both.		X		X				X	
Addresses both critical structure and critical function identification.	X				X	X	X		

Question	Range of Replies	Assessment Tool	RAND, Finding and Fixing Vulnerabilities in Information Systems, The Vulnerability Assessment and Mitigation Methodology, 2003	Securities Industry Association, Business Continuity Planning Committee Critical Infrastructure Guide	BITS ITSP Expectations Matrix	ODP, State Homeland Security Assessment and Strategy Program, Special Needs Jurisdiction Tool Kit	Risk Analysis and management for Critical Asset Protection (RAMCAP™)	DHS, Target Capability List	Commission on Accreditation for Law Enforcement Agencies (CALEA)	Emergency Management Accreditation Program (EMAP)	National Incident Management System (NIMS)	Sandia National Labs, Risk Assessment Methodology for Water (RAM-W)
----------	------------------	-----------------	--	---	-------------------------------	---	--	-----------------------------	--	---	--	---

Descriptive Section

Includes the evaluation of protection measures and standards.		X	X									X
Includes the evaluation of each protection measure for identified key assets	X						X		X			X
Includes the evaluation of each protection measure for identified key assets as part of a comprehensive security process (detection, assessment, delay, response).				X	X							

4b. Vulnerability Quantification: Are vulnerabilities quantified?

Not quantified.	X	X	X				X		X		
Relative probabilities or likelihoods based on general						X					X
Relative probabilities or likelihoods based on failure analysis.					X			X			X
Absolute probabilities or likelihoods based on failure analysis.				X							

5. Consequence: Does the CI-VA / RM Tool identify critical structures (such as utility systems, mechanical systems, fire alarm system, wall & window design, roofing system, structural system, security systems and site layout) and/or critical functions (i.e., primary services or outputs and the critical activities that take place at the site)

Does not address critical structure or critical function identification.							X				
Addresses only critical structure or critical function identification, but not both.			X			X			X		
Addresses both critical structure and critical function identification.		X									X

Question	Range of Replies	"Good Practice" tools										
	Assessment Tool	The Vulnerability Self Assessment Tool™ (VSAT) for Water & Wastewater Utilities	FEMA, Reference Manual to Mitigate Terrorist Attacks Against Buildings	Kaiser Center Hazard and Vulnerability Analysis	NCR Healthcare Organization Guided Vulnerabilities Assessment and Preparedness Planning	Media Security and Reliability Council (MSRC) Adopted Best Practices Recommendations	NRIC Best Practice	National Security Telecommunications Advisory Committee (NSTAC) Reports	FFIEC Guidelines, BITS studies and recommendations for IT security	Banking and Financial Regulatory and Supervisory Oversight	General Industry Practices - Trade Associations National, State, Regional	Loudon County: Hazard Identification and Risk Analysis

Descriptive Section											
Includes the evaluation of protection measures and standards.	x			x							
Includes the evaluation of each protection measure for identified key assets		x						x	x	x	x
Includes the evaluation of each protection measure for identified key assets as part of a comprehensive security process (detection, assessment, delay, response).											

4b. Vulnerability Quantification: Are vulnerabilities quantified?

Not quantified.			x	x							
Relative probabilities or likelihoods based on general	x	x						x	x	x	
Relative probabilities or likelihoods based on failure analysis.	x										
Absolute probabilities or likelihoods based on failure analysis.											x

5. Consequence: Does the CI-VA / RM Tool identify critical structures (such as utility systems, mechanical systems, fire alarm system, wall& window design, roofing system, structural system, security systems and site layout) and/or critical functions (i.e., primary services or outputs and the critical activities that take place at the site)

Does not address critical structure or critical function identification.			x	x							x
Addresses only critical structure or critical function identification, but not both.											
Addresses both critical structure and critical function identification.	x				x	x	x	x	x	x	

Assessment Tool	American Petroleum Industries: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries	ODP: Special Needs Jurisdiction Tool Kit	Ohio DOT: Guide to conducting Critical Asset Protection Self Assessments
Question	Range of Replies		

Descriptive Section

Includes the evaluation of protection measures and standards.			
Includes the evaluation of each protection measure for identified key assets			x
Includes the evaluation of each protection measure for identified key assets as part of a comprehensive security process (detection, assessment, delay, response).	x	x	

4b. Vulnerability Quantification: Are vulnerabilities quantified?

