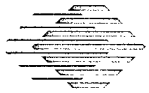


Carnegie Mellon
Software Engineering Institute

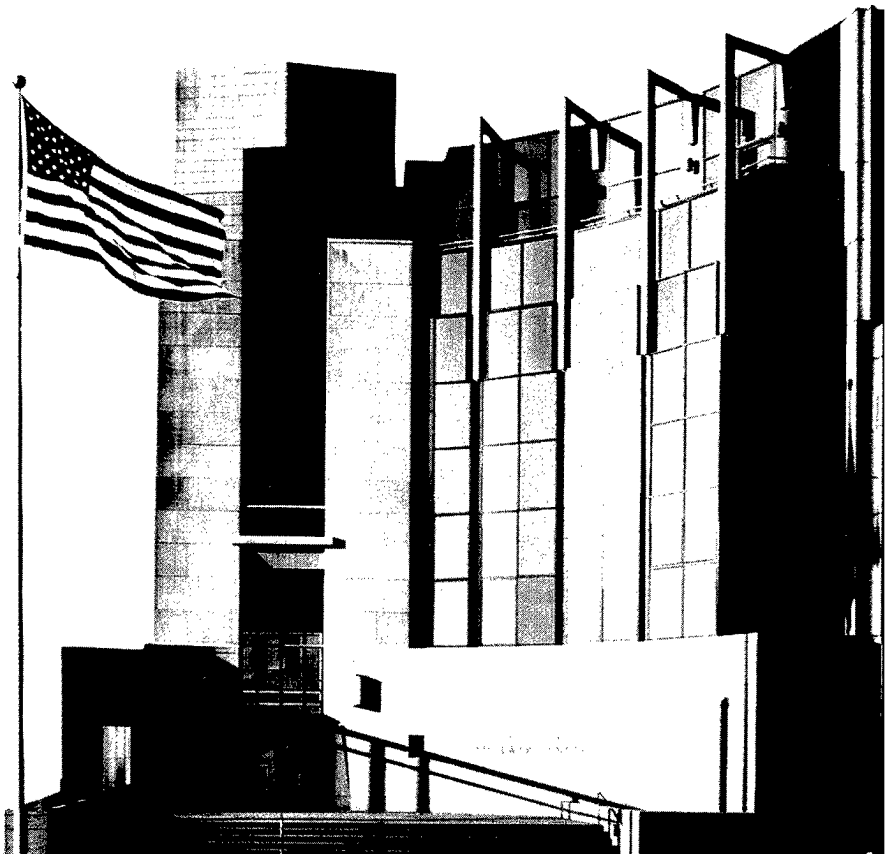
# OCTAVE[SM] Criteria, Version 2.0

Christopher J. Alberts
Audrey J. Dorofee

*December 2001*







TECHNICAL REPORT
CMU/SEI-2001-TR-016
ESC-TR-2001-016

Carnegie Mellon University does not discriminate and Carnegie Mellon University is required not to discriminate in admission, employment, or administration of its programs or activities on the basis of race, color, national origin, sex or handicap in violation of Title VI of the Civil Rights Act of 1964, Title IX of the Educational Amendments of 1972 and Section 504 of the Rehabilitation Act of 1973 or other federal, state, or local laws or executive orders.

In addition, Carnegie Mellon University does not discriminate in admission, employment or administration of its programs on the basis of religion, creed, ancestry, belief, age, veteran status, sexual orientation or in violation of federal, state, or local laws or executive orders. However, in the judgment of the Carnegie Mellon Human Relations Commission, the Department of Defense policy of "Don't ask, don't tell, don't pursue" excludes openly gay, lesbian and bisexual students from receiving ROTC scholarships or serving in the military. Nevertheless, all ROTC classes at Carnegie Mellon University are available to all students.

Inquiries concerning application of these statements should be directed to the Provost, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, telephone (412) 268-6684 or the Vice President for Enrollment, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, telephone (412) 268-2056.

Obtain general information about Carnegie Mellon University by calling (412) 268-2000.

Carnegie Mellon
Software Engineering Institute
Pittsburgh, PA 15213-3890

# OCTAVE[SM] Criteria, Version 2.0

CMU/SEI-2001-TR-016
ESC-TR-2001-016

Christopher J. Alberts
Audrey J. Dorofee

*December 2001*

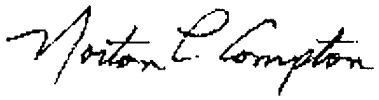
**Networked Systems Survivability Program**

This report was prepared for the

SEI Joint Program Office
HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER



Norton L. Compton, Lt Col., USAF
SEI Joint Program Office

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.



This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 52.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

printed 12/11/2001 12:49 PM version 1 sdc

# Table of Contents

# List of Tables

# Abstract

Today, we rely on access to digital data that are accessible, dependable, and protected from misuse. Unfortunately, this need for accessible data also exposes organizations to a variety of new threats that can affect their information. The Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE[SM]) enables organizations to understand and address their information security risks. OCTAVE is led by a small, interdisciplinary team of an organization's personnel and focuses on an organization's assets and the risks to those assets. It is a comprehensive, systematic, context-driven, and self-directed evaluation approach. The essential elements of the OCTAVE approach are embodied in a set of criteria that define the requirements for OCTAVE. This report describes the OCTAVE criteria. The goal of this report is to define a general approach for evaluating and managing information security risks. Organizations can then develop methods that are consistent with the OCTAVE criteria.

[SM] Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.

# Acknowledgements

We would like to acknowledge the following individuals for reviewing this report and providing comments:

- Julia Allen
- Rich Caralli
- Linda Pesante
- Carol Sledge
- Brad Willke
- Bill Wilson
- Carol Woody

We would also like to acknowledge Suzanne Couturiaux for editing the document and David Biber for providing the graphics.

# 1 Introduction

Security is a complex discipline with both organizational and technological components. Consider the following scenario. A financial organization is required to protect the privacy of its customers. The company's security policy explicitly requires role-based access to information. Management has made a large investment in technology to ensure that the organization complies with its security policy. For example, all major systems have access control mechanisms to restrict access to system resources. When people start to work for the company, they are assigned access to system resources based on their job responsibilities. Compliance with the access control policy is enforced through technological mechanisms.

However, when people leave the company, their access to systems is rarely terminated. Even though these people no longer have roles with the company, they can access its systems and sensitive financial information. In addition, when people change jobs within the company, they not only acquire additional access privileges for the new jobs, they also keep the access privileges from their old jobs. While procedures require that employees be given appropriate access when they move from one job classification to another, those procedures do not require revoking access rights that are no longer necessary. Some people who have been working at the company for many years can access just about anything they want. Even though the company has the technological means for enforcing role-based access to information and systems, organizational practices and incomplete procedures make this fact irrelevant.

Think about how much you rely upon access to information and systems to do your job. Today, information systems are essential to most organizations because virtually all information is captured, stored, and accessed in digital form. We rely on digital data that are accessible, dependable, and protected from misuse. Systems are interconnected in ways that could not be imagined 10 years ago. Networked systems have enabled unprecedented access to information. Unfortunately, they have also exposed our information to a variety of new threats. Organizations need approaches that enable them to understand their information risks and create strategies to address those risks.

The Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE[SM]) enables an organization's personnel to sort through the complex web of organizational and technological issues to understand and address its information security risks. OCTAVE

[SM] Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.

defines an approach to information security risk evaluations that is comprehensive, systematic, context driven, and self directed. The approach requires a small, interdisciplinary analysis team of business and information technology personnel from the organization to lead its evaluation process.

The essential elements, or requirements, of the OCTAVE approach are embodied in a set of criteria. There can be many methods consistent with these criteria, but there is only one set of OCTAVE criteria. At this point, we have developed one method consistent with the criteria. That method, which we documented in the *OCTAVE Method Implementation Guide, v2.0* [Alberts 01a], was designed with large organizations in mind. We are presently developing a method for small organizations. In addition, others might define methods for specific contexts that are consistent with the criteria. Figure 1 illustrates these points.

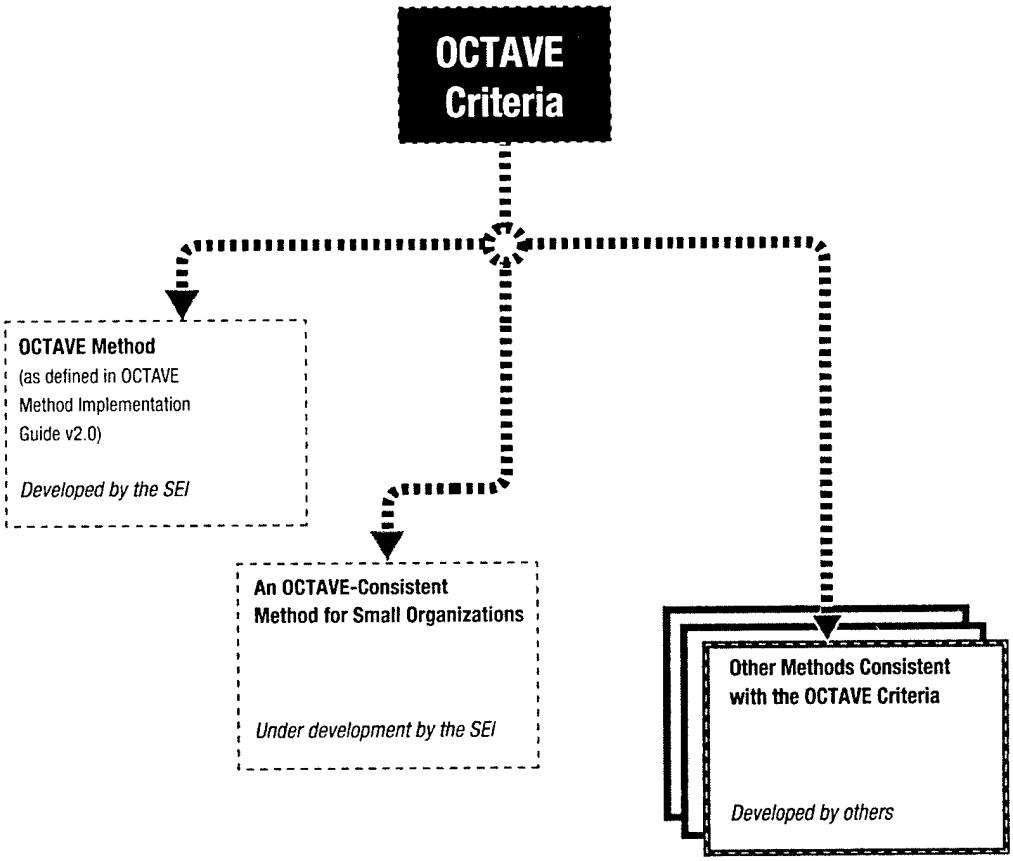



*Figure 1: Multiple Methods Consistent with the OCTAVE Criteria*

Next, we present some background information about how we arrived at the need for a set of criteria.

