Risk-Assessment Methodologies for Use in the Electric Utility Industry

Version: 09/09/05

Prepared by the Risk-Assessment Working Group
of the North American Electric Reliability Council's
Critical Infrastructure Protection Committee

Foreword

One of the goals of the Risk-Assessment Working Group (RAWG) of the North American Electric Reliability Council's (NERC) Critical Infrastructure Protection Committee (CIPC) is to encourage the development of risk-assessment capability within the electricity sector by identifying applicable risk-assessment methodologies. This document helps meet that goal by providing an overview of approaches to risk assessments and guidance on risk-assessment methods applicable in the electricity sector.

Based on the response to the draft of this document, there is clearly a desire within the industry to better understand risk and risk assessments. The document is structured such that methodologies can easily be added or deleted based on the needs or experience of the industry. The RAWG intends to review and revise the document annually.

This document would not have been possible without the tireless effort of the coordinating author, Garill Coles, and the assistance of the contributing authors: Ted Almay, Jeff Dagle, Steve Dische, Tom Flowers, Bill Flynt, Cliff Glantz, Scott Mix, Lyman Shaffer, Chris Shepherd, and Bob Windus. The review and guidance given by Stuart Brindley and Pat Laird, Chair and Vice-Chair of the CIPC, were also invaluable and are gratefully acknowledged.

Ted Heller
Chair, Risk-Assessment Working Group

Executive Summary

To protect against terrorism and other threats, national security strategies are being developed with an emphasis on protecting critical infrastructure and other key assets. Unified protection efforts, involving both public and private partnerships, are being initiated.

The electricity sector is one of the major components of North America's critical infrastructure. As part of the effort to improve the security and robustness of the electricity industry, the industry itself must continue its efforts to evaluate threats, identify potential vulnerabilities, understand consequences, characterize risks, and make efficient and cost-effective risk-management decisions. In 2002, the North American Electric Reliability Council's (NERC) Critical Infrastructure Protection Committee (CIPC) issued security guidelines on vulnerability and risk assessments for the electricity sector. This document is a supplement to the 2002 guidelines and provides summary information on security risk assessments. It also includes background information, the basic components of security risk assessments, tips on how to set up a risk-assessment framework, and several risk-assessment methods that may be used as part of an organization's risk assessment.

The risk assessments presented in this document are briefly described below.

- The Edison Electric Institute (EEI) Security Committee has recently developed a basic approach to assessing the risk and vulnerability of an electric company's key facilities. This approach can be used by asset owners from large combination gas and electric companies to small entities with minimal security staffs.
- The U.S. Department of Homeland Security (DHS) is developing the Risk Analysis and Management for Critical Asset Protection (RAMCAP), a comprehensive approach to risk assessment in all critical infrastructures (i.e., from simple screening tools to sophisticated quantitative methods).
- Australia/New Zealand Risk Management Guideline (AS/NZS 4360:2004) provides general risk-assessment and management guidance.
- The U.S. Department of Energy (DOE) Vulnerability and Risk Assessment Program (VRAP) is focused on vulnerability assessments.
- Risk Assessment Methodology for Dams (RAM-D^{SM}) and Risk Assessment Methodology for Transmission (RAM-T^{SM}) provide tools for assessing security risks for dams and electrical power transmission systems.

- The Pacific Northwest National Laboratory's Communication Assessment Prioritization Program (CAPP) provides qualitative and semiquantitative tools that are adaptable for evaluating security risks.
- The American Electric Power (AEP) method uses an "attack tree" to identify and characterize risks.
- The Electric Power Research Institute (EPRI) developed the "Security Vulnerability Self-Assessment Guidelines for the Electric Power Industry" to provide guidance, templates, and checklists to assess security vulnerability.

This is not an all-inclusive list; however, it represents the large number of tools and techniques available. Some methods are applicable to a particular kind of asset (e.g., dams or computer systems) while others are more general. Some approaches have a track record while others have not yet been finalized. Some approaches involve detailed analytical assessments while others are more basic. Regardless of the method used, the assessment should answer three important questions: What is critical? What is vulnerable? What can be done to reduce the vulnerabilities?

In selecting a risk-assessment approach, an organization should choose one appropriate to its objectives, requirements, and available resources.

Acronyms, Definitions, and Initialisms

AEP	American Electric Power
CAPP	Communication, Assessment, and Prioritization Program
CIPC	Critical Infrastructure Protection Committee
Consequence	The damage to a component, system, or facility resulting from harm or perpetrated threat.
Critical Assets	Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.
Critical Cyber Assets	Those cyber assets essential to the reliable operation of critical assets.
Cyber Assets	Those programmable electronic devices and communication networks including hardware, software, and data essential to the operation of bulk electric system assets.
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
EEI	Edison Electric Institute
Entity	The facility or critical asset owner or operator
FBI	U.S. Federal Bureau of Investigation
Incident	Any physical or cyber event that disrupts, or could lead to a disruption, of the functional operation of a critical asset, or compromises, or attempts to compromise, the electronic or physical security perimeters.
Intruder	Any unauthorized individual or any individual performing unauthorized activity within a facility or asset.
NERC	North American Electric Reliability Council
Physical Security Perimeter	The border surrounding any facility and other clearly defined locations wherein critical assets are housed and access is controlled.
PNNL	Pacific Northwest National Laboratory
RAMCAP	Risk Analysis and Management for Critical Asset Protection

RAM-D^{SM}	Risk Assessment Methodology for Dams
RAM-T^{SM}	Risk Assessment Methodology for Transmission
Risk	A measure of uncertainty concerning the likelihood and consequence of a future event.
Risk Assessment	Awareness, identification, analysis, and determination (quantitative or qualitative) of risk to a facility or asset.
Threat	Any event or circumstance with the potential to endanger an asset or a population.
VRAP	Vulnerability Risk-Analysis Program
Vulnerability	The degree to which a component, system, or facility is open to attack or damage.

Contents

Figures

1.0 Introduction

To protect against terrorism and other threats, national security strategies are being developed with an emphasis on protecting critical infrastructure and other key assets. Unified protection efforts, involving both public and private partnerships, are being initiated.

The electricity sector is one of the major components of North America's critical infrastructure. As part of the effort to improve the security and robustness of the electricity industry, the industry itself must continue its efforts to evaluate threats, identify potential vulnerabilities, understand consequences, characterize risks, and make efficient and cost-effective risk-management decisions. In 2002, the North American Electric Reliability Council's (NERC) Critical Infrastructure Protection Committee (CIPC) issued security guidelines on vulnerability and risk assessments for the electricity sector. This document is a supplement to the 2002 guidelines and provides summary information on security risk assessments. It also includes background information, the basic components of security risk assessments, tips on how to set up a risk-assessment framework, and several risk-assessment methods that may be used as part of an organization's risk assessment.

The goal of this document is to assist organizations in identifying and adapting risk-assessment methods to evaluate threats to key assets, identify potential security vulnerabilities, estimate the potential consequences of an adverse event, and characterize risk levels. This document presents an overview of a number of risk-assessment approaches that represent the large number of tools and techniques available. Some approaches are applicable to a particular kind of asset (e.g., dams or computer systems) while others are more general. Some approaches have a long track record while others have not yet been finalized. Some approaches are detailed analytical assessments while others are relatively basic but may be quite reasonable given the circumstances. In choosing a risk-assessment approach, an organization should evaluate its objectives, requirements, and available resources. Risk-assessment information can be combined with information on potential protective measures and mitigation techniques to make cost-effective risk-management decisions.