Not quantified.			x
Relative probabilities or likelihoods based on general	x		
Relative probabilities or likelihoods based on failure analysis.			
Absolute probabilities or likelihoods based on failure analysis.		x	

5. Consequence: Does the CI-VA / RM Tool identify critical structures (such as utility systems, mechanical systems, fire alarm system, wall& window design, roofing system, structural system, security systems and site layout) and/or critical functions (i.e., primary services or outputs and the critical activities that take place at the site)

Does not address critical structure or critical function identification.			
Addresses only critical structure or critical function identification, but not both.			
Addresses both critical structure and critical function identification.	x	x	x

Question	Range of Replies	USCG, Outer Continental Shelf Facility Security Plans Review	DOJ, Department of Justice Standards for Protection of Federal Facilities	AMSA, Asset Based Vulnerability Checklist for Wastewater Utilities	DOJ, NIJ Special report: A Method to Assess the Vulnerability of U.S. Chemical Facilities	National Environmental Training Center, Protecting Your Community's Assets: A Guide for Small Wastewater Systems	EPA, Protect Your Water For Life: Vulnerability Assessment Fact sheet	DOE, Vulnerability Assessment Methodology, Electric Power Infrastructure	Dept. of Veterans Affairs, Physical Security Assessment for Department of Veterans Affairs Facilities	NERC, Security Guidelines for the Electricity Sector
----------	------------------	--	---	--	---	--	---	--	---	--

Descriptive Section

Addresses both critical structure and critical function identification and analyzes the probability and/or range of credible consequences.								x		
--	--	--	--	--	--	--	--	---	--	--

6. Risk Reduction: Does the CI-VA / RM Tool determine risk reduction and cost benefit of mitigation?

Does not address risk reduction processes.		x								
Directs risk reduction steps for particular measures.	x		x							
Estimates risk reduction effectiveness in terms of threat, vulnerability, and consequence of loss of a particular asset.				x	x		x	x	x	
Estimates risk reduction effectiveness in terms of threat, vulnerability, and consequence of loss in context of a larger system and the entire sector.										

Assessment Tool	American Chemistry Council, Transportation Security Guidelines for the US Chemical Industry	AASHTO, A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection	American Chemistry Council, Site Security Guidelines for the US	NIST, Pub 800-26 Security Self-Assessment Guide for Information Technology Systems	DOJ, Assessment and Strategy Development Tool Kit	CIAO, Vulnerability Assessment Framework 1.1	DoD, Physical Security Evaluation Guide	NPR, Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries	BITS, Framework for Managing Technology Risk for IT Service Provider Relationships	BITS, Calculator: BITS Key Risk Measurement Tool for Information Security Operational Risks
-----------------	---	--	---	--	---	--	---	---	--	---

Question Range of Replies

Descriptive Section

Addresses both critical structure and critical function identification and analyzes the probability and/or range of credible consequences.		x						x		
--	--	---	--	--	--	--	--	---	--	--

6. Risk Reduction: Does the CI-VA / RM Tool determine risk reduction and cost benefit of mitigation?

Does not address risk reduction processes.							x			
Directs risk reduction steps for particular measures.	x		x	x		x			x	x
Estimates risk reduction effectiveness in terms of threat, vulnerability, and consequence of loss of a particular asset.		x						x		
Estimates risk reduction effectiveness in terms of threat, vulnerability, and consequence of loss in context of a larger system and the entire sector.										

Question	Range of Replies	Assessment Tool									
		FEMA, Emergency Management Guide for Business and Industry									
		NFPA 1600, Standard on Disaster / Emergency Management and Business Continuity Programs, 2004 Edition									
		FFIEC, Operations, IT Examination Handbook									
		FFIEC, Information Security, IT Examination Handbook									
		FFIEC, Management, IT Examination Handbook									
		NCS, Public Switched Network Assessment Guidelines									
		NCS, The Electronic intrusion threat to national Security and Emergency Preparedness (NS/EP) Internet Communications									
		NISCC, Good Practice Guide, Telecommunications Resilience									
		DOE, Energy Infrastructures Risk Management Checklists for Small and Medium Sized Energy Facilities									
		AWWA, Interim Voluntary Security Guidance for Water Utilities, December 9, 2004									

Descriptive Section											
Addresses both critical structure and critical function identification and analyzes the probability and/or range of credible consequences.											