## 1.1 Background

In June 1999, we published a technical report describing the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework [Alberts 99]. The framework was a specification for an information security risk evaluation targeted at large organizations. The technical report featured a dataflow diagram that specified the components of an information security risk evaluation: a set of eight processes, each with required inputs, activities, and outputs. The development of the framework was based upon our extensive involvement in the development and delivery of the proprietary Information Security Evaluation (ISE) and, earlier, the Software Risk Evaluation (SRE) [Williams 99]. Both techniques were developed previously at the Software Engineering Institute. As we designed the framework, we also incorporated the results of our research into information security risk evaluations that were being conducted throughout the community.

When we first started developing the framework, our goal was to define the requirements for a general approach for evaluating and managing information security risks. However, we realized that a general approach implemented in a small organization of 10 employees would look different than that in a multinational corporation. Thus, we believed that we needed to examine both extremes before we could define the requirements for a general evaluation approach.

We designed the OCTAVE Method with large organizations in mind, using the OCTAVE Framework as a starting point for the method. A second method, targeted at small organizations, is evolving from the OCTAVE Method. The development and testing of these methods helped us to identify the common (or essential) requirements of the OCTAVE approach and has led to the refinement of the framework into the OCTAVE criteria.

## 1.2 Purpose

This technical report documents the OCTAVE criteria. Our goal in writing this document is to define a general approach for evaluating and managing information security risks. We encourage organizations to develop methods that are consistent with the OCTAVE criteria.[1] This document does not provide specific implementation details about any method. For detailed information on the OCTAVE Method, see the *OCTAVE Method Implementation Guide, v2.0.*

[1] Organizations wishing to use the OCTAVE name with their products or services should contact the Software Engineering Institute's licensing agent.

This report is organized as follows:

- Section 2 provides an overview of the OCTAVE approach.
- Section 3 introduces the structure of the OCTAVE criteria.
- Section 4 addresses the principles of OCTAVE.
- Section 5 addresses the OCTAVE attributes.
- Section 6 addresses the OCTAVE outputs.
- Section 7 provides a summary.
- Appendix A provides an example set of activities that produce the required outputs of OCTAVE.
- Appendix B shows the relationship between the OCTAVE criteria and the OCTAVE Method.

# 2 What Is OCTAVE?

An information security risk evaluation must handle both organizational and technological issues to be effective. It must address the computing infrastructure as well as how people use the infrastructure as a part of their jobs. Thus, an evaluation needs to incorporate the context in which people use the infrastructure to meet the business objectives of the organization, as well as technological security issues related to the infrastructure.

## 2.1 Key Concepts

We view using information security risk evaluations to improve an organization's security posture as a sound business practice. Since most organizations rely upon access to electronic data to conduct business, the data need to be adequately protected from misuse. The ability of an organization to achieve its mission and meet its business objectives is directly linked to the state of the computing infrastructure and to the manner in which people interact with the infrastructure. For an organization to be in the best position to achieve its mission, its people need to understand which information-related assets are important, as well as what they should be doing to protect those assets. In other words, people in the organization need to be involved in the evaluation.

*OCTAVE is a self-directed information security risk evaluation.* This core concept of OCTAVE is defined as a situation where people from an organization manage and direct an information security risk evaluation for their organization. The organization's people direct risk evaluation activities and are responsible for making decisions about the organization's efforts to improve information security. In OCTAVE, an interdisciplinary team, called the analysis team, leads the evaluation.

The analysis team includes people from both the business units and the information technology (IT) department, because information security includes both business- and technology-related issues. People from the business units of an organization understand what information is important to complete their tasks as well as how they access and use the information. The information technology staff understands issues related to how the computing infrastructure is configured, as well as what is important to keep it running. Both of these perspectives are important in understanding the global, organizational view of information security risk.

Risk is the possibility of suffering harm or loss. It breaks down into three basic components: asset, threat, and vulnerability. Thus, an information security risk evaluation must account for

all three components of risk. *OCTAVE is an asset-driven evaluation approach.* It requires an analysis team to

- identify information-related assets (e.g., information and systems) that are important to the organization
- focus risk analysis activities on those assets judged to be most critical to the organization

OCTAVE requires the analysis team to consider the relationships among critical assets, the threats to those assets, and vulnerabilities (both organizational and technological) that can expose assets to threats. It requires the analysis team to evaluate risks in an operational context. In other words, *OCTAVE focuses on how operational systems are used* to conduct an organization's business and how those systems are at risk due to security threats.

When a team completes an OCTAVE, it creates a protection strategy for organizational improvement and risk mitigation plans to reduce the risk to the organization's critical assets. Thus, *OCTAVE incorporates both strategic and tactical views of risk.*

## 2.2 Three Aspects – Three Phases

The organizational, technological, and analysis aspects of an information security risk evaluation lend it to a three-phased approach. OCTAVE is organized around these basic aspects (illustrated in Figure 2), enabling organizational personnel to assemble a comprehensive picture of the organization's information security needs. In Section 6 of this document, we explore the phases of OCTAVE in greater detail. The phases are

- *Phase 1: Build Asset-Based Threat Profiles* – This is an organizational evaluation. Staff members from the organization contribute their perspectives on what is important to the organization (information-related assets) and what is currently being done to protect those assets. The analysis team consolidates the information and selects the assets that are most important to the organization (critical assets). The team then describes security requirements for the critical assets and identifies threats to the critical assets, creating threat profiles.
- *Phase 2: Identify Infrastructure Vulnerabilities* – This is an evaluation of the information infrastructure. The analysis team identifies key information technology systems and components that are related to each critical asset. The team then examines the key components for weaknesses (technology vulnerabilities) that can lead to unauthorized action against critical assets.
- *Phase 3: Develop Security Strategy and Plans* – During this part of the evaluation, the analysis team identifies risks to the organization's critical assets and decides what to do about them. The team creates a protection strategy for the organization and mitigation plans to address the risks to the critical assets, based upon an analysis of the information gathered.


*Figure 2: OCTAVE Phases*

## 2.3 Part of a Continuum

OCTAVE provides an organization-wide view of the current information security risks. It provides a snapshot in time, or a baseline, that can be used to focus mitigation and improvement activities. During OCTAVE, an analysis team performs activities to

- *identify* the organization's information security risks
- *analyze* the risks to determine priorities
- *plan* for improvement by developing a protection strategy for organizational improvement and risk mitigation plans to reduce the risk to critical organizational assets

An organization will not improve unless it implements its plans. These improvement activities are performed after OCTAVE has been completed. After OCTAVE, the analysis team, or other designated personnel

- *plan* how to implement the protection strategy and risk mitigation plans by developing detailed action plans. This activity can include a detailed cost-benefit analysis among strategies and actions, and it results in detailed implementation plans.

- *implement* the detailed action plans
- *monitor* the action plans for schedule and for effectiveness. This activity includes monitoring risks for any changes.
- *control* variations in plan execution by taking appropriate corrective actions

Note that these activities are nothing more than a *plan-do-check-act* cycle.

An information security risk evaluation is part of an organization's information security risk management activities. OCTAVE is the evaluation activity, not the continuous process. Thus, it has a defined beginning and end. Figure 3 shows the relationship among these activities and where OCTAVE fits in. In addition, you should note that there is a continuous aspect to the Identify and Analyze activities.

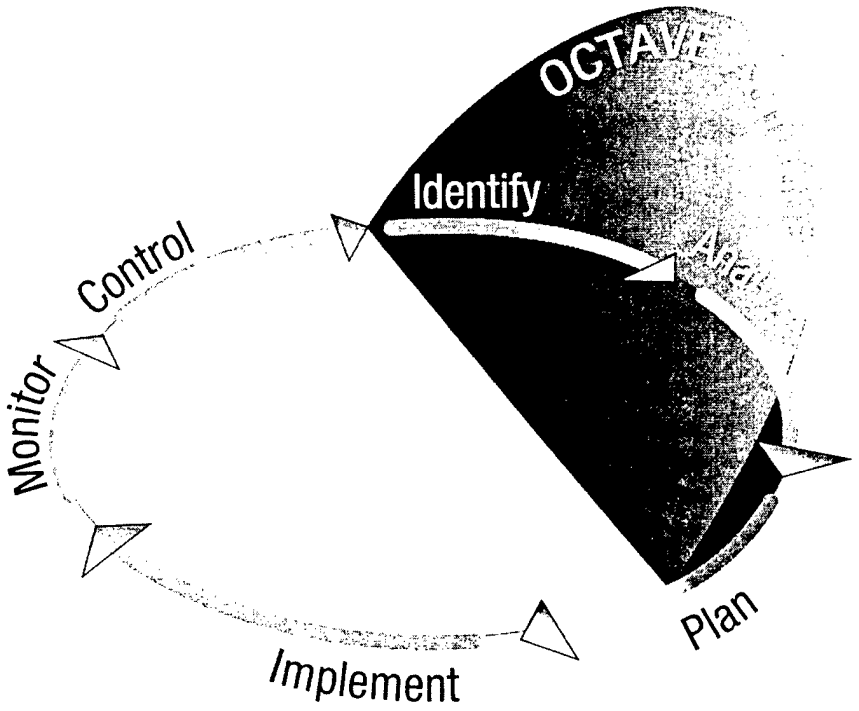



*Figure 3: OCTAVE and Risk Management Activities*

Periodically, an organization will need to "reset" its baseline by conducting another OCTAVE. The time between evaluations can be predetermined (e.g., yearly) or triggered by major events (e.g., corporate reorganization or redesign of an organization's computing infrastructure). In between evaluations, an organization can periodically identify new risks, analyze these risks in relation to existing risks, and develop mitigation plans for them.