This document is divided into seven chapters and eight Web-accessible appendices. Chapter 2 presents background on critical infrastructure protection and focuses on threats to critical infrastructure and potential vulnerabilities. Chapter 3 defines "risk" and "risk assessment" and discusses the role that risk assessment can play in identifying and managing security risks. Chapter 4 presents guidance on choosing a risk-assessment method. Chapter 5 provides a brief overview of several available risk-assessment methods. Chapter 6 presents follow-up considerations, and Chapter 7 provides references. Appendices A through H provide detailed information on individual risk-assessment methods and are available via the Internet.

2.0 Critical Infrastructure Protection: Threats and Vulnerabilities

A critical infrastructure protection program is an important element in effectively dealing with threats and vulnerabilities. Threats are posed by an individual or a group that possess the capability to do harm and the intent to do harm. Domestic and international terrorists, adversary nations, disaffected individuals or groups, disgruntled employees, and organized adversarial groups are all potential sources of threat. Threats may originate from individuals or groups with knowledge of the systems and equipment used in the electric power industry. Although insider information may be held by disgruntled or compromised employees within North America, detailed information on equipment and operating procedures may also be gathered from open sources or from employees or former employees.

In targeting critical infrastructure, potential adversaries may employ a wide range of conventional methods of attack, including bombs, guns, or chemicals. They are also gaining expertise in less traditional means, such as cyber attacks. Cyber or information attacks involve the use of digital control and information systems to deny, exploit, corrupt, or destroy an adversary's resources. As critical infrastructure and business systems become more reliant on interconnected computer systems, more and more damage can be done to economic resources through cyber warfare or telecommunications disruptions.

To assess threats, one commonly accepted framework involves identifying the threat purveyors' objectives and goals, potential targets, the means by which a threat might be carried out, and the knowledge and tactics required. This process is useful to identifying realistic threats.

There is a distinction between threats and hazards. Hazards are situations or things that possess inherent and known danger. Empirical databases concerning hazards exist or can be created from historical records to determine the statistical probability of a future event. The effects of an incident involving a hazard can be forecast with relative precision because of the hazard's known attributes. Security threats are more difficult than routine hazards to characterize or quantify. The capabilities and intent of the purveyor of a threat may not be known, and the adaptive, thinking nature of the purveyor makes statistical analysis and calculations of probability a challenge.

The assessment of hazards falls within the discipline of safety, while the assessment of threats and protection against them fall within the discipline of security. Often, the same group within an enterprise manages the responsibility for both sources of risk. Some safety and security efforts are mutually reinforcing; however, safety and security are not synonymous and the two disciplines are different.

The ease and low cost of acquiring attack capability and conducting an attack illustrate the need for an effective security system. In addition, business trends, such as deregulation and globalization, have heightened infrastructure vulnerability by increasing the interdependence of one infrastructure on others. While each component or asset in the electricity sector is unique,

most facilities have security vulnerabilities. Some facilities are located in remote areas, some are easily accessible and open to the public, and some are unmanned. Nearly all facilities have key assets that are exposed. For dams, such assets include spillways and flood-control gates, flow-control systems, concrete gravity and arch sections, earth embankments, turbines, navigation locks, and internal galleries. For transmission facilities, such as substations, such assets include critical transformers, circuit breakers, reactors, and control and monitoring systems.

For most facilities, physical security is often the primary concern. However, for many facilities, cyber security is also an important consideration. Facilities with very tight physical security may have digital connections (e.g., modems, network connections, and wireless connections) that make them vulnerable to cyber exploitation. A cyber attack can be as disruptive as a physical attack.

Vulnerability to physical or cyber attack varies from one facility to another. Any methodology must consider the unique characteristics of each site. It is assumed that a perpetrator knows where and what to attack to disrupt or destroy the operations of electrical and mechanical systems. We must therefore know at least as much as potential perpetrators to effectively counter the attack. We must also understand the capabilities of the existing physical protection system. Also critical is the complete understanding of the consequences of a security-system failure. By developing this understanding, risks can be accurately assessed.

In spite of the complexities of the security issue, many government agencies, industry groups, and private enterprises have made progress towards development of guidance for critical infrastructure protection. Government agencies include the U.S. Departments of Homeland Security (DHS), Energy (DOE), and Defense (DoD), and Public Safety and Emergency Preparedness Canada. Within the electricity sector, support has been provided by NERC, the Edison Electric Institute (EEI), and EPRI.

3.0 General Information: Risk, Risk Assessment, and Risk Management

3.1 What is Risk?

Everyone routinely assesses risks in their everyday lives — even if they are unaware of it. For example, we assess risk when we consider what car to buy, what speed to drive given the current weather and traffic conditions, whether to drive or fly to vacation destinations, whether to immediately pull over and rest or press on when starting to feel tired, and whether or not to pass a slower-moving vehicle on a narrow two-lane road. These decisions are not typically made using a formal, quantitative risk-evaluation process; however, risk is still implicitly considered when choosing a course of action. Some people have a higher tolerance for risk than others.

In its simplest mathematical form, risk is the product of probability and consequence (Equation 3.1).

Risk = probability that an adverse event will occur × consequences of that adverse event (3.1)

Some formulations of risk break the probability term down into more specific components that capture information on target selection, the initiation of an attack, the effectiveness of protective and mitigation measures, and other factors. Other formulations assume that a threat exists and that an attack will be launched. By assuming the probability of an attack is 1.0, risk becomes dependent on the effectiveness of existing protective and mitigation measures to prevent an adverse event from producing significant consequences

Estimating the probability of an adverse event can be much more difficult than estimating the consequences of an adverse event. Asset owners and operators familiar with a class of assets can generally determine the consequences of that asset being damaged, manipulated, or destroyed. This determination should include both familiar and unusual consequences. The consequences might include human health and safety implications, environmental implications, business impacts (short-term and long-term), regulatory implications, and public perception impacts. A post-event analysis of every large-scale emergency should be performed to glean lessons-learned in these areas.

3.2 What is Risk Assessment?

Risk assessment is a process for systematically evaluating and comparing risks. Although many risk-assessment methodologies exist, most share a common logic and sequence. Figure 3.1 illustrates the key steps found in almost every structured risk assessment. These steps include an identification and characterization of assets, threats, countermeasures, vulnerabilities, probabilities of an adverse event, and consequences of an adverse event. The order of the steps may vary. The amount of time and attention provided to each element will also vary according to the approach taken and the particular objectives. Each step in the risk-assessment process will be described in more detail in Section 4.1.