6. Risk Reduction: Does the CI-VA / RM Tool determine risk reduction and cost benefit of mitigation?

Does not address risk reduction processes.	x		x				x	x		
Directs risk reduction steps for particular measures.		x		x	x	x				
Estimates risk reduction effectiveness in terms of threat, vulnerability, and consequence of loss of a particular asset.									x	x
Estimates risk reduction effectiveness in terms of threat, vulnerability, and consequence of loss in context of a larger system and the entire sector.										

Question	Range of Replies	Assessment Tool							
		AWWA, Interim Voluntary Security Guidance for Wastewater / Storm water Utilities, December 9, 2004							
		ASDWA/NRWA, Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems Serving Populations Between 3,300 and 10,000, November 13, 2002							
		ASIS, Business Continuity Guideline, 01 2005							
		BITS, BITS Guide to Business-Critical Telecommunications Services, November 2004							
		Compendium of Supporting Documents to the National Strategy for Critical Infrastructure Assurance Version 1.0, May 13, 2002.							
		DOE, Energy Infrastructures Risk Assessment Checklists for State Governments, December 4, 2001							
		EOC Checklist							
		NIST SP800-53, Recommended Security Controls for Federal Information Systems, February 2005							
		USCG, Navigation and Vessel Inspection Circular NO. 05 03, December 15, 2003							

Descriptive Section

Addresses both critical structure and critical function identification and analyzes the probability and/or range of credible consequences.									
--	--	--	--	--	--	--	--	--	--

6. Risk Reduction: Does the CI-VA / RM Tool determine risk reduction and cost benefit of mitigation?

Does not address risk reduction processes.						X	X	X	X
Directs risk reduction steps for particular measures.			X		X				
Estimates risk reduction effectiveness in terms of threat, vulnerability, and consequence of loss of a particular asset.	X			X					
Estimates risk reduction effectiveness in terms of threat, vulnerability, and consequence of loss in context of a larger system and the entire sector.									

Assessment Tool	RAND, Finding and Fixing Vulnerabilities in Information Systems, The Vulnerability Assessment and Mitigation Methodology, 2003	Securities Industry Association, Business Continuity Planning Committee Critical Infrastructure Guide	BITS ITSP Expectations Matrix	ODP, State Homeland Security Assessment and Strategy Program, Special Needs Jurisdiction Tool Kit	Risk Analysis and management for Critical Asset Protection (RAMCAP™)	DHS, Target Capability List	Commission on Accreditation for Law Enforcement Agencies (CALEA)	Emergency Management Accreditation Program (EMAP)	National Incident Management System (NIMS)	Sandia National Labs, Risk Assessment Methodology for Water (RAM-W)
Question	Range of Replies									

Descriptive Section

Addresses both critical structure and critical function identification and analyzes the probability and/or range of credible consequences.	x			x	x			x		
--	---	--	--	---	---	--	--	---	--	--

6. Risk Reduction: Does the CI-VA / RM Tool determine risk reduction and cost benefit of mitigation?

Does not address risk reduction processes.		x	x				x			
Directs risk reduction steps for particular measures.	x					x			x	x
Estimates risk reduction effectiveness in terms of threat, vulnerability, and consequence of loss of a particular asset.				x	x			x		
Estimates risk reduction effectiveness in terms of threat, vulnerability, and consequence of loss in context of a larger system and the entire sector.										