## 2.4 Business and Security Practices

To meet its business objectives, each organization implements a unique set of business practices. Because OCTAVE examines the link between organizational, or business, issues and technological issues, the information that an analysis team gathers and the recommendations that it makes can affect other organizational business practices. For example, one organization that performed an OCTAVE identified an action to summarize the results of the evaluation and include the summary as input to its strategic planning process. Many such links exist; however, it is beyond the scope of this document to directly address them.

Finally, we do want to stress one point about how business practices are implemented in organizations. Although many business practices tend to be similar, the specific ways in which practices are implemented in different organizations vary based on the characteristics of the organizations. Consider the differences in management practices at a small start-up company in contrast to the practices required in a large, established organization. Both organizations require a set of similar management practices (e.g., planning, budgeting), but the practices are implemented differently. Similarly, we have found that the way in which organizations implement an information security risk evaluation practice differs based on a variety of organizational factors. OCTAVE implemented in a large multinational corporation is different than OCTAVE in a small start-up organization. However, there are required outputs and attributes of the OCTAVE approach that remain the same across organizational types. In this document, we define those requirements in the form of a set of criteria. In the next section, we highlight the structure of the OCTAVE criteria.

# 3 Structure of the OCTAVE Criteria

The OCTAVE criteria are a set of principles, attributes, and outputs. Principles are the fundamental concepts driving the nature of the evaluation. They define the philosophy that shapes the evaluation process. For example, self direction is one of the principles of OCTAVE. The concept of self direction means that people inside the organization are in the best position to lead the evaluation and make decisions.

The requirements of the evaluation are embodied in the attributes and outputs. Attributes are the distinctive qualities, or characteristics, of the evaluation. They are the requirements that define the basic elements of the OCTAVE approach and define what is necessary to make the evaluation a success from both the process and organizational perspectives. Attributes are derived from the OCTAVE principles. For example, one of the attributes of OCTAVE is that an interdisciplinary team (the analysis team) staffed by personnel from the organization lead the evaluation. The principle behind the creation of an analysis team is self direction.

Finally, outputs are the required results of each phase of the evaluation. They define the outcomes that an analysis team must achieve during each phase. We recognize that there is more than one set of activities that can produce the outputs of OCTAVE. It is for this reason that we do not specify one set of required activities. However, in Appendix A of this document, we present a set of activities that can be used to produce the required outputs.

Table 1, on the next page, highlights the OCTAVE criteria. In the remainder of this document, we formally define each principle, attribute, and output.

*Table 1: The OCTAVE Criteria*

| OCTAVE Criteria | | | | |
|---|---|---|---|---|
| **Principles** | **Attributes** | **Outputs** | | |
| | | **Phase 1 Outputs** | **Phase 2 Outputs** | **Phase 3 Outputs** |
| Self-Direction<br>Adaptable Measures<br>Defined Process<br>Foundation for a Continuous Process<br>Forward-Looking View<br>Focus on the Critical Few<br>Integrated Management<br>Open Communication<br>Global Perspective<br>Teamwork | RA.1 Analysis Team<br>RA.2 Augment Analysis Team Skills<br>RA.3 Catalog of Practices<br>RA.4 Generic Threat Profile<br>RA.5 Catalog of Vulnerabilities<br>RA.6 Defined Evaluation Activities<br>RA.7 Documented Evaluation Results<br>RA.8 Evaluation Scope<br>RA.9 Next Steps<br>RA.10 Focus on Risk<br>RA.11 Focused Activities<br>RA.12 Organizational and Technological Issues<br>RA.13 Business and Information Technology Participation<br>RA.14 Senior Management Participation<br>RA.15 Collaborative Approach | RO1.1 Critical Assets<br>RO1.2 Security Requirements for Critical Assets<br>RO1.3 Threats to Critical Assets<br>RO1.4 Current Security Practices<br>RO1.5 Current Organizational Vulnerabilities | RO2.1 Key Components<br>RO2.2 Technology Vulnerabilities | RO3.1 Risks to Critical Assets<br>RO3.2 Risk Measures<br>RO3.3 Protection Strategy<br>RO3.4 Risk Mitigation Plans |

# 4 Principles of OCTAVE

Principles are the fundamental concepts that define the philosophy behind the evaluation process. They shape the evaluation approach and provide the basis for the evaluation process. We have grouped the principles into the following three areas:

- *Information Security Risk Evaluation Principles*: These are key aspects that form the foundation of effective information security risk evaluations.
  - self direction
  - adaptable measures
  - defined process
  - foundation for a continuous process
- *Risk Management Principles*:[2] These are basic principles common to effective risk management practices.
  - forward-looking view
  - focus on the critical few
  - integrated management
- *Organizational and Cultural Principles*:[2] These are aspects of the organization and its culture that are essential to the successful management of information security risks.
  - open communication
  - global perspective
  - teamwork

The principles are shown graphically in Figure 4.

[2] These principles are similar in scope and intent to those documented in the *Continuous Risk Management Guidebook* [Dorofee 96].

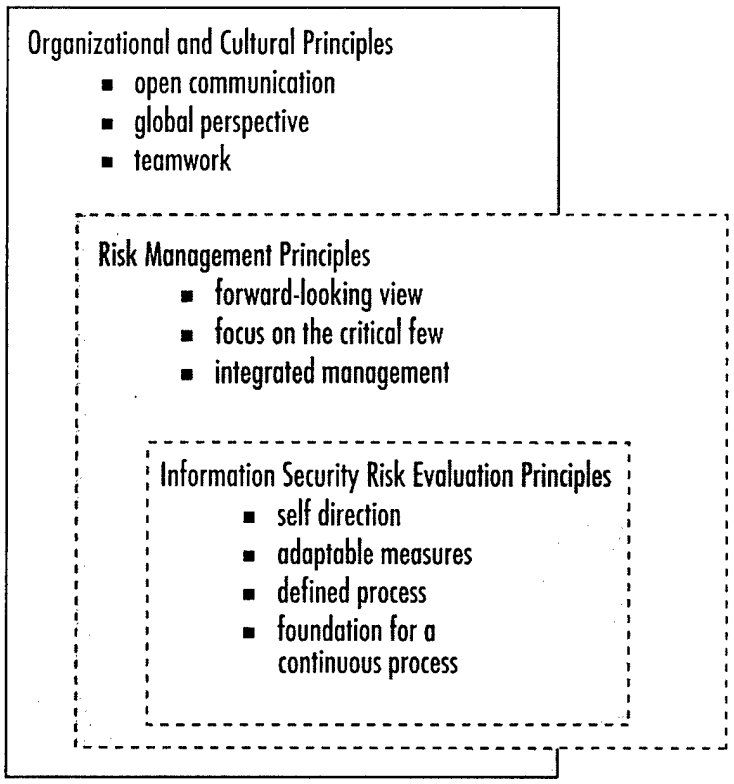



*Figure 4: The Principles of OCTAVE*

## 4.1 Information Security Risk Evaluation Principles

In this section, we focus on principles that form the basis of effective information security risk evaluations, starting with self direction.

### Self Direction

Self direction describes a situation where people in an organization manage and direct information security risk evaluations for their organization. These people are responsible for directing the risk management activities and for making decisions about the organization's security efforts. Self direction requires

- taking responsibility for information security by leading the information security risk assessment and managing the evaluation process
- making the final decisions about the organization's security efforts, including which improvements and actions to implement

## Adaptable Measures

A flexible evaluation process can adapt to changing technology and advancements. It is not constrained by a rigid model of current sources of threats or by what practices are currently accepted as "best." Because the information security and information technology domains change very rapidly, an adaptable set of measures against which an organization can be evaluated is essential. Adaptable measures require

- current catalogs of information that define accepted security practices, known sources of threat, and known technological weaknesses (vulnerabilities)
- an evaluation process that can accommodate changes to the catalogs of information

## Defined Process

A defined process describes the need for information security evaluation programs to rely upon defined and standardized evaluation procedures. Using a defined evaluation process can help to institutionalize the process, ensuring some level of consistency in the application of the evaluation. A defined process requires

- assigning responsibilities for conducting the evaluation
- defining all evaluation activities
- specifying all tools, worksheets, and catalogs of information required by the evaluation
- creating a common format for documenting the evaluation results

## Foundation for a Continuous Process

An organization must implement practice-based security strategies and plans to improve its security posture over time. By implementing these practice-based solutions, an organization can start institutionalizing good security practices, making them part of the way the organization routinely conducts business. Security improvement is a continuous process, and the results of an information security risk evaluation provide the foundation for continuous improvement. A foundation for a continuous process requires

- identifying information security risks using a defined evaluation process
- implementing the results of information security risk evaluations
- setting up the ability to manage information security risks over time
- implementing security strategies and plans that incorporate a best-practice approach to security improvement

## 4.2 Risk Management Principles

Next, we look at broader principles that focus on concepts common to effective risk management approaches.

### Forward-Looking View

A forward-looking view requires an organization's personnel to look beyond the current problems by focusing on risks to the organization's most critical assets. The focus is on managing uncertainty by exploring the interrelationships among assets, threats, and vulnerabilities, and exploring the resulting impact on the organization's mission and business objectives. A forward-looking view requires

- thinking about tomorrow, focusing on managing the uncertainty presented by a range of risks
- managing organizational resources and activities by incorporating the uncertainty presented by information security risks

### Focus on the Critical Few

This principle requires the organization to focus on the most critical information security issues. Every organization faces constraints on the number of staff members and funding that can be used for information security activities. Thus, the organization must ensure that it is applying its resources efficiently, both during an information security risk evaluation and afterwards. A focus on the critical few requires

- using targeted data collection to collect information about security risks
- identifying the organization's most critical assets and selecting security practices to protect those assets

### Integrated Management

This principle requires that security policies and strategies be consistent with organizational policies and strategies. The organization's management proactively considers tradeoffs among business and security issues when creating policy, striking a balance between business and security goals. Integrated management requires

- integrating information security issues in the organization's business processes
- considering business strategies and goals when creating and revising information security strategies and policies

## 4.3 Organizational and Cultural Principles

Finally, we examine the principles that help to create an organizational culture that is conducive to effective risk management.