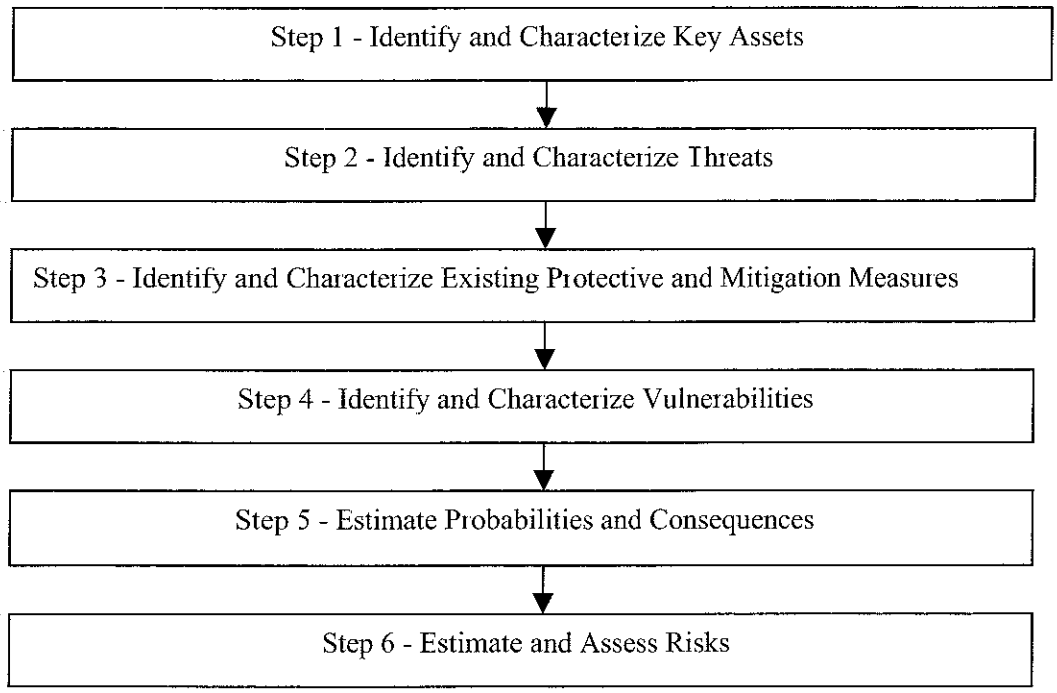

Figure 3.1. General Steps in a Risk Assessment

In a risk assessment, statistical analysis and calculations relating to the probability and frequency of the risk event may be used to determine the likelihood, when known. Where no relevant or reliable data are available, subjective estimates may be used. To avoid subjective biases in the evaluation of the risks, past records, industry practice and experience, organizational experience, experimentation, and specialist or expert judgment may be employed. When possible, confidence metrics should be reported for each risk-level estimate.

3.3 What is Risk Management?

Risk management is the process of managing the likelihood of an adverse event. Risk assessment is a component of risk management. Risk management provides an integrated management approach. Figure 3.2 shows a common risk-management approach. Items 1 through 4 are the risk-assessment portion of this method. Item 5 represents the risk-management activities conducted after the risk assessment is completed.

In general, risk is managed as a portfolio, addressing enterprise-wide risk across the scope of operations. Risk management addresses "inherent," or pre-action, risk (i.e., risk that would exist absent any action) as well as "residual," or post-action, risk (i.e., the risk that remains after actions have been taken).

One or more of the following techniques can be used to manage risk: avoidance, mitigation, acceptance, and transfer. Avoidance is preventing an incident from happening. Mitigation is reducing the likelihood or consequences of an incident. Acceptance is understanding that not all risks can be eliminated and assuming that portion of risk that management cannot — or chooses not to — prevent, mitigate, or transfer. Transfer of risk is moving risk to another party, perhaps through insurance, contract, or other techniques.

Protection of both physical and cyber assets is a necessary component of risk-management for the electric power industry. Security measures address risk avoidance, mitigation, and acceptance. However, risk assessment must precede risk management.

3.4 Why Perform Risk Assessment and Management?

A common management maxim is that one cannot manage what is not measured. Failure to conduct a systematic risk assessment will make any risk-management program problematic, leading to wasted resources and ineffective security.

A properly executed risk assessment focuses an enterprise's efforts on the most significant risk and provides data supporting prudent, appropriate, and cost-effective management controls where they are needed most.

3.5 Limitations of Risk Assessment and Risk Management

Even with robust security measures, risk will remain. There is no perfect system, no single correct answer, and no perfect security. Because of the thinking and adaptive nature of perpetrators — always seeking surprise in the time, manner, and place of their attacks —an event may occur or an unanticipated attack succeed.

1. Identification of assets and loss impacts
    - 1.1 Determine the critical assets that require protection
    - 1.2 Identify possible undesirable events.
    - 1.3 Prioritize the assets based on consequence of loss

2. Identification and characterization of the threat
    - 2.1 Identify threat categories and potential adversaries.
    - 2.2 Assess intent and motivation of the adversary.
    - 2.3 Assess capability of adversary or threat
    - 2.4 Determine frequency of threat-related incidents based on historical data.
    - 2.5 Estimate degree of threat relative to each critical asset and undesirable events.

3. Identification and analysis of vulnerabilities using a realistic threat
    - 3.1 Identify potential vulnerabilities related to specific assets or undesirable events.
    - 3.2 Identify existing countermeasures and their level of effectiveness in reducing vulnerabilities
    - 3.3 Estimate the degree of vulnerability relative to each asset.

4. Assessment of risk and the determination of priorities for the protection of critical assets
    - 4.1 Estimate the degree of impact relative to each critical asset
    - 4.2 Estimate the likelihood of an attack by a potential adversary.
    - 4.3 Estimate the likelihood that a specific vulnerability will be exploited. The estimate can be based on factors such as prior history or attacks on similar assets, intelligence, and warning from law enforcement agencies, consultant advice, the company's own judgment, and additional factors.
    - 4.4 Prioritize risks based on an integrated assessment.

5. Identification of risk-reduction measures, costs, and trade-offs.
    - 5.1 Identify potential countermeasures to reduce the vulnerabilities
    - 5.2 Identify potential facility changes that reduce the consequences from an event.
    - 5.3 Estimate the cost of the countermeasures.
    - 5.4 Conduct a cost-benefit and trade-off analysis.
    - 5.5 Prioritize options and recommendations for senior management.

Figure 3.2. A Commonly-Used Approach to Risk Management

4.0 Risk Assessment in the Electricity Sector

4.1 Types of Risk Assessments – Qualitative, Semiquantitative, and Quantitative

Risk-analysis applications vary in refinement and precision, depending on the information and data available. Analysis methods may be qualitative, semiquantitative, or quantitative

4.1.1 Qualitative Risk Assessment

A qualitative risk assessment may be used to identify assets that need to be assessed in more detail and to support simple and rapid assessments. In a qualitative framework, a single assessor or a team may compile information. Quantitative information may be captured and reported in a qualitative risk assessment, but risk levels are determined subjectively. Qualitative analysis is often used where numerical data are inadequate or unavailable. A qualitative approach is also used when resource limitations (e.g., staffing, staff expertise, or budget) and schedules prohibit a more quantitative assessment. Figure 4-1 presents a sample form that may be used for a qualitative analysis. Separate forms may be completed for each asset. Entries that cannot fit in the space provided should be continued on separate forms.

As in all risk assessments, qualitative assessments start with information gathering on risk factors. After the information is gathered and analyzed, risks are evaluated subjectively. In such assessments, levels such as "acceptable risk" or "unacceptable risk" or similar terms may be used. Alternatively, risk levels may be classified as low, medium, or high.

Assets with unacceptably high risk levels may be immediately targeted for risk reduction. Other assets may be subjected to further examination using a semiquantitative or quantitative approach. These methods support a cost-effective risk-management strategy that prioritizes risk-management activities.

Qualitative Risk-Assessment Information Form

Asset Name: _____ Risk-Assessment Coordinator: _____
Date Assessment Began: _____ Date Assessment Completed: _____

Step 1 - Identify and Characterize Key Assets: _____
_____
_____
_____
_____
Sources of Information:

Step 2 - Identify and Characterize Threats: _____
_____
_____
_____
Sources of Information: _____

Step 3 - Identify and Characterize Existing Protective and Mitigation Measures: _____

_____

_____

_____

_____

_____

Sources of Information: _____

Step 4 - Identify and Characterize Vulnerabilities: _____

_____

_____

_____

_____

_____

Sources of Information: _____

Step 5 - Estimate Probabilities and Consequences:

_____

_____

_____

_____

Sources of Information: _____

Step 6 - Estimate and Assess Risk (Overall Risk Rating): _____

Suggested Follow-up Actions: _____

Figure 4.1. A Sample Information Reporting Form for a Qualitative Risk Assessment

4.1.2 Semiquantitative Assessment

Semiquantitative assessments use relative scales to describe risk. For example, risk may be put into categories such as negligible, low, medium, high, or very high. The number of risk levels defined may be as few as three or as many as ten or more.