Question	Range of Replies	"Good Practice" tools										
Assessment Tool		The Vulnerability Self Assessment Tool™ (VSAT) for Water & Wastewater Utilities	FEMA, Reference Manual to Mitigate Terrorist Attacks Against Buildings	Kaiser Center Hazard and Vulnerability Analysis	NCR Healthcare Organization Guided Vulnerabilities Assessment and Preparedness Planning	Media Security and Reliability Council (MSRC) Adopted Best Practices Recommendations	NRIC Best Practice	National Security Telecommunications Advisory Committee (NSTAC) Reports	FFIEC Guidelines, BITS studies and recommendations for IT security	Banking and Financial Regulatory and Supervisory Oversight	General Industry Practices - Trade Associations National, State, Regional	Loudon County: Hazard Identification and Risk Analysis

Descriptive Section

Addresses both critical structure and critical function identification and analyzes the probability and/or range of credible consequences.		x										
--	--	---	--	--	--	--	--	--	--	--	--	--

6. Risk Reduction: Does the CI-VA / RM Tool determine risk reduction and cost benefit of mitigation?

Does not address risk reduction processes.			x									
Directs risk reduction steps for particular measures.	x			x	x	x	x					x
Estimates risk reduction effectiveness in terms of threat, vulnerability, and consequence of loss of a particular asset.		x		x				x	x	x		
Estimates risk reduction effectiveness in terms of threat, vulnerability, and consequence of loss in context of a larger system and the entire sector.								x	x	x		

Assessment Tool	American Petroleum Industries: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries	ODP: Special Needs Jurisdiction Tool Kit	Ohio DOT: Guide to conducting Critical Asset Protection Self Assessments
Question	Range of Replies		

Descriptive Section

Addresses both critical structure and critical function identification and analyzes the probability and/or range of credible consequences.			
--	--	--	--

6. Risk Reduction: Does the CI-VA / RM Tool determine risk reduction and cost benefit of mitigation?

Does not address risk reduction processes.			x
Directs risk reduction steps for particular measures.			
Estimates risk reduction effectiveness in terms of threat, vulnerability, and consequence of loss of a particular asset.			
Estimates risk reduction effectiveness in terms of threat, vulnerability, and consequence of loss in context of a larger system and the entire sector.	x	x	

Appendix D: Bibliography

American Chemistry Council, *Handling and Transportation Guide for Ethylene, Refrigerated Liquid - Cryogenic Ethylene*, (April 2004).

American Chemistry Council, *Responsible Care® Security Code*, Fact sheet (September 2003)

American Chemistry Council, *Site Security for the U.S Chemical Industry* (October 2001).

American Chemistry Council, *Transportation Security Guidelines for the U.S Chemical Industry*.

American Petroleum Industries: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, (May 2003).

American Water Works Association (AWWA) *Interim Voluntary Guidelines for Designing an Online Contaminant Monitoring System* (December 2004).

American Water Works Association (AWWA), *Interim Voluntary Security Guidance for Water Utilities* (December 2004).

American Water Works Association (AWWA), *Interim Voluntary Security Guidance for Wastewater / Stormwater Utilities* (December 2004).

AMSA, *"Asset Based Vulnerability Checklist for Wastewater Utilities"* (January 2002). ASIS, *Business Continuity Guideline, A practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery* (January 2005).

ASIS, *Threat Advisory System Response Guideline (TASR), Considerations And Potential Actions in Response to the Department of Homeland Security Advisory System*. (September 2004).

Association of State Drinking Water Administrators/National Rural Water Association (ASDWA/NRWA), *Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems Serving Populations Between 3,300 and 10,000* (November 2002).

Banking and Finance Sector-*Compendium of Supporting Documents to The National Strategy for Critical Infrastructure Assurance*, Version 1.0, (May 2002).

BITS ITSP *Expectations Matrix*

BITS, *BITS Guide to Business-Critical Telecommunications Services*, (November 2004).

BITS, *Framework for Managing Technology Risk for IT Service Provider Relationships* version II (November 2003).

BITS, Calculator: *BITS Key Risk Measurement Tool for Information Security Operational Risk* (2004).

Commission on Accreditation for Law Enforcement Agencies (CALEA):
<http://www.calea.org/>

Commonwealth of Virginia State Corporation Commission, Special Report Of The Division Of Communications, *Preparation for and Response to Hurricane Isabel by Virginia's Telecommunications Providers* (September 20,2004).

Contingency Planning Guide for Information Technology Systems (June 2002)

Critical Infrastructure Assurance Office (CIAO), *Vulnerability Assessment Framework 1.1* (October 1998).