### Open Communication

Information security risk management cannot succeed without open communication of security-related issues. Information security risks cannot be addressed if they aren't communicated to and understood by the organization's decision makers. A fundamental concept behind most successful risk management programs is a culture that supports open communication of risk information through a collaborative evaluation approach. Often, evaluation methods provide staff members with ways of expressing information so that the information is not attributed to them, allowing for a free expression of ideas. Open communication requires

- evaluation activities that are built upon collaborative approaches (e.g., workshops)
- encouraging exchanges of security and risk information among all levels of an organization
- using consensus-based processes that value the individual voice

### Global Perspective

This principle requires members of the organization to create a common view of what is most important to the organization. Individual perspectives pertaining to information security risk are solicited and then consolidated, creating a global picture of the information security risks with which the organization must deal. A global perspective requires

- identifying the multiple perspectives of information security risk that exist in the organization
- viewing information security risk within the larger context of the organization's mission and business objectives

### Teamwork

No individual can understand all of the information security issues facing an organization. Information security risk management requires an interdisciplinary approach, including both business and information technology perspectives. Teamwork requires

- creating an interdisciplinary team to lead the evaluation
- knowing when to include additional perspectives in the evaluation activities
- working cooperatively to complete evaluation activities
- leveraging people's talents, skills, and knowledge

The principles that we defined in this section are broad concepts that form the foundation for information security risk evaluation activities. Next, we examine how these concepts are implemented in an evaluation approach by focusing on the attributes of OCTAVE.

# 5 OCTAVE Attributes

Attributes are the distinctive qualities, or characteristics, of the evaluation. They form the requirements of the OCTAVE approach and define what is necessary to make the evaluation a success from both the process and organizational perspectives. Each OCTAVE attribute is defined using the following:

- requirements – the essential elements of the attribute
- importance – why the attribute is important to the evaluation process

## 5.1 Relationship Between OCTAVE Attributes and Principles

Earlier in this report, we indicated that the principles of OCTAVE shape the nature of the attributes. Table 2 illustrates the primary relationships between the principles and attributes. Note that each attribute is numbered for easy cross-referencing. In the next section, we define each attribute, beginning with RA.1, Analysis Team.

*Table 2: Mapping OCTAVE Principles to Attributes*

| Mapping of Principles to Attributes | |
|---|---|
| **Principle** | **Attribute** |
| Self Direction | RA.1 Analysis Team |
| | RA.2 Augmenting Analysis Team Skills |
| Adaptable Measures | RA.3 Catalog of Practices |
| | RA.4 Generic Threat Profile |
| | RA.5 Catalog of Vulnerabilities |
| Defined Process | RA.6 Defined Evaluation Activities |
| | RA.7 Documented Evaluation Results |
| | RA.8 Evaluation Scope |
| Foundation for a Continuous Process | RA.9 Next Steps |
| | RA.3 Catalog of Practices |
| Forward-Looking View | RA.10 Focus on Risk |
| Focus on the Critical Few | RA.8 Evaluation Scope |
| | RA.11 Focused Activities |
| Integrated Management | RA.12 Organizational and Technological Issues |
| | RA.13 Business and Information Technology Participation |
| | RA.14 Senior Management Participation |
| Open Communication | RA.15 Collaborative Approach |
| Global Perspective | RA.12 Organizational and Technological Issues |
| | RA.13 Business and Information Technology Participation |
| Teamwork | RA.1 Analysis Team |
| | RA.2 Augment Analysis Team Skills |
| | RA.13 Business and Information Technology Participation |
| | RA.15 Collaborative Approach |

## 5.2 Attribute Requirements

### Analysis Team (RA.1)

**Requirements**

An analysis team staffed by personnel from the organization must lead the evaluation activities. The analysis team must be interdisciplinary in nature, including people from both the business units and the information technology department. The analysis team must manage and direct the information security risk evaluation for its organization, and it must be responsible for making decisions based on the information gathered during the evaluation process.

**Importance**

This attribute is important because it ensures that ultimate responsibility for conducting the evaluation is assigned to a team of individuals from the organization. Using an analysis team to lead the evaluation helps to ensure that

- people who understand the business processes and who understand information technology work together to improve the organization's security posture
- the evaluation is run by personnel who understand how to apply all worksheets and tools used during the evaluation
- the method is applied consistently across the organization
- people in the organization feel "ownership" of the evaluation results, making them more likely to implement the recommended strategies and plans

## Augmenting Analysis Team Skills (RA.2)

**Requirements**

The evaluation process must allow the analysis team to augment its skills and abilities by including additional people who have specific skills required by the process or who possess required expertise. These additional people can be from other parts of the organization, or they can be from an external organization.

**Importance**

The analysis team is responsible for analyzing information and making decisions during the evaluation. However, the core members of the analysis team may not have all of the knowledge and skills needed during the evaluation. At each point in the process, the analysis team members must decide if they need to augment their knowledge and skills for a specific task. They can do so by including others in the organization or by using external experts. This attribute is important because it ensures that the analysis team has the required skills and knowledge to complete the evaluation. This attribute also allows an organization to conduct an information security risk evaluation even when it does not have all of the required knowledge and skills within the organization. Thus, it provides an avenue for working with external experts when appropriate.

## Catalog of Practices (RA.3)

**Requirements**

The evaluation process must assess an organization's security practices by considering a range of strategic and operational security practice areas. These are formally defined in a catalog of practices. (An example can be found in the *OCTAVE Catalog of Practices* [Alberts 01b].) The catalog of practices used by an organization must be consistent with all laws, regulations, and standards of due care with which the organization must comply.

Strategic practices focus on organizational issues at the policy level and provide good, general management practices. They address business-related issues, as well as issues that require organization-wide plans and participation. Since strategic practices are based on good management practice, they should be fairly stable over time. The following list provides an example of typical strategic practice areas:

- *Security Awareness and Training* addresses how well security-related practices are understood by general staff members and information technology staff members. One way to enhance the staff's understanding of information security practice is through training and education.
- *Security Strategy* focuses on the integration of information security issues into the business strategy of the organization.
- *Security Management* defines information security roles and responsibilities as well as management's support for information security activities.
- *Security Policies and Regulations* addresses the organizational and management direction for information security, including which mandated regulations must be met. This area also deals with the staff's understanding of policies and enforcement of policies.
- *Collaborative Security Management* focuses on good practice when working with third parties (contractors, Internet service providers, managed service providers, partners, etc.).
- *Contingency Planning/Disaster Recovery* addresses plans to counteract disruptions in business activities and in systems and networks.

Operational practices focus on technology-related issues dealing with how people use, interact with, and protect technology. They are subject to changes as technology advances and new or updated practices arise to deal with those changes. The following list provides an example of typical operational practice areas:

- Physical Security
  - *Physical Security Plans and Procedures* focuses on whether physical security policies and procedures for the facility exist and whether they have been tested.
  - *Physical Access Control* addresses policies and procedures for controlling physical assess to work areas and to information technology assets.
  - *Monitoring and Auditing Physical Security* defines an organization's approach for ensuring that physical security policies and procedures are implemented and are effective.
- Information Technology Security
  - *System and Network Management* focuses on practices for the secure operation of information technology systems and networks.
  - System *Administration Tools* focuses on tools and mechanisms for secure system and network administration.
  - *Monitoring and Auditing IT Security* defines an organization's approach for ensuring that information technology security policies and procedures are implemented and are effective.
  - *Authentication and Authorization* includes practices for verifying users to systems and for controlling access to networks, systems, and applications.
  - *Vulnerability Management* focuses on procedures for periodically assessing and managing technology vulnerabilities.
  - *Encryption* addresses security practices for using encryption to protect an organization's data during data storage and transmission.
  - *Security Architecture and Design* focuses on integrating security into the formal design of the infrastructure's architecture and topology.
- Staff Security
  - *Incident Management* includes practices for identifying, reporting, and responding to suspected security incidents and violations.
  - *General Staff Practices* focuses on staff members' understanding of their security roles and responsibilities and following security policies and procedures.

**Importance**

Using a catalog of practices is important because it allows an organization to evaluate itself against a known and accepted measure. This helps the organization to understand what it is currently doing well with respect to security (its current security practices) and what it is not doing well (its organizational vulnerabilities). The catalog of practices is also important because it creates the structure for an organization's protection strategy. Finally, the catalog provides a basis for selecting actions to include in risk mitigation plans.

## Generic Threat Profile (RA.4)

**Requirements**

The evaluation process must assess threats to the organization's critical assets by considering a broad range of potential threat sources that are formally defined in a generic threat profile. Typical categories of threat include

- *Human Actors Using Network Access* – The threats in this category are network-based threats to an organization's critical assets. They require direct action by a person and can be deliberate or accidental in nature.
- *Human Actors Using Physical Access* – The threats in this category are physical threats to an organization's critical assets. They require direct action by a person and can be deliberate or accidental in nature.
- *System Problems* – The threats in this category are problems with an organization's information technology systems. Examples include hardware defects, software defects, unavailability of related enterprise systems, malicious code (e.g., viruses, Trojan horses), and other system-related problems.
- *Other Problems* – The threats in this category are problems or situations that are outside the control of an organization. This category of threats includes natural disasters (such as floods, earthquakes, and storms) that can affect an organization's information technology systems as well as interdependency risks. Interdependency risks include the unavailability of critical infrastructures (telecommunications, electricity, etc.). Other types of threats outside the control of an organization can also be included here. Examples of these threats are power outages or broken water pipes.