In a semiquantitative approach, different scales are used to characterize the probabilities of adverse events and their consequences. The analyzed probability and consequence do not need to bear a precise relationship to the real likelihood or consequence for the analysis to proceed, as long as an ordinal level of detail exists. The objective is to produce an ordered ranking of risks as opposed to an actual quantification of risk. Care should be exercised in interpreting the results of a semiquantitative analysis since the results do not reflect the true relationships between the analyzed risks, only the relative order in which the level of risk should be analyzed, particularly in cases of extreme likelihood or consequence.

4.1.3 Quantitative Assessments

Quantitative analysis uses absolute numerical quantities for both consequence and likelihood. The accuracy of the analysis depends on the completeness and accuracy of the quantities used. Quantitative analysis often uses monetary consequences and historically derived statistical probability rather than subjective estimates for the analysis. Quantitative analysis can often be used to focus risk analysis on extreme events. It cannot be used where pure numerical values cannot be accurately derived (e.g., loss of business, goodwill).

When estimates used in the quantitative analysis are imprecise, a sensitivity analysis should be performed to determine what effects changes in assumptions might have on the calculated level of risk.

For some components of the electricity sector, formal quantitative risk assessments are performed routinely. In other areas of the electricity sector, risk assessments are typically less structured.

4.2 Steps in a Risk Assessment

For many years, a simple framework for conducting risk assessments (as presented in Figure 3-1) has been used by security professionals within the electricity sector. This approach has been used by organizations from small companies to large corporations. This approach is well-suited for conducting qualitative assessments, including many screening-level risk assessments. More

thorough and detailed applications of this approach, often employing structured techniques and models, are used for performing in-depth risk assessments.

In any risk assessment, gathering appropriate information is critical to success. Internal and external resources may be needed to provide sufficient information to identify and characterize assets, threats, existing security measures, vulnerabilities, and the consequences of security events. The following paragraphs identify the main actions and information needed in each step of a risk-assessment process.

Step 1- Identify and Characterize Key Assets

Asset identification and characterization set the scope for the risk evaluation. Organizations should focus on critical assets, as defined by NERC, or on assets that are deemed essential or important to the entity. Such assets, if destroyed, degraded, or compromised, could have an appreciable impact on electric power service, reduce the number or effectiveness of redundant or backup systems, affect environmental quality, negatively affect business objectives, or adversely affect the public perception of the organization.

For asset identification and characterization, information will be needed on the asset's role, setting, operational requirements, and infrastructure requirements, any interdependencies with peer companies, security management policy and procedures relating to the asset, and any formal organizational framework for identifying and assessing risks.

Activities conducted in this step include:

- Defining the organization's critical functions and services.
- Defining the resources (technology, staff, and facilities) that support each critical function or service
- Documenting any critical events or services that are time-sensitive or predictable and require a higher-than-normal priority.
- Identifying any critical non-electronic media required to support the organization's critical functions or services.
- Identifying key relationships and interdependencies among the organization's critical resources, functions, and services.

Step 2- Identify and Characterize Threats

To identify and characterize threats, the assessment team should review its own history of incidents and obtain information from government agencies on the current threats posed against the organization's type of assets. An entity's security department may already be routinely gathering this information, in which case all that may be needed would be a simple reevaluation.

If an organization's security department is not routinely collecting this information and monitoring the threat environment, an appropriate person within the risk-management, emergency planning, or operations groups should be given this assignment. The organization may also contract with a professional security consulting firm or request assistance from industry partners or groups in collecting and evaluating threat information.

In a qualitative assessment, the characterization of threats may be superficial or nonexistent. The type of adversaries considered should be presented explicitly. If a type of threat is omitted from consideration, such as the threat posed by organizational insiders, this omission should be noted. In the absence of a known threat, a general threat assumption should be used.

Step 3 - Identify and Characterize Existing Protective and Mitigation Measures

This step involves the identification and detection of protection measures currently deployed to reduce the likelihood or consequences of an adverse event. A careful inspection of the asset or interviews with asset owners, asset operators, and security experts should help to identify existing protective and mitigation measures. Physical, organizational, and cyber-security measures should be characterized. In the realm of physical security, protective measures might include fences, vehicle barriers, intrusion detection alarms, surveillance equipment, and secure enclosures. In the organizational realm, they might include background checks for employees, an employee identification system (e.g., security badges), restrictions on vendor access to equipment, and a behavioral observation program for employees. In the realm of cyber security, they may include communication flow controls, access controls, modem protections, software checks, and operating system settings.

This step also involves identifying and characterizing the mitigation measures available to reduce the consequences of an adverse event. Asset owners, asset operators, and emergency response personnel are often excellent sources for such information. Mitigation measures include spare-parts inventories for critical equipment, mutual-aid agreements, and backup systems and plans.

Step 4 - Identify and Characterize Vulnerabilities

The vulnerability assessment involves reviewing the physical layout and the existing protection of critical company facilities and systems. The risk-assessment team should solicit information from staff members familiar with the role, equipment, operational procedures, interconnections, and interdependencies of the assets being assessed. Questions about the physical, cyber, and organizational security of the asset and its components, interconnections, and interdependencies should be raised.

Some risk-assessment methods provide a list of questions to ask when assessing vulnerabilities. Lacking a predefined list of questions, the open-ended questions may be directed toward asset

owners and operators (as the consummate insiders) on how they might destroy, damage, or compromise the asset.

Step 5 - Estimate Probabilities and Consequences

This step uses information on the key assets, potential threats, protection and mitigation measures, and vulnerabilities to estimate the probability of an adverse event and the consequences of that event. How much effort goes into estimating the probabilities and consequences of adverse events depends on the type of risk assessment being conducted. In a qualitative assessment, probability information may be collected but not assessed. The probability of an adverse event is often too difficult to characterize or very uncertain—putting it outside the scope of many qualitative and some semiquantitative approaches.

The potential consequences are evaluated based on the function of the asset and what might happen if the asset were damaged, destroyed, or compromised. The impact of mitigation measures should be considered in this assessment. An assessment may discuss impacts in a number of areas (e.g., public /worker health and safety, continuity of service to customers, business impacts to the organization, regulatory impacts, or public perception impacts), or it may focus on just one critical area. Consequences are often based on both the severity and duration of the negative impact (e.g., loss of power to many customers for a period of several hours)

Activities conducted in this step of the risk-assessment process include:

- Estimating the decline in effectiveness over time of each critical function or service.
- Estimating the maximum elapsed time that a critical function or service can be unavailable without a catastrophic impact.
- Estimating the maximum amount of information or data that can be lost without a catastrophic impact to a critical function or service.
- Estimating financial losses over time for each critical function or service
- Estimating tangible (nonfinancial) impacts over time for each critical function or service.
- Estimating intangible impacts over time for each critical function or service.
- Identifying any existing interim or workaround procedures for the organization's critical functions or services.

Step 6 - Estimate and Assess Risks

In this last step of the risk-assessment process, the information gathered in previous steps (particularly Step 5) is used to develop estimates of the risk levels for the assets being considered. As discussed in Section 5.2, different techniques are employed for estimating risk

based on the needs of the assessment. Regardless of how risk is estimated, at the end of the process, the team must prepare a narrative report describing the means used to assess the risk and the findings from each step of the process. This report will be considered sensitive and proprietary and must be protected from unauthorized release. The report conveys the risk-assessment results for subsequent use in risk-management decisions. The report also serves as a reference for future risk assessments.