Department of Defense, *"Physical Security Evaluation Guide Form"* (July 1996).

Department of Energy (DOE), *"Vulnerability Assessment Methodology, Electric Power Infrastructure "* (September 2002).

Department of Energy (DOE), *Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities* (August 2002).

Department OF Homeland Security, Target Capability List Version 1.1, Office of State and Local Government Coordination and Preparedness, (May 2003).

Department of Justice (DOJ), NIJ Special report, Final Version: *"A Method to Assess the Vulnerability of U.S. Chemical Facilities"* (November2002).

Department of the Treasury, *Improving Business Continuity in the Financial Services Sector: A Model for Starting Regional Coalitions* (December 2004).

Department of the Treasury, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (March 2005).

Department of Veterans Affairs, *"Physical Security Assessment for Department of Veterans Affairs Facilities, Recommendations Of The National Institute Of Building Sciences Task Group"* (September 2002).

Department of Energy, *Energy Infrastructure Vulnerability and Risk Assessment Checklists for State Governments*, Draft Version (December 2001).

Emergency Management Accreditation Program (EMAP): EMAP standard. (2004)
Louisville, KY: Emergency Management Accreditation Program (EMAP).
<http://www.emaponline.org/>

Emergency Operation Center (EOC) *Assessment Checklist Guide Emergency Planning Response and Recovery for Company of all Sizes.*

EPA 816-F-02-025, *Protect Your Water For Life: Vulnerability Assessment Factsheet* (November 2002).

Federal Deposit Insurance Corporation, *Risk Assessment Tools and Practices for Information System Security*, (July 1999).

Federal Financial Institutions Examination Council (FFIEC), *Business Continuity Planning - BCP, IT Examination Handbook* (March 2003).

Federal Financial Institutions Examination Council (FFIEC), *Information Security - IS, IT Examination* (December 2002).

Federal Financial Institutions Examination Council (FFIEC), *Management - MGT, IT Examination Handbook* (June 2004).

Federal Financial Institutions Examination Council (FFIEC), *Operations - OPS, IT Examination Handbook* (July 2004).

FEMA, *Emergency Management Guide for Business and Industry. A step-By-step approach to emergency, planning, response and recovery for companies of all sizes.*

FEMA, *Reference Manual to Mitigate Terrorist Attacks Against Buildings*, Risk Management Series, FEMA 426 (December 2003).

Federal Reserve Bank of New York, *Best Practices to Assure Telecommunications Continuity for Financial Institutions and the Payment and Settlements Utilities*, (September 2004)

George Mason University, *Coordinating Critical Transportation Infrastructure Vulnerability Assessment and Needs Prioritization for the National Capital Region* PUBP 710/722 Practicum (June 2003).

Kaiser Center Hazard and Vulnerability Analysis, 2001 Kaiser Foundation Health Plan, Inc. http://www.gnyha.org/eprc/general/templates/Hazard_Assessment_KP.pdf

Media Security and Reliability Council (MSRC) *Adopted Best Practices Recommendations*, (Dec. 2003) http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-241972A1.doc

National Communications System (NCS), *Public Switched Network Assessment Guidelines* (September 2000).

National Communications System (NCS), *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Internet Communications*, An Awareness Document (December 2000).

National Defense research Institute (RAND), *Finding and Fixing Vulnerabilities in Information Systems, The Vulnerability Assessment and Mitigation Methodology* (2003).

National Environmental Training Center, *"Protecting Your Community's Assets: A Guide for Small Wastewater Systems "* (November 2002).

National Incident Management System (NIMS): <http://www.fema.gov/nims>

National Infrastructure Advisory Council (NIAC), *Best Practices for Government to Enhance the Security of National Critical Infrastructures*(April 2004).

National Infrastructure Advisory Council (NIAC), *Cross Sector Interdependencies and Risk Assessment Guidance* (January 2004).

National Institute of Standards and Technology (NIST) Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems* (June 2002).

National Institute of Standards and Technology (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (February 2005).

National Institute of Standards and Technology (NIST), Technology Administration U.S. Department of Commerce *"Security Self-Assessment Guide for Information Technology Systems"* Special Publication 800-26 (2001).