**Importance**

Using a generic threat profile is important because it allows an organization to identify the threats to its critical assets based on known potential sources of threat. The profile also uses a structured way of representing potential threats and yields a comprehensive summary of threats to critical assets. This profile is important because it provides a complete and simple way to record and communicate threat information.

## Catalog of Vulnerabilities (RA.5)

**Requirements**

The evaluation process must assess the technological weaknesses (technology vulnerabilities) in the key components of the computing infrastructure by considering a range of technology vulnerabilities based on platform and application. Vulnerability evaluation tools (software, checklists, scripts) examine infrastructure components for technology vulnerabilities contained in the catalog. Two examples of catalogs of vulnerabilities are

- CERT® Knowledgebase[3]
- Common Vulnerabilities and Exploits (CVE)[4]

**Importance**

Using a catalog of vulnerabilities is important because it allows an organization to evaluate its technology base against known technology vulnerabilities. Identifying which vulnerabilities are present in the organization's key components provides the organization with information about how vulnerable its computing infrastructure currently is.

---

® CERT is registered in the U.S. Patent and Trademark Office.

[3] The CERT® Knowledgebase contains a public database describing vulnerabilities and a restricted-access catalog containing descriptive information regarding more than 1,300 vulnerabilities. It can be accessed at <http://www.cert.org/kb/>.

[4] CVE is a community effort led by the MITRE Corporation. It can be accessed at <http://www.cve.mitre.org>.

## Defined Evaluation Activities (RA.6)

**Requirements**

The procedures for performing each evaluation activity and the artifacts used during each activity must be defined and documented. This includes

- procedures for preparing for the evaluation
- procedures for scoping the evaluation
- procedures for completing each evaluation activity
- specifications for all tools and worksheets required by each activity
- specifications for catalogs of information that define accepted security practices, known sources of threat, and known technological weaknesses

**Importance**

Implementing defined evaluation activities helps to institutionalize the evaluation process in the organization, ensuring some level of consistency in the application of the process [GAO 99]. It also provides a basis upon which the activities can be tailored to fit the needs of a particular business line or group.

## Documented Evaluation Results (RA.7)

**Requirements**

The organization must document the results of the evaluation, either in paper or electronic form. Organizations typically document and archive the following types of information:

- the risks to the organization's critical assets
- security strategies and plans to improve the organization's security posture

**Importance**

It is important to establish a permanent record of evaluation results. A database of information can serve as source material for subsequent evaluations and is also useful when tracking the status of plans and actions after the evaluation. For example, the information that is recorded can also be used as lessons learned. When risks to a critical asset are identified, staff members can look at the mitigation plans for risks to similar assets. Organizational personnel can understand which mitigation actions have been effective in the past and which haven't. This can help them to create more effective mitigation plans.

## Evaluation Scope (RA.8)

**Requirements**

The extent of each evaluation must be defined. The evaluation process must include guidelines to help the organization decide which operational areas (business units) to include in the evaluation.

**Importance**

Setting the scope of an evaluation is important for ensuring that the evaluation results are useful to the organization. If the scope of an evaluation becomes too broad, it is often difficult to analyze all of the information that is gathered. Setting a manageable scope for the evaluation reduces the size of the evaluation, making it easier to schedule and perform the activities. In addition, the areas of an organization can be prioritized for the evaluation. Essentially, the highest-risk areas can be examined first or more frequently [GAO 99].

## Next Steps (RA.9)

**Requirements**

The evaluation must include an activity where organizational personnel identify the next steps required to implement security strategies and plans. This activity often requires active sponsorship and participation from the organization's senior managers. Next steps typically include the following information:

- what the organization will do to build on the results of the evaluation
- who will be involved in implementing security strategies and plans
- plans for future activities to evaluate information security risks

**Importance**

Identifying the next steps that people in the organization must take to implement the protection strategy and the mitigation plans is essential for security improvement. The people in the organization need to build upon the results of the evaluation. Getting senior management sponsorship is the first critical step toward making this happen.

## Focus on Risk (RA.10)

**Requirements**

The evaluation must focus on assessing an organization's information security risks by examining the interrelationships among assets, threats to the assets, and vulnerabilities (including both organizational and technological weaknesses).

**Importance**

This attribute is important because it requires the organization's personnel to focus on security issues and their effect on the organization's business objectives and mission. Personnel must look beyond the organizational and technological weaknesses that are present in the organization and examine how those weaknesses are related to the organization's critical assets and the threats to those assets, thus establishing the risk to those assets.

## Focused Activities (RA.11)

**Requirements**

The evaluation process must include guidelines for focusing evaluation activities. Examples include

- workshops that efficiently elicit security-related information from an organization's staff members
- analysis activities that use asset information to focus threat and risk identification activities
- analysis activities that use asset and threat information to set the scope of the infrastructure vulnerability evaluation
- planning activities that establish risk priorities using risk measures (impact, probability)

**Importance**

Focusing each activity on the most critical information security issues is important for ensuring that the organization is applying its resources efficiently. If too much information is gathered, it is often difficult to analyze the information. Focusing on the most important information reduces the size of the evaluation, making it easier to perform the activities while still collecting the most meaningful data and producing the most meaningful results.

## Organizational and Technological Issues (RA.12)

**Requirements**

The evaluation process must examine both organizational and technological issues. Information security risk evaluations typically include the following practice- and vulnerability-related information:

- current security practices used by staff members
- missing or inadequate security practices (also called organizational vulnerabilities)
- technological weaknesses present in key information technology systems and components

**Importance**

Because security has both organizational and technological components, it is important that an evaluation surface both organizational and technological issues. The analysis team analyzes both types of issues in relation to the mission and business objectives of the organization when creating the organization's protection strategy and risk mitigation plans. By doing this, the team is able to address security by creating a global picture of the information security risks with which the organization must deal.

## Business and Information Technology Participation (RA.13)

**Requirements**

The evaluation process must include participants from both the business units and the information technology department. This includes the establishment of an interdisciplinary analysis team. (See Attribute RA.1.) It also includes the need for participants from key areas (business units) of the organization to contribute their perspectives about security-related issues during knowledge elicitation activities. Note that participants must include representatives from multiple organizational levels (senior management, middle management, and staff).

**Importance**

Incorporating multiple perspectives is essential for ensuring that a broad range of risk factors is considered. Staff members who work in the business lines of an organization understand the relative importance of business operations and the systems and information that support these operations. In general, they are in the best position to understand the business impact of disruption or abuse to business systems and operations and the impact of potential mitigation actions. Information technology staff members, including information security experts, understand the design of existing systems and the impact of technology-related vulnerabilities. They are also in the best position to evaluate the tradeoffs of mitigation actions when evaluating their effect on system performance.

## Senior Management Participation (RA.14)

**Requirements**

Senior managers in the organization must have defined roles during the evaluation process. Typically, an organization's senior managers

- demonstrate active sponsorship of the evaluation
- participate in workshops to contribute their understanding of security-related issues and their effect on business processes
- review and approve security strategies and plans
- define the next steps required to implement security strategies and plans

**Importance**

This is the single most important success factor for information security risk evaluations. Senior management participation demonstrates strong sponsorship of the evaluation. This level of sponsorship helps to ensure that

- staff members are available to participate in the evaluation
- staff members take the evaluation seriously and are willing to participate
- the findings are implemented after the evaluation

The senior managers' active participation in an information security risk evaluation is also important to the success of the initiative. Senior managers can help to define the scope of the assessment and can help to identify participants. If senior managers support the evaluation, people in the organization tend to participate actively. If senior managers do not support the evaluation, then staff support for the evaluation will dissipate quickly.

## Collaborative Approach (RA.15)

**Requirements** Each activity of the evaluation process must include interaction and collaboration among the people who are participating in that activity. Collaboration can be achieved through the use of workshops or other interactive methods.

**Importance** A collaborative approach is an essential attribute of information security risk evaluations. Because security is interdisciplinary in nature, completing the evaluation activities requires interdisciplinary knowledge and skills. Thus, it is important that each evaluation activity require all participating individuals to interact and collaborate, ensuring that the necessary skills and knowledge are used to complete that activity satisfactorily.

This far, we have focused on the broad concepts (principles) and the characteristics of the evaluation (attributes). Next, we complete the criteria by examining the required outputs of the evaluation.

# 6 OCTAVE Outputs

The OCTAVE criteria define an approach for evaluating an organization's information security risks. Thus far in this document, we have examined the principles and attributes of the approach. Now, we will explore the required outputs of the evaluation. The OCTAVE outputs define the outcomes that an analysis team must achieve during the evaluation. We organize them according to data category. The following list highlights the basic types of data produced by information security risk evaluations:

- organizational data
- technological data
- risk analysis and mitigation data

Thus, we present OCTAVE as a three-phased approach for information security risk evaluations. The three phases illustrate the interdisciplinary nature of information security by emphasizing its organizational and technological aspects. In Section 6.1, we describe each phase of OCTAVE. The phase descriptions provide sufficient context to enable you to understand the nature of the outputs.

In Sections 6.2 through 6.4, we present the requirements of each output of OCTAVE by phase. Note that each attribute is numbered for easy cross-referencing. Outputs are defined using the following information:

- requirements – the essential characteristics of the output
- importance – why the output is important to the evaluation process

## 6.1 Evaluation Phases

The organizational, technological, and analysis aspects of an information security risk evaluation provides a conceptual framework for describing the evaluation and its outputs. We have structured OCTAVE using this conceptual framework. The result is a three-phased approach, corresponding to the major aspects of information security risk evaluations.

The following are the three phases of OCTAVE:

- Phase 1: Build Asset-Based Threat Profiles
- Phase 2: Identify Infrastructure Vulnerabilities
- Phase 3: Develop Security Strategy and Plans

In the following sections, we describe each OCTAVE Phase.