5.0 Performing a Risk Assessment

This section discusses the selection and conduct of a risk assessment, the use of risk-assessment tools, and risk-assessment approaches.

5.1 Guidance for Selecting and Conducting a Risk Assessment

Some key considerations when designing a risk- assessment include:

- Scope and objectives of the risk assessment.
- Makeup of the risk-assessment team.
- Methods to gain the cooperation of asset owners, asset operators, and other information providers.
- Procedures for identifying the assets to be assessed.
- Characterization of threat information.
- Characterization of protection and mitigation measures.
- Characterization of vulnerability information.
- Characterization of the probabilities and consequences of adverse events.
- Presentation and documentation of risk information.
- Peer review of assessment team results.

5.1.1 Scope and Objectives of the Risk Assessment

The scope and objectives of the risk assessment are critical in determining the risk-assessment method used. In defining the scope and objectives, the following questions must be considered.

- How broad is the scope of the risk assessment, and how detailed does it need to be? Understanding the scope is essential for planning. The scope helps to determine the technical approach, the schedule of the assessment, and the resources required.
- What are the resource and scheduling constraints for conducting the assessment? Considering the resources available to the risk-assessment team (including budget and personnel) and the schedule for key milestones helps to limit the risk assessment and adopt a workable approach.
- What categories of security are to be considered? Cyber-security risks have increased substantially in the past few years because of the growing importance of digital systems in the electric power industry, the increase in digital connectivity, and the relative ease of mounting a cyber attack. It is recommended that any risk assessment consider physical, organizational, and cyber threats and vulnerabilities. Organizational security addresses vulnerabilities in operational practices and encompasses security clearances and background checks for workers, security training, continuous observation programs to identify potential behavioral problems before they escalate, and security requirements for vendors and contractor employees. Cyber security involves safeguarding the confidentiality, availability, and integrity of computer resources, digital controls, and electronic data.
- Which assets need to be assessed? In some risk assessments, attention may be focused on only a few critical assets. In other studies, the assessment may cover a much broader set of assets important to the organization's operations and income. It is important to understand whether the assessment needs to focus on large systems or facilities or individual components of the systems or facilities (e.g., to help identify where vulnerabilities may be concentrated).
- Will this be a new assessment or a follow-up to a previous assessment? For a follow-up to a previous assessment, information may be readily available. However, the existing data would have to be reviewed for relevancy and accuracy.
- Who is the sponsor for the risk assessment and who will be using the results? The sponsor may play a major role in setting requirements. The users of the risk assessment will help determine the level of detail and complexity required.
- How will the results of the risk assessment be used? If the risk assessment will provide input for a particular risk-management tool or technique, this factor may determine whether the risk assessment needs to be qualitative, semiquantitative, or quantitative. Figure 5.1 illustrates how the determination of scope, schedule, and resources influences the selection of a risk-assessment method.
- What is needed from senior managers to support the risk assessment? The support of senior managers is essential for gaining the resources to conduct a risk assessment. Senior management may also help marshalling the support and cooperation of other needed participants.

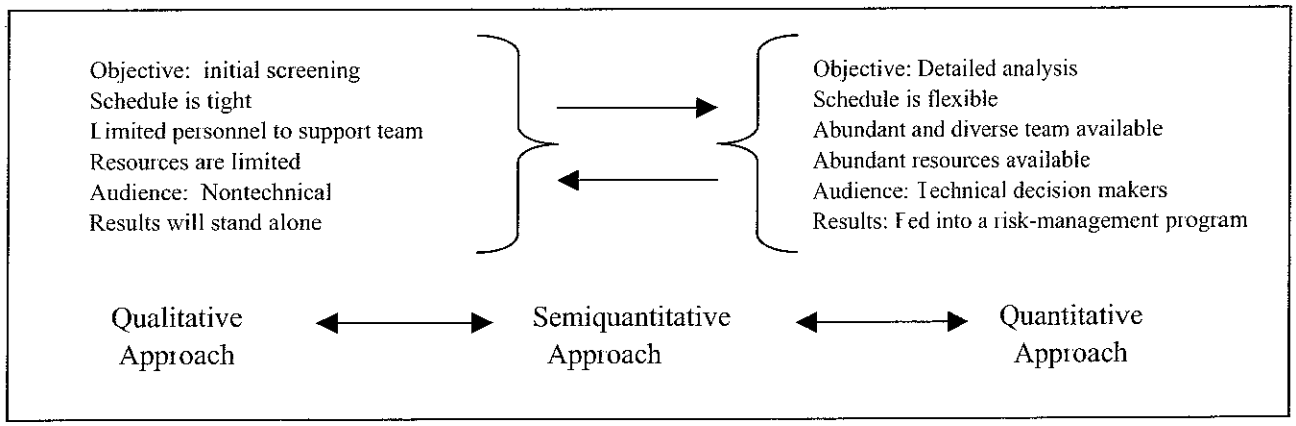

Figure 5.1. The Influence of Scope, Schedule, and Resources on the Selection of a Risk-Assessment Method

5.1.2 Risk-Assessment Team

To perform the risk assessment, the knowledge and expertise of a wide range of technical experts is essential. These include personnel with expertise in the operation of the asset, its components, and interconnections. Also required are participants knowledgeable in physical, organizational, and cyber security. Moreover, expertise in environmental, business, emergency response, disaster recovery, public relations, and regulatory matters may be of assistance in evaluating potential consequences

In addition to skilled team members, communication within the risk-assessment team is important. This may be achieved by regular meetings or electronic communications.

5.1.3 Gaining the Cooperation of Staff Members

A risk assessment is only as accurate as the information used in generating the estimates. Staff members may become defensive when vulnerability and consequence information is requested about their assets. They may assume that vulnerabilities in the system or asset under their purview will be perceived negatively and indicate a failure to properly secure the asset. As a result, potential vulnerabilities and associated consequences may be minimized by knowledgeable staff members. To avoid this problem, all participants in the risk-assessment should be thoroughly briefed on the objectives and purpose of the assessment. Asset owners must be assured that the results of the study will be used solely to address security issues and that there will be no negative implications in having higher risk scores. Complete and accurate information cannot be obtained without first gaining the trust and cooperation of asset owners, operators, and information providers.

5.1.4 Identifying Assets

Asset identification and characterization is the first major step of information-gathering in a risk assessment. A thorough understanding of the scope and objectives of the risk assessment will help set the parameters for identifying the assets and determining the type and amount of information needed to support the assessment.

Asset identification should include the preparation of a written description of what each asset does; the role it plays; and what might happen if the asset were destroyed, disabled, or otherwise compromised. This information would include direct impacts on the electric power supply and indirect impacts (e.g., impacts on other assets involved in providing electric power, impacts on business systems, impacts on safety and security systems). In general, the more quantitative the risk assessment, the more quantitative the information must be in the characterization of the assets

5.1.5 Characterizing Threats

The identification and characterization of threats is the next major step in many risk assessments. This step is optional and is sometimes skipped. In such cases, it is often assumed that threats simply exist and will be carried out. The risk assessment then moves on to the characterization of protective measures, vulnerabilities, and the probabilities and consequences of an adverse event. If threats are characterized as part of the risk assessment, information should be obtained from various governmental and industry sources. The uncertainty in quantified threat information should also be considered as part of the assessment.