National Security Telecommunications Advisory Committee (NSTAC), *Vulnerabilities Task Force Report Concentration of Assets: Telecom Hotels* (February 2003).

National Security Telecommunications Advisory Committee (NSTAC) Reports: NSTAC Protecting Systems Task Force Report on Enhancing the Nation's Network Security Efforts, (May 2000).

Network Reliability and Interoperability Council Best Practices 2004: www.bell-labs.com/user/krauscher/nric/

NFPA 1600, *Standard on Disaster / Emergency Management and Business Continuity Programs*, (2004 Edition).

NISCC, *Good Practice Guide, Telecommunications Resilience*. V1.0 (May 2004)

North American Electric Reliability Council (NERC), *"Security Guidelines for the Electricity Sector"* version 1,0 (June 2002).

NPRA, *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries*. (May 2003).

Ohio Department of Transportation: Guide to conducting Critical Asset Protection Self Assessments: http://transit.safety.volpe.dot.gov/training/Archived/EPSSeminarReg/CD/documents/OHIO_DOT/CriticalAsset.doc

Office of the Comptroller of the Currency, 2000-14: *Infrastructure Threats – Intrusion Risks*, (May 2000).

Office of the Comptroller of the Currency, 99-9: *Infrastructure Threats from Cyber-Terrorists*, (March 1999).

Office of the Comptroller of the Currency, 98-38: Technology Risk Management: PC Banking Description, Guidance for Bankers and Examiners, (May 2000).

Office of the Comptroller of the Currency, 98-3: Technology Risk Management – Control of Risks Associated with Technology, (February, 1998).

Office for Domestic Preparedness (ODP), *State Homeland Security Assessment and Strategy Program Special Needs Jurisdiction Tool Kit*.

President's Information Technology Advisory Committee, Report to the President *Cyber Security: A Crisis of Prioritization* (February 2005).

Risk Analysis and Management for Critical Asset Protection (RAMCAP), *Applied to Terrorism and Homeland Security*, version 1.x (August 2005).

Sandia National Labs, Risk Assessment Methodology for Water (RAM-W): <http://www.sandia.gov/ram/RAMW.htm>

SAND2001-3188, Unlimited Release, *Development of the Capabilities to Analyze the Vulnerability of Bulk Power Systems* (October 2001)

Securities Industry Association (SIA), *Business Continuity Planning Committee, Critical Infrastructure Guide*, (January 2005).

TCRP/SCAN-JNB/JBSMAB-03-006, *Summary of Resources Prioritizing Transportation Anti-Terrorism Security Measures* (February 2003).

The American Association of State Highway and Transportation Officials (ASHTO), *"A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection* (May 2002).

The National Academy of Sciences, *Public Water Supply Distribution Systems: Assessing and Reducing Risks* - First Report ISBN: 0-309-54967-1 (2005).

The Payments Risk Committee, *Best Practices to Assure Telecommunications Continuity for Financial Institutions and the Payment & Settlements Utilities* (New York, September 2004).

U.S. Department of Transportation (USDOT), *Vulnerability Assessment of the Transportation Infrastructure Relying of the Global Positioning System*, Final Report (August 2001).

U.S Department of Commerce, Manual of Security Policies and Procedures, *"Department of Justice Standards for Protection of Federal Facilities"* (April 2003).

U.S Department Of Justice, *"Fiscal Year 1999, State Domestic Preparedness Support Program, "Assessment and Strategy Development Tool Kit"*.

U.S. Coast Guard (USCG), *Navigation and Vessel Inspection Circular NO. 05 03*, (December 15, 2003).

U.S. Department of Transportation (USDOT), *Transit System Security Program Planning Guide*, final report (January 1994).

U.S. Department of Transportation (USDOT), *Vulnerability Assessment of the Unauthorized Access to Customer Information and Customer Notice*, (March 2005)

USCG/DHS, *Outer Continental Shelf Facility Security Plans Review*, (USCG-2003-14759).

The Vulnerability Self Assessment Tool™ (VSAT) for Water & Wastewater Utilities - <http://www.vsatusers.net/overview.html>

This Page Intentionally Blank