### 6.1.1 Phase 1: Build Asset-Based Threat Profiles

In today's business environment, the computing infrastructure is distributed across organizations. In addition, many business processes are distributed, with staff members performing specialized job functions. Thus, all staff members play a role in information security. Each person has unique knowledge of what information is important to completing his or her job tasks. Each person also has a unique perspective about which security practices are currently being used to protect the organization's information-related assets as well as which security practices are missing or inadequate. In Phase 1, the staff members from across an organization have the opportunity to contribute what they know about the organization's information security issues through a series of knowledge elicitation workshops.

Phase 1 is an organizational evaluation that includes knowledge elicitation, data consolidation, and analysis activities. In the knowledge elicitation activities, staff members from across the organization contribute their perspectives about

- what is important to the organization (information-related assets)
- what is currently being done to protect those assets (security practices)
- missing or inadequate security practices (organizational vulnerabilities)

The knowledge elicitation activities require representative groups of staff members from across the organization to participate, including people from both the business and information technology areas of the organization. In addition, multiple organizational levels (senior management, operational area management, staff) must be represented. The analysis team members facilitate the knowledge elicitation activities, ensuring that all activities are completed satisfactorily.

In the data consolidation and analysis activities, the analysis team

- groups information from the knowledge elicitation workshops
- selects the assets that are most important to the organization (critical assets)
- describes security requirements for the critical assets
- identifies threats to the critical assets

In all Phase 1 activities, the analysis team can include selected personnel to augment its skills when necessary.

The required outputs for Phase 1 are

- RO1.1 Critical Assets
- RO1.2 Security Requirements for Critical Assets
- RO1.3 Threats to Critical Assets
- RO1.4 Current Security Practices
- RO1.5 Current Organizational Vulnerabilities

The knowledge elicitation workshops are important for identifying what is really happening in the organization with respect to information security. The data consolidation and analysis activities are important because they capture the organizational view of information security. The outputs of the data consolidation and analysis activities are important because those outputs are used to

- focus subsequent evaluation activities
- create the basis for the organization's protection strategy and risk mitigation plans that are created during Phase 3

### 6.1.2 Phase 2: Identify Infrastructure Vulnerabilities

Phase 2 is an evaluation of the information infrastructure. Phase 2 includes data gathering and analysis activities. The analysis team

- scopes the examination of the computing infrastructure using the critical assets and threats to those assets
- identifies key information technology systems and components that are related to each critical asset
- runs vulnerability evaluation tools against the key components
- analyzes the resulting data to identify weaknesses (technology vulnerabilities) that can lead to unauthorized action against critical assets

The analysis team members are the key participants in Phase 2 activities. In addition, key information technology staff members can be included if the analysis team needs to enhance its knowledge and skills in information technology. These additional people can be a part of the organization or can be from an external organization. It is important to ensure that the individuals leading this activity have an in-depth understanding of information technology and computer security issues.

The required outputs for Phase 2 are

- RO2.1 Key Components
- RO2.2 Current Technology Vulnerabilities

Phase 2 captures the technological view of information security, resulting in an understanding of the technology vulnerabilities that are present in and apply to network services, architecture, operating systems, and applications. Phase 2 is important because

- the outputs of Phase 1 are examined in relation to the computing infrastructure
- the outputs of Phase 2 document the present state of the computing infrastructure with respect to technological weaknesses that could be exploited by human threat actors

### 6.1.3 Phase 3: Develop Security Strategy and Plans

Phase 3 includes risk analysis and risk mitigation activities. During risk analysis, the analysis team identifies and analyzes the risks to the organization's critical assets. Specifically, the team

- gathers data used to measure the risks to critical assets (e.g., impact descriptions and probability data)
- defines the risk evaluation criteria for risk measures, establishing a common understanding of the qualitative measures (high, medium, low) of impact
- evaluates risks against the evaluation criteria

During risk mitigation, the analysis team creates a protection strategy and mitigation plans based upon an analysis of the information gathered. Specifically, the team

- develops a protection strategy for organizational improvement and risk mitigation plans to protect the organization's information-related assets
- identifies next steps that will be taken to implement the protection strategy and the mitigation plans

The analysis team members are the key participants in Phase 2 activities. If appropriate, the analysis team can include selected personnel to augment its skills. The organization's senior managers review and approve the protection strategy and risk mitigation plans.

The required outputs for Phase 3 are

- RO3.1 Risks to Critical Assets
- RO3.2 Risk Measures
- RO3.3 Protection Strategy
- RO3.4 Risk Mitigation Plans

Phase 3 is important because it is in this phase that the analysis team makes sense of its information security issues and develops a strategy and plans for improvement. Phase 3 includes both risk analysis and risk mitigation activities. The risk analysis activities of Phase 3 are important because they

- put information security threats into the context of what the organization is trying to achieve, resulting in explicit statements of risk to the organization's critical assets
- establish the criteria for measuring risks and a basis for setting priorities when developing risk mitigation plans

The risk mitigation activities of Phase 3 are important because they

- result in a protection strategy designed to improve the organization's security posture
- result in a risk mitigation plan for each critical asset designed to protect that critical asset
- require the organization's senior managers to review the protection strategy and risk mitigation plans from the organizational perspective, developing senior management sponsorship of the evaluation results
- define what the organization will do to implement the results of the evaluation, enabling ongoing security improvement

In the next three sections, we examine the required outputs by phase.

## 6.2 Phase 1 Outputs

### Critical Assets (RO1.1)

**Requirements**

The evaluation process must identify which assets are critical. An asset is something of value to the organization [Hutt 95]. Critical assets are those that are believed to be the most important assets to the organization. The organization will suffer a large adverse impact if the security requirements of these assets are violated.

Information security risk evaluations typically include the following categories of assets:[5]

- information – documented (paper or electronic) data or intellectual property used to meet the mission of the organization
- systems – information systems that process and store information. Systems are a combination of information, software, and hardware assets. Any host, client, or server can be considered to be a system.
- software – software applications and services (operating systems, database applications, networking software, office applications, custom applications, etc.)
- hardware – information technology physical devices (workstations, servers, etc.)
- people – the people in the organization, including their skills, training, knowledge, and experience

**Importance**

The organization's critical assets are used to focus all future evaluation activities.

[5] This list was created using information in these references: [Fites 89], [BSI 95], [Hutt 95], and [Caelli 91].

## Security Requirements for Critical Assets (RO1.2)

**Requirements**

Security requirements outline the important qualities of an asset, and they must be identified for each critical asset. The following are security requirements that are typically considered during an evaluation:

- confidentiality – the need to keep proprietary, sensitive, or personal information private and inaccessible to anyone who is not authorized to see it
- integrity – the authenticity, accuracy, and completeness of an asset
- availability – when or how often an asset must be present or ready for use

**Importance**

Security requirements provide a basis for risk mitigation plans that are developed during Phase 3.

## Threats to Critical Assets (RO1.3)

**Requirements**

The evaluation process must include a structured way of recording threats. A threat is an indication of a potential undesirable event [NSTISSC 98]. It refers to a situation where a person could do something undesirable or where a system malfunction or natural occurrence could cause an undesirable outcome. Threats typically include the following types of components:

- asset – something of value to the organization
- actor – who or what may violate the security requirements (confidentiality, integrity, availability) of an asset
- motive – determination of whether the actor's intentions are deliberate or accidental (applies only to human actors)
- access – how the asset will be accessed by the actor, i.e., network access and physical access (applies only to human actors)
- outcome – the immediate outcome (disclosure, modification, destruction, loss, interruption) of violating the security requirements of an asset

**Importance**

Understanding the threats to critical assets helps to form the basis for examining the information infrastructure for technology vulnerabilities during Phase 2 and for identifying and analyzing risks during Phase 3.

## Current Security Practices (RO1.4)

**Requirements**

The evaluation must identify security practices currently being used by the organization. Security practices are those actions presently used by the organization to initiate, implement, and maintain its internal security [BSI 95]. Security practices are used to protect an organization's information-related assets.

**Importance**

Identifying which security practices are currently being used by the organization helps staff members understand what they are doing well and which security practices they need to maintain. The current security practices used by the organization form the basis upon which a protection strategy for the organization can be built.

## Current Organizational Vulnerabilities (RO1.5)

**Requirements**

The evaluation must identify organizational vulnerabilities that are present in the organization. Organizational vulnerabilities are weaknesses in organizational policy or practice that can result in unauthorized actions occurring. They are indications of missing or inadequate security practices.

**Importance**

Identifying which organizational vulnerabilities are currently present in the organization helps staff members understand which security practices they need to improve. Those areas of improvement can be incorporated into an organization's protection strategy and risk mitigation plans.

## 6.3 Phase 2 Outputs

### Key Components (RO2.1)

**Requirements**

The evaluation must identity key infrastructure components to examine for technology vulnerabilities. Key components are devices that are important in processing, storing, or transmitting critical information. They represent assets related to critical assets. Components from the following classes are typically considered during an information security risk evaluation:

- servers – hosts within your information technology infrastructure that provide information technology services to your organization
- networking components – devices important to your organization's networks. Routers, switches, and modems are all examples of networking components.
- security components – devices that have security as their primary function (e.g., a firewall)
- desktop workstations – hosts on your networks that staff members use to conduct business
- home computers – home personal computers (PCs) that staff members use to access information remotely via your organization's networks
- laptops – portable PCs that staff members use to access information remotely via your organization's networks
- storage devices – devices where information is stored, often for backup purposes
- wireless components – devices, such as cell phones and wireless access points, that staff members may use to access information (e.g., email)
- others – any other type of device that could be part of your threat scenarios but that does not fall into the above classes

**Importance**

Key components are selected infrastructure components that are evaluated for technology vulnerabilities. These components set the scope of the technology vulnerability evaluation.

## Current Technology Vulnerabilities (RO2.2)

**Requirements**

The information security risk evaluation must identify technology vulnerabilities in the computing infrastructure. Technology vulnerabilities are weaknesses in systems that can directly lead to unauthorized action [NSTISSC 98]. Technology vulnerabilities are present in and apply to network services, architecture, operating systems, and applications. Types of technology vulnerabilities include design, implementation, and configuration vulnerabilities.