An important element of the threat assessment is an understanding of an adversary's knowledge of the assets and his or her vulnerabilities. It is easy to underestimate the knowledge and capabilities of an adversary, particularly when insider information is involved. Because the equipment and practices of the electric power industry are well documented world wide, it may be easy for an adversary to gather inside information from industry workers in other organizations.

5.1.6 Characterizing Protection and Mitigation Measures

The identification and characterization of existing protection and mitigation measures is the third step of a risk assessment. It is often conducted simultaneously with the vulnerability assessment. Information on protection and mitigation measures may be obtained through interviews with asset owners/operators and emergency response personnel. It can also be obtained from on-site

inspections, which may reveal measures that were not reported, were erroneously described during interviews, or have been modified in the field.

As part of this characterization, formal physical and cyber-security programs should be described, including an explanation of how these programs work. Security policies, procedures, hardware, and software should be listed as well as plans to mitigate adverse events.

5.1.7 Characterizing Vulnerability Information

Characterizing vulnerabilities is the fourth step in the risk-assessment process. Vulnerabilities are typically addressed after identifying and characterizing the key assets, potential threats, and the security measures employed to protect them. The timing of this step is independent of the third step of identification and characterization of existing protection and mitigation measures. Depending on the scope of the study, the assessment of vulnerabilities should consider both "outsider" and "insider" threats. While insider threats may be considered less credible, they should still be assessed first. The likelihood of an insider threat can be characterized in the fifth step, discussed below.

The assessment of vulnerabilities may require input from staff members with expertise in a number of different fields. Asset owners/operators can provide some information while physical, organizational, and cyber-security specialists may be able to fill in any gaps

5.1.8 Characterizing Information on Probabilities and Consequences

Estimating probabilities of an adverse event and evaluating potential consequences is the fifth step in the risk-assessment process. For a simple qualitative assessment, this step may be quite simple, or it may be skipped. In some semiquantitative risk-assessment approaches, probability may not be considered explicitly. Instead, a surrogate for likelihood may be used — such as a measure of the susceptibility of the asset to exploitation. It is important, particularly for quantitative approaches, that the probability estimates include an indication of the uncertainty.

The characterization of consequences may be an inaccurate or incomplete element in risk assessment. Potential consequences may be underestimated by asset owners/operators. Consequences are often seen as emerging from a chain of events and alternative pathways that may result in great consequences are sometimes missed. Careful questioning of systems personnel may assist them in exploring different scenarios. For example, the most obvious consequence of a cyber-security event may be the loss of availability of a digital asset while the more severe consequence may be the loss of integrity of the asset (e.g., a system seems to be operating normally but is actually performing erroneously).

A consequence assessment must consider a broad range of consequences including human health and safety, environmental concerns, continuity of operations, and economic, business revenue, regulatory, and stakeholder/public perception impacts. If one or more of these areas are neglected, the overall consequences may be underestimated. For example, an organization that focuses on the continuity of power may miss adverse impacts in the areas of business revenue or public perception.

5.1.9 Presenting Results and Providing Documentation

Documentation of risk results and the supporting technical information is an important component of a risk assessment. Documentation provides a record of the information used to formulate an assessment and serves as a reference for the risk-assessment team. It may be used to provide technical support and quality assurance information during any peer or independent reviews of the risk assessment. Documentation is also very useful for future studies.

5.1.10 Technical Review of Assessment Team Results

After a risk assessment is completed, an independent peer review of the assessment findings is recommended. The peer review may be conducted by internal or external reviewers. The purpose of the peer review is to ensure that the results are calculated according to the method report, that results are free of error, and that the results "make sense". Questionable results should be reviewed for accuracy. If the peer-review team has questions about some of the results, it might indicate that additional explanation is needed.

5.2 Using an Existing Risk-Assessment Tool, Model, or Guidance Document

A risk-assessment team may apply a risk-assessment tool, model, or guidance document directly or modify it to better meet its goals. The following are a collection of tools, models, and guidance documents used in the energy sector for risk-assessment:

- EEI Security Committee's Approach.
- DHS Risk Analysis and Management Approach for Critical Asset Protection (RAMCAP).
- Australia/New Zealand Standard (AS/NZS 4360:2004) Risk Management.
- DOE Vulnerability and Risk Assessment Program (VRAP).
- Risk Assessment Methodology for Dams (RAM-D) and Risk Assessment Methodology for Transmission (RAM-T).

- Pacific Northwest National Laboratory (PNNL) Communication Assessment Prioritization Program (CAPP).
- AEP model.
- The EPRI "Security Vulnerability Self-Assessment Guidelines for the Electric Power Industry."

In considering the above approaches, an organization should weigh the scope of its planned assessment and the capabilities of the existing approaches against the resources required to implement the approach.

Ultimately, entities should adopt a risk-assessment process that fits the culture of the organization, exposes critical asset interdependencies, assesses risks, determines levels of risk acceptance (risk posture), and identifies required and cost-justified controls.

Tools to facilitate the conduct of risk assessments, such as tables, questionnaires, and standard report formats, help ensure a consistent approach and prevent teams from "reinventing the wheel." Such tools can be developed in-house or can be adapted from those used by others. Computerized methods help speed up the documentation process and provide easy access to data collected and risk-assessment results. Those responsible for risk-assessment should periodically refine the tools based on experience. Most of these tools are simple, but some can automate most of the analysis process.

5.3 Discussion of Selected Risk-Assessment Approaches

In this section, selected risk-assessment approaches are summarized.

5.3.1 Edison Electric Institute (EEI) Security Committee Vulnerability Risk Assessment Model

The EEI Security Committee has developed a basic low-cost approach to assessing the risk and vulnerability of an electric company's assets. This straightforward method, based on the DOE VRAP methodology and the NERC vulnerability assessment guideline, follows the approach taken by corporate security professionals in the industry for many years. It can be used by both large and small entities where a high degree of analytical rigor is unnecessary.

Analysis Approach:

The first step of the process is to make a list of critical facilities and systems.
A cross-functional team should participate.

The second step is to conduct a risk assessment. The senior security staff member from the corporate security department should contact federal and local agencies to obtain their assessment of the generic risk posed against classes of facilities (i.e., control rooms, substations, power plants, hydro generation facilities, etc.). If a company does not have a professional security staff, a staff member from the risk-management, emergency planning, or operations groups should be given this assignment. The company can also contract with professional security consulting firms.

The third step is to conduct a vulnerability assessment of the critical facilities and systems. This assessment involves reviewing the physical layout and existing protection of these facilities and systems. The quickest way to conduct the assessment is to form a team consisting of a physical security professional and an operational person familiar with that type of facility. Someone familiar with the information technology structure and someone from the engineering staff could also participate.

The fourth step is to identify mitigation measures such as physical security, work processes, or emergency-response strategies, which could reduce the vulnerability of an asset or class of assets. The fifth step involves implementing those mitigation measures identified.

As the sixth and final step, the team would prepare a straightforward, narrative report describing the means taken to assess the risk, its identification of vulnerabilities, and recommended mitigation measures. Because threat conditions are not static, the company would continue to monitor them. It would promptly reevaluate the vulnerabilities and mitigation measures if the nature of the risk changed sufficiently. Otherwise, a review of the overall vulnerability assessment should be performed at least annually.

Additional information on this approach is available.

5.3.2 Risk Analysis and Management for Critical Asset Protection (RAMCAP)

RAMCAP is being developed by DHS to provide a common set of methodologies and tools for assessing risks and identifying and developing cost-effective protection and mitigation strategies. RAMCAP will provide approaches and tools to support all critical infrastructures sectors, and also support the development of specialized tools to address the needs of individual sectors.