**Importance**

Technology vulnerabilities are important because they are specific weaknesses in an organization's computing infrastructure that could be exploited by human threat actors. Thus, identifying technology vulnerabilities helps to capture the present state of the computing infrastructure. In addition, patterns of technology vulnerabilities can indicate problems with the current security practices in your organization (organizational vulnerabilities).

## 6.4 Phase 3 Outputs

### Risks to Critical Assets (RO3.1)

**Requirements**

The evaluation process must include a structured way of recording risks. Risk is the possibility of suffering harm or loss. It is the potential for realizing unwanted negative consequences of an event [Rowe 88]. Risk refers to a situation where a person could do something undesirable or where a system malfunction or natural occurrence could cause an undesirable outcome, resulting in a negative impact or consequence. Essentially, a risk includes the threat to an asset plus the resulting impact on the organization. Risks typically include the following types of components:

- asset – something of value to the organization
- actor – who or what may violate the security requirements (confidentiality, integrity, availability) of an asset
- motive – determination of whether the actor's intentions are deliberate or accidental (applies only to human actors)
- access – how the asset will be accessed by the actor, i.e., network access and physical access (applies only to human actors)
- outcome – the immediate outcome (disclosure, modification, destruction, loss, interruption) of violating the security requirements of an asset
- impact – a description of the effect of a threat on an organization's mission and business objectives

**Importance**

Identifying the risks to critical assets captures the effect of threats on the organization's mission and business objectives. Understanding the risks to critical assets is important because it focuses on the effect of threats on the organization by putting threats into the context of what the organization is trying to achieve. It forms the basis for setting priorities during Phase 3.

## Risk Measures (RO3.2)

**Requirements**

The evaluation process must establish a means to measure the level of risk to each critical asset. Impact value is an essential risk measure. It is a measurement of the ultimate effect on an organization's mission and business objectives resulting from a threat to a critical asset. Probability is an optional risk measure in the risk analysis. It is a measurement of the likelihood of occurrence of a threat. Impact value and probability (if used) are typically measured using a qualitative scale of high, medium, and low. The qualitative scale needs to be established based on what is important to an organization. Quantitative measurements of impact value and probability can be used provided that sufficient data to support quantitative measurement or estimation exist.

**Importance**

Understanding impact measures for risks is important because these measures are used when setting mitigation priorities during Phase 3. Probability measures, if used, are important in refining mitigation priorities.

## Protection Strategy (RO3.3)

**Requirements**

A protection strategy must be an output of the evaluation process. An organization's protection strategy defines its direction with respect to efforts to improve information security. It includes approaches for enabling, implementing, and maintaining security practices in an organization. A protection strategy tends to incorporate long-term organization-wide initiatives and is structured using the practice areas defined in the catalog of practices. (See Attribute RA.3.)

**Importance**

Creating a protection strategy is important because it charts a course for organizational improvement with respect to information security activities.

## Risk Mitigation Plans (RO3.4)

**Requirements**

Risk mitigation plans to protect critical assets must be an output of the evaluation process. Risk mitigation plans for critical assets define the mitigation actions intended to reduce the risks to the organization's critical assets. During the development of these plans, the analysis team has considered organizational resources and constraints. Risk mitigation plans tend to incorporate actions, or countermeasures, designed to counter the threats to the assets. The actions are based on the practices contained in the catalog of practices. (See Attribute RA.3.)

**Importance**

Creating risk mitigation plans is important because they set the actions required to protect the organization's critical assets.

# 7 Summary

OCTAVE is an approach for information security risk evaluations that is comprehensive, systematic, context driven, and self directed. It enables an organization to sort through both organizational and technological issues to understand and address its information security risks. It provides a snapshot in time, or a baseline, that can be used to focus mitigation and improvement activities. Thus, OCTAVE can be viewed as a tool that facilitates information security improvement.

An interdisciplinary team, called the analysis team, leads the evaluation activities and is responsible for making decisions about the organization's efforts to improve information security. OCTAVE requires the team to consider the relationships among critical assets, the threats to those assets, and vulnerabilities (both organizational and technological) that can expose assets to threats. It requires the analysis team to evaluate risks in an operational context. At the conclusion of the evaluation, the team creates a protection strategy for organizational improvement and risk mitigation plans to reduce the risk to the organization's critical assets. Thus, the process incorporates both strategic and tactical views of risk.

The essential elements of OCTAVE are embodied in a set of criteria. There can be many methods consistent with these criteria, but there is only one set of OCTAVE criteria. These criteria define an approach for evaluating an organization's information security risk using a set of principles, attributes, and outputs. The OCTAVE principles are the fundamental concepts that drive the nature of the evaluation and define the philosophy that shapes the evaluation process. Attributes are the distinctive characteristics of the evaluation and are derived from the principles. They define what is necessary to make the evaluation a success from both the process and organizational perspectives. Finally, the outputs define the outcomes that an analysis team must achieve during the evaluation. By implementing a risk evaluation practice based on the OCTAVE criteria, an organization can start to improve its overall security posture.

# References


**[Alberts 99]** Alberts, Christopher J.; Behrens, Sandra G.; Pethia, Richard D.; & Wilson, William R. *Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE℠) Framework, Version 1.0* (CMU/SEI-99-TR-017, ADA 367718). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, June 1999. <http://www.sei.cmu.edu/publications/documents/99.reports/99tr017/99tr017abstract.html>.

**[Alberts 01a]** Alberts, Christopher & Dorofee, Audrey. *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE℠) Method Implementation Guide, v2.0.* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001.

**[Alberts 01b]** Alberts, Christopher J.; Dorofee, Audrey J.; & Allen, Julia H. *OCTAVE℠ Catalog of Practices, v2.0* (CMU/SEI-2001-TR-020). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001. <http://www.sei.cmu.edu/publications/documents/01.reports/01tr020.html>.

**[BSI 95]** British Standards Institution. *Information Security Management, Part 1: Code of Practice for Information Security Management of Systems* (BS7799: Part 1: 1995). London, England: British Standard Institution, February 1995.

**[Caelli 91]** Caelli, William; Longley, Dennis; & Shain, Michael. *Information Security Handbook.* New York, NY: Stockton Press. 1991.

**[Dempsey 97]** Dempsey, Rob & Bruce, Glen. *Security in Distributed Computing.* Upper Saddle River, NJ: Prentice-Hall, Inc., 1997.

**[Dorofee 96]** Dorofee, A.; Walker, J.; Alberts, C.; Higuera, R.; Murphy, R.; & Williams, R. *Continuous Risk Management Guidebook.* Pittsburgh, PA, Software Engineering Institute, Carnegie Mellon University, 1996.

**[Fites 89]** Fites, P.E.; Kratz, M.P.; & Brebner, A.F. *Control and Security of Computer Information Systems*. Rockville, MD, Computer Science Press, Inc., 1989, pp. 7-61.

**[GAO 99]** United States General Accounting Office. *Information Security Risk Assessment, Practices of Leading Organizations* (GAO/AIMD-00-33). Washington, D.C.: GAO, November 1999.

**[Hutt 95]** Hutt, Arthur E.; Bosworth, Seymour; & Hoyt, Douglas B. *Computer Security Handbook*, 3rd ed. New York, NY: John Wiley & Sons, Inc., 1995.

**[NSTISSC 98]** National Security Telecommunications and Information Systems Security Committee. *Index of National Security Telecommunications Information Systems Security Issuances* (NSTISSI No. 4014). Ft. Mead, MD: NSTISSC Secretariat, January 1998.

**[Rowe 88]** Rowe, William D. *An Anatomy of Risk*. Malibu, FL: Robert E. Crier, 1988.

**[Williams 99]** Williams, Ray C.; Pandelios, George J.; & Behrens, Sandra G. *Software Risk Evaluation (SRE) Method Description, Version 2.0* (CMU/SEI-99-TR-029, ADA 001008). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999. <http://www.sei.cmu.edu/publications/documents/99.reports/99tr029/99tr029abstract.html>.

# Appendix A: A Set of Activities Consistent with the OCTAVE Criteria

In this appendix, we present a set of requirements for activities that are consistent with the OCTAVE criteria. These are the requirements that we used when we developed the OCTAVE Method [Alberts 01]. We recognize that there is more than one set of activities that can produce the outputs of OCTAVE. For this reason, we do not include this set of activities as part of the OCTAVE criteria.

Activities are defined here as the operations performed during an information security risk evaluation. Table 3 illustrates 16 activities that can be used to produce the OCTAVE outputs. We present the activities according to the phases defined in Section 6 of this document.

*Table 3: OCTAVE Activities by Phase*

| OCTAVE Activities | | |
|---|---|---|
| **Phase 1 Activities (P1)** | **Phase 2 Activities (P2)** | **Phase 3 Activities (P3)** |
| P1.1 Identify Assets | P2.1 Select Infrastructure Components to Evaluate | P3.1 Identify Risks to Critical Assets |
| P1.2 Identify Current Security Practices | P2.2 Run Vulnerability Evaluation Tools | P3.2 Create Risk Evaluation Criteria |
| P1.3 Identify Current Organizational Vulnerabilities | P2.3 Review Vulnerabilities and Summarize Results | P3.3 Evaluate Risks to Critical Assets |
| P1.4 Identify Critical Assets | | P3.4 Create Protection Strategy |
| P1.5 Describe Security Requirements for Critical Assets | | P3.5 Create Risk Mitigation Plans |
| P1.6 Create Threat Profiles for Critical Assets | | P3.6 Review Protection Strategy and Risk Mitigation Plans with Management |
| | | P3.7 Identify Next Steps |

Table 4 illustrates the relationships between the attributes and activities of OCTAVE. You will notice that the diagram for each activity contains coded inputs and outputs. The following list indicates the numbering scheme throughout this appendix:

- I – indicates an input
- O – indicates an output
- PX.Y – indicates Activity Y in Phase X
- _Z – indicates a sequence number for an input or output

For example, IP2.1_1 indicates that this is the first input of Activity P2.1, while OP3.3_3 indicates that this is the third output of Activity P3.3. Each input and output is explained in Section A.4, Data Dictionary, using the numbered codes as a key.