Some of the tools and techniques employed by RAMCAP will be easy and general. Others will be more sophisticated and should be used only by experienced practitioners and decision-makers. Existing risk assessments based on qualitative methods can be used to support the RAMCAP approach. However, translation and calibration methods must be developed to allow DHS to compare risk-assessment information across sectors.

Additional information on this approach is available.

5.3.3 Australia/New Zealand Standard (AS/NZS 4360:2004) Risk Management

The governments of Australia and New Zealand developed AS/NZS 4360:2004 to provide standardized risk-management guidance for their industries. Rather than require the use of specific tools, this approach established a risk-assessment and management framework. The standard lays out general concepts that can be applied based on organizational needs, structure, culture, objectives, and practices.

The concept of threat and vulnerability to threat are not explicitly addressed in this method. However, it could be used in conjunction with other technical guidance or standards which do so.

The purpose of AS/NZS 4360:2004 is to guide organizations in:

- Establishing a rigorous decision-making and planning process with regard to risks and tradeoffs between risk and returns.
- Providing better identification of threats and opportunities.
- Determining acceptable variability and uncertainty.
- Proactively managing risks, rather than reacting to them.
- Effectively using and allocating resources in risk management.
- Reducing the cost of managing risk, including improving incident management.
- Improving trust and confidence in the organization by stakeholders.
- Improving compliance with applicable legislation.
- Improving corporate governance.

The risk-assessment and management framework lays out an iterative process, consisting of a series of well-defined steps. These steps provide insight into the analysis process and support better decision-making based on the results. However, it is not clear how the standard addresses once-in-a-lifetime events, nor is effective control well defined in the standard. Users of this standard should consider these shortcomings when applying the standard.

The standard describes the following five-step framework. Note that the first three steps are part of the risk-assessment process, and the last two steps involve risk-management activities.

1. Establish the Context – Establish the organization and management context for the remainder of the process. Establish the evaluation criteria and the structure of the analysis to be performed.

2. Identify the Risks – Includes the "what, why, and how" for risks that are identified.

3. Analyze the Risks – Determines existing controls as well as the consequences of the risks. The analysis should also include the likelihoods that the identified risks will occur. The consequence and likelihood of each risk may be combined to produce an estimated risk level.

4. Evaluate the Risks – The estimated risk levels developed in Step 3 are compared against the criteria established in Step 1 to prioritize the risks for management attention. Low levels of risk may be deemed "acceptable" and require no treatment.

5. Treat the Risks – For unacceptable risks, appropriate remediation plans are developed. These plans should include funding.

At each step of the process, actions taken and justification for the actions must be recorded. These records must be sufficient to satisfy an independent (internal or external) audit

Additional information on this approach is available.

5.3.4 Vulnerability Risk Analysis Program (VRAP)

The VRAP is intended to help energy-sector organizations identify and understand the threats to, and vulnerabilities of, their infrastructures and to stimulate action to mitigate significant problems. The VRAP consists of ten actions, each performed by a team of experts:

1. Assess the threat environment.
2. Assess physical security.
3. Conduct a physical asset analysis.
4. Assess operations security.
5. Examine policies and procedures.
6. Conduct an impact analysis.
7. Assess infrastructure interdependencies.
8. Analyze the network architecture.
9. Conduct penetration testing.
10. Conduct a risk characterization.

The objectives of the assessment are to:

- Identify all critical physical and cyber vulnerabilities and develop appropriate response options.
- Identify and rank all key assets from a security perspective.

- Develop the business case for making security investments and organizational changes to enhance security.
- Enhance awareness and make security an integral part of the business strategy.

In addition, the VRAP methodology calls for pre-assessment and post-assessment phases. The pre-assessment phase includes:

- Identifying the assessment objectives and measures of success.
- Specifying the elements of the methodology that will be used in the assessment.
- Engaging knowledgeable personnel and ensuring their access to resources and information.
- Deciding what type of assessment (internal, facilitated, external, or hybrid) to conduct
- Developing an assessment schedule.

The post-assessment phase includes:

- Prioritizing assessment recommendations.
- Developing an action plan.
- Capturing lessons learned and best practices.
- Conducting training.

Additional information on this approach is available

5.3.5 Risk Assessment Methodology for Dams (RAM-D^{SM}) and Risk Assessment Methodology for Transmission (RAM-T^{SM})

The RAM-D^{SM} and the RAM-T^{SM} models are tools to systematically assess and improve the physical protection systems of dams and electrical transmission systems. The RAM-D^{SM} tool ranks the effectiveness of proposed security risk-reduction improvements at dams, thus providing management with a decision-making tool for allocation of resources. The RAM-T^{SM} has been used similarly by U.S. federal power marketing administrations. The RAM methodology helps to define the likelihood of an attack, the consequences of a successful attack, and the effectiveness of the physical protection system in preventing an attack.

To calculate the risk at a particular facility, the methodology uses forms to collect the input factors of the risk equation. The information on the check sheets and worksheets drives the RAM

process through the risk-management sequence. The information required to complete the worksheets comes from published information, observation, expert judgment, experience, and project interviews. The completed worksheets describe the adversaries and estimate the likelihood of an attack by each credible one; estimate the consequences of attacks on critical assets; and estimate the asset vulnerability and the effectiveness of the security system or the likelihood of its defeat. After estimating these factors, the risk equation can calculate a relative risk value.

This methodology provides management justification for reducing any unacceptably high risks. The methodology provides a systematic way to compare the risk reduction afforded by various strategies as well as the costs and impacts of deploying specific security or mitigation efforts.

The risk-reduction module in RAM guides the selection of security system upgrades to protect critical assets or mitigate the vulnerabilities and consequences identified in the analysis. Risk-reduction efforts increase the effectiveness of the security system by applying integrated detection, delay, and response measures. Risk reduction can also be achieved by mitigating consequences through early warning systems, improved emergency evacuation, and other contingency plans. As an alternative business case, the project manager may establish a lower threat definition by accepting the associated risk and preparing for security enhancements during periods of heightened alerts.

Additional information on this approach is available

5.3.6 Communication, Assessment and Prioritization Program (CAPP)

The CAPP provides a risk-assessment and risk-management approach that can address a variety of issues. This approach focuses on identifying issues, collecting information on these issues, assessing the organization's ability to address these issues, conducting simple semiquantitative assessments of risk and ability to manage risk, and improving risk management.

The concept of threat and vulnerability to threat are not explicitly addressed in this method. However, the approach could be used in conjunction with other technical guidance or standards which do so.

The CAPP approach was originally developed as an environmental risk-assessment and management tool, but can be adapted to address security issues. The CAPP process has two major components. The first component, the Qualitative Issue Characterization (QuIC), is used to gather and record information on issues, their potential impacts, and the organization's ability to address these issues. The second component of CAPP, the Semiquantitative Evaluation (SEQUEL), allows staff members to convert the qualitative information collected during the first component into a semiquantitative assessment of risk and the ability of the organization to manage this risk. This information can then be used to make cost-effective risk-management

decisions. The SEQUEL approach can identify areas where the organization is properly managing issues and others where it needs to improve its capabilities or reallocate resources.

The CAPP approach evaluates risks from the perspective of the organization, regulatory agencies, and key stakeholders. Assessors consider consequences that may affect:

- Human health, safety, and environment quality.
- Finance and business performance.
- Regulatory compliance.
- Stakeholder perception.

Initially, the user must formulate a series of potential scenarios that capture events associated with high risks. These include events with low probabilities and substantial consequences and events with high probabilities and less substantial consequences. Once scenarios are developed, the user estimates the risk for each scenario by summing the scores in four impact categories: human health and environment quality, regulatory, business, and stakeholder perception.

In the risk-management component, the user assesses the organization's ability to manage risks by considering the adequacy of existing policies and procedures, the allocation of resources to address problems, and the effectiveness of policy implementation. Different risk-management approaches can be analyzed for their effectiveness in balancing risk and the organization's ability to manage that risk.

Additional information on this approach is available.

5.3.7 American Electric Power (AEP) Attack Tree Methodology

The AEP Attack Tree Methodology is designed to dynamically evaluate business risk associated with both cyber and physical security. In this approach, threat trees (also known as fault trees) are used to determine whether the conditions necessary for a threat to be realized exist and are unmitigated. A threat tree consists of threat outcomes (such as long-term service disruption to a large area) in which preexisting conditions must be true for an adversary to realize the threat (for instance, a circuit breaker is accessible through Internet connectivity). In turn, any condition can have one or more preconditions. Two or more conditions at the same level, sharing the same parent node, can be combined in an "and" or "or" relationship. Determining whether one or more vulnerabilities are associated with a threat is simply a matter of starting at a leaf condition (a node in the threat tree with no child nodes) and following it up to the root threat. If a path is unbroken by a mitigated node or a broken "and" condition exists, a vulnerability exists.

This information, combined with intelligence about adversaries, can be used to create an attack tree. Certain vulnerabilities are more likely to be exploited based on the attacker's capabilities

(resources, geographic location, and industry experience) while others will be virtually impossible to exploit.

The impact of a threat can be calculated quickly from the attack tree, which can in turn be used to justify expenditures on mitigation strategies. Impact can be calculated by adding the financial and operational impact of the root of the tree to any impact created as attackers work their way up the tree. Some of the intermediate nodes in the tree may have an adverse impact, even if the attacker does not have the capabilities to extend further up the tree.

Once an impact is calculated, it is possible to calculate the value of investing in mitigation strategies. Based on the impact and the likelihood of occurrence, it is possible to determine whether countermeasures should be applied to that vulnerability or whether the vulnerability is so difficult to exploit (or has so little impact) that they are unnecessary.

Additional information on this approach is available.

5.3.8 Electric Power Research Institute (EPRI) Security Vulnerability Self-Assessment Guidelines for the Electric Power Industry

EPRI "Security Vulnerability Self-Assessment Guidelines for the Electric Power Industry" provides detailed guidelines and technical information to assist any organization in the electric industry in performing its own security self-assessment. Project management guidelines as well as templates and checklists for information gathering and assessment are supplied.

Many of these guidelines are a compendium of "best practices" and "lessons learned" acquired by members of EPRI's Enterprise Information Security Program in performing their own security assessments. Information from EPRI's members and consultants as well as publicly available information has been included. The approach to developing threat profiles, target selection, and potential attack scenarios comes from EPRI's Electricity Infrastructure Security Assessment, which was undertaken following the events of September 11, 2001.

These vulnerability self-assessment guidelines offer practical suggestions for examining critical assets, facilities, and networks for cyber and physical security weaknesses and assessing the effectiveness of protective measures already in place. The self-assessment is a significant piece of an overarching risk-assessment program. Knowledge of vulnerabilities helps companies develop strategies to reduce their overall exposure.

Additional information on this approach is available.

Follow-On Considerations

This chapter discusses considerations for follow-up after risk assessments. Careful documentation is necessary for reliable analyses, and institutional guidance is needed for managing risk.

6.1 Documentation of Assessment and Follow-On Actions

This section discusses the documentation needed of the assessment, such as prioritization of results and identification of risk-reduction measures. It also discusses needed follow-on activities. For example, if the risk-assessment approach does not include a cost-benefit analysis, then that might be an appropriate follow-on activity

All information collected in risk assessments should be stored in a database for ease of use, simplicity of retrieval, and availability as a future baseline, with care given to the sensitive nature of the information. The documentation may be useful in subsequent analyses and as input for future risk-management plans and risk assessments. Controlled paper copies of the risk analysis may be maintained so that the appropriate managers can monitor risk and the status of risk-control implementation. Additional documentation provided to corporate-level and business-unit management may consist of risk-assessment reports, the status of summary databases, and the business unit's external connectivity status. Internal or external auditors may also use the documentation to review the decisions made during the risk-assessment process. Audit reviews provide a valuable critique of the risk-management decision-making process

A series of standardized reports should be produced from the risk-assessment process, including a detailed risk analysis report and an internal and regulatory compliance report, as well as recommendations for implementation of specific risk-mitigation controls. Care should be given to protecting sensitive information. The reports estimate the costs for each recommended countermeasure, including licensing, training, development, implementation, and recurring support. The organization must consider this information when deciding what new controls to implement and what risks to accept. In addition, the organization should institute procedures to measure the effectiveness of actions taken and their impact on operations.

Each organization needs managerial procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and addressing any identified weaknesses. In addition, recovery plans should be tested periodically in disaster-simulation exercises. Companies should segregate duties within the organization to ensure that one individual cannot control all aspects of a process or computer operation and thereby, intentionally or unintentionally, perform unauthorized actions or gain unauthorized access to assets without detection.

6.2 Development of Management Response to a Study

Ongoing management support is required for the process of vulnerability assessment, risk assessment, disaster recovery, and continuity planning to ensure that, when unexpected events occur, controls are in place. Controls are necessary for critical operations to continue without undue interruption and to ensure that critical and sensitive data are protected. An organization should have procedures in place to protect information resources and minimize the risk of unplanned operational interruptions, as well as a plan to recover critical operations, should interruptions occur. These plans should consider the activities performed at control centers, transmission substations, microwave substations, generation plants, and general support facilities as well as the activities performed by users of specific applications.

6.0 References

Australian/New Zealand Standard, Risk Management. 2004. AS/NZS 4360:2004. Available for purchase on the Internet at http://www.riskmanagement.com.au/

Brown, B. W., B. A. Bowen, F.V. DiMassa, C.S. Glantz, A.L. Roybal, S.J. Ortiz. 1996. *Environmental Risk Communication, Assessment, and Prioritization Program (CAPP) Version 1.1 - User's Guide*. PNNL-11338. Pacific Northwest National Laboratory, Richland, Washington. Information on CAPP available at: http://mepas.pnl.gov/earth/capp.html

Federal Bureau of Investigation (FBI) 2005. *Your Local FBI Office, Field Divisions*. Accessed on February 4, 2005 at http://www.fbi.gov/contact/fo/fo.htm

National Aeronautics and Space Administration (NASA) 2002. *Fault Tree Handbook with Aerospace Applications*. Version 1.1. Accessed February 4, 2005 at http://www.hq.nasa.gov/office/codeq/doctree/fthb.pdf

National Strategy for Physical Protection of Critical Infrastructures and Key Assets. 2003. Accessed February 4, 2005 at http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf

North American Electric Reliability Council (NERC). 2001. *An Approach to Action for the Electricity Sector*. Version 1.0. Accessed February 4, 2005 at ftp://www.nerc.com/pub/sys/all_updl/cip/ApproachforAction_June2001.pdf

North American Electric Reliability Council (NERC). 2002. *Security Guidelines for the Energy Sector: Vulnerability and Risk Assessment*. Version 1.0. Accessed February 4, 2005 at http://www.esisac.com/publicdocs/Guides/V1-VulnerabilityAssessment.pdf

Public Safety and Emergency Preparedness Canada (PSEPC). 20 January 2004. *Selection Criteria to Identify and Rank Critical Infrastructure Assets*. Available at http://www.ocipep.gc.ca/critical/nciap/nci_criteria_e.asp