In this appendix, we define each activity using the following information:

- activity description – the essential elements of the activity, including the goal of the activity and the questions that are answered by performing the activity
- participants – who is essential to the completion of the activity
- diagram – a graphic depiction of the inputs and outputs of the process
- importance – why the activity is important to the evaluation process

*Table 4: Mapping OCTAVE Attributes to Activities*

| Mapping of Attributes to Activities | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Activities | | | | | | | | | | | | | | | |
| **Attributes** | **P1.1** | **P1.2** | **P1.3** | **P1.4** | **P1.5** | **P1.6** | **P2.1** | **P2.2** | **P2.3** | **P3.1** | **P3.2** | **P3.3** | **P3.4** | **P3.5** | **P3.6** | **P3.7** |
| R.1 Analysis Team | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| R.2 Augmenting Analysis Team Skills | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| R.3 Catalog of Practices | | X | X | | | | | | | | | | X | X | | |
| R.4 Generic Threat Profile | | | | | | X | | | | | | | | | | |
| R.5 Catalog of Vulnerabilities | | | | | | | | X | | | | | | | | |
| R.6 Defined Evaluation Activities | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| R.7 Documented Evaluation Results | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| R.8 Evaluation Scope | X | X | X | | | | | | | | | | | | | |
| R.9 Next Steps | | | | | | | | | | | | | | | X | X |
| R.10 Focus on Risk | | | | X | X | X | | | | X | X | X | X | X | X | X |
| R.11 Focused Activities | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| R.12 Organizational and Technological Issues | X | X | X | | | | | | | X | X | X | X | X | X | X |
| R.13 Business and Information Technology Participation | X | X | X | | | | | | | X | X | X | X | X | X | X |
| R.14 Senior Management Participation | X | X | X | | | | | | | | | | | | X | X |
| R.15 Collaborative Approach | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |

## A.1 Phase 1 (Build Asset-Based Threat Profiles) Activities

Phase 1 of OCTAVE is entitled Build Asset-Based Threat Profiles. It is an organizational evaluation. Phase 1 focuses on the people in the organization and requires staff members throughout the organization to participate by contributing their unique perspectives about the following:

- the information-related assets that they use in their jobs
- the current security practices that are used by the organization
- which organizational vulnerabilities are present in the organization

The analysis team consolidates the information, creating an organization-wide view of information-related assets, current security practices, and current organizational vulnerabilities. The team then

- selects the assets that are most important to meeting the mission and business objectives of the organization (the critical assets)
- creates a set of security requirements for each critical asset
- creates a unique threat profile for each critical asset that describes the range of threats that applies to each critical asset

Phase 1 is composed of the following six activities:

| | |
|---|---|
| P1.1 | Identify Assets |
| P1.2 | Identify Current Security Practices |
| P1.3 | Identify Current Organizational Vulnerabilities |
| P1.4 | Identify Critical Assets |
| P1.5 | Describe Security Requirements for Critical Assets |
| P1.6 | Create Threat Profiles for Critical Assets |

## P1.1 Identify Assets

**Activity Description**

The goal of Activity P1.1 is to create an organization-wide listing of information-related assets. The following key questions must be answered during this activity. The questions focus on identifying which assets are important to meeting the mission and business objectives of the organization.

| Key Questions for P1.1: Identify Assets |
| --- |
| • What are the organization's important assets? |
| • Are there any other assets that the organization is required to protect (e.g., by law or regulation)? |
| • What related assets are important? |
| • Which assets are the most important? Why? |

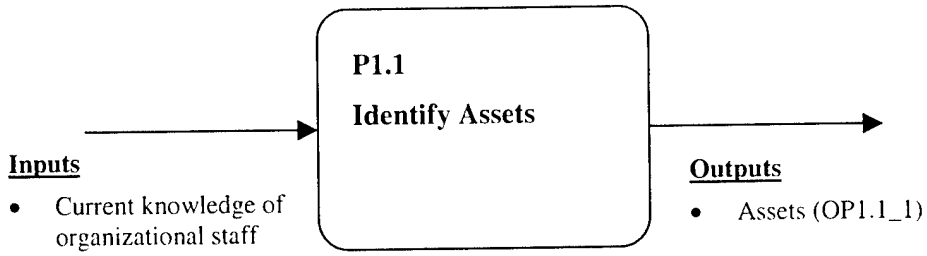
During Activity P1.1, information-related assets that are important to meeting the mission and business objectives of the organization are identified. People from different areas of the organization (e.g., business and information technology areas) and from multiple organizational levels (e.g., senior management, operational area management, and staff) contribute their unique perspectives about which information-related assets they use in their jobs. The analysis team consolidates the individual perspectives, creating an organization-wide view of information-related assets. It is important to solicit the multiple perspectives about assets. People from different parts of the organization rely on different assets to perform their tasks. Before a global perspective of assets can be created, the individual perspectives must be identified.

**Participants**

A representative group of staff members from across the organization participates in this activity. This group includes people from both the business and information technology areas of the organization. In addition, multiple organizational levels (senior management, operational area management, staff) must be represented. The analysis team members facilitate the activity, ensuring that the activity is completed satisfactorily.

**Diagram**

The following diagram shows the inputs and outputs of Activity P1.1: Identify Assets.




**Importance**

An asset is something of value to the organization. Information-related assets typically include information, systems, software, hardware, and people. Information-related assets are important to meeting the mission and business objectives of the organization. By knowing which of these assets are most important to the organization, management can use its limited resources to focus on protecting the most important information-related assets.

**Notes**

Activity P1.1 consists of two distinct components: a knowledge elicitation component and a consolidation component. The knowledge elicitation component requires staff members from across the organization to contribute their understanding of which information-related assets are important to the organization. The analysis team then consolidates the individual perspectives, creating an organization-wide view of information-related assets.

Activity P1.2, Identify Current Security Practices, and Activity P1.3, Identify Current Organizational Vulnerabilities, also have knowledge elicitation components. Note that Activities P1.1, P1.2, and P1.3 can be conducted together during a single session.

When staff members from across the organization create an organization-wide listing of information-related assets, they can also be asked to identify the security requirements for and perceived threats to their most important assets. The analysis team can use the security requirements data as input to Activity P1.5, Describe Security Requirements for Critical Assets. The team can use the perceived threat data as input to Activity P1.6, Create Threat Profiles for Critical Assets. Collecting security requirements and perceived threat informa-

tion can be very useful in certain instances. For example, in very large organizations, the analysis team might not have sufficient insight into all operational areas participating in the evaluation. To gain more insight into the operational areas, the analysis team might find it useful to elicit the security requirements and perceived threats from staff members who are participating in the evaluation.

Because people from different areas of the organization (e.g., business and information technology areas) and from multiple organizational levels (e.g., senior management, operational area management, and staff) contribute their unique perspectives during this activity, it is important to structure the knowledge elicitation component of the activity carefully. The analysis team should make sure that open communication is encouraged. For example, if a workshop format is being used to elicit information, the analysis team might want to assign people to workshops according to organizational level. People tend to discuss issues more openly when there are no real or perceived reporting relationships among the participants in the workshop.

## P1.2 Identify Current Security Practices

**Activity Description**

The goal of Activity P1.2 is to create an organization-wide listing of the current security practices used by the organization. The following key questions must be answered during this activity. The questions focus on what people in the organization believe they are doing to protect the organization's important information-related assets.

| Key Questions for P1.2: Identify Current Security Practices |
| --- |
| • What is the organization currently doing well with respect to protecting its important information-related assets? |
| • Are there specific policies, procedures, and practices unique to specific assets? What are they? |
| • Is the organization's protection strategy effective? Why? Why not? |

When people are answering the first key question, they must consider their organization's practices in relation to a catalog of practices. (See Attribute RA.3, Catalog of Practices, of the OCTAVE criteria.) This allows people to evaluate their organization's security practices against a known and accepted measure of security practice.

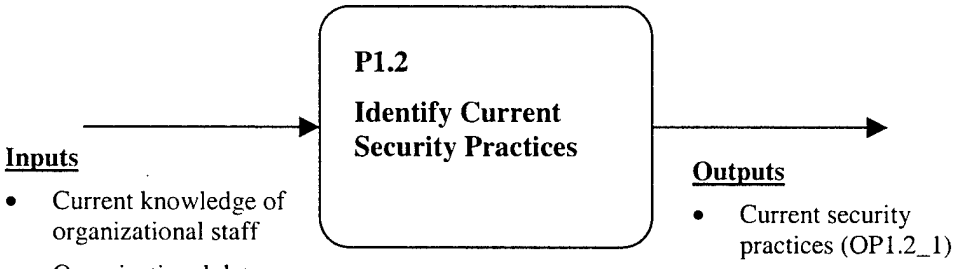
During Activity P1.2, current security practices used by the organization to protect its information-related assets are identified. People from different areas of the organization (e.g., business and information technology areas) and from multiple organizational levels (e.g., senior management, operational area management, and staff) contribute their unique perspectives about which security practices are used by the organization. The analysis team consolidates the individual perspectives, creating an organization-wide view of current security practices. It is important to solicit the multiple perspectives about current security practices used by the organization. People from different parts of the organization often have different opinions about what the organization is currently doing to protect its assets. Before a global perspective of current security practices can be created, the individual perspectives must be identified.

**Participants**

A representative group of staff members from across the organization participates in this activity. This group includes people from both the business and information technology areas of the organization. In addition, multiple organizational levels (senior management, operational area management, staff) must be represented. The analysis team members facilitate the activity, ensuring that the activity is completed satisfactorily.

**Diagram**

The following diagram shows the inputs and outputs of Activity P1.2: Identify Current Security Practices.




**Inputs**

- Current knowledge of organizational staff
- Organizational data (IP1.2_1)
- Laws and regulations (IP1.2_2)
- Catalog of practices (IP1.2_3)
- Assets (OP1.1_1)

**Outputs**

- Current security practices (OP1.2_1)

**Importance**

Security practices are actions that help initiate, implement, and maintain security within an organization. It is important for people in an organization to understand which security practices are currently being used to protect the organization's information-related assets. This helps staff members understand what they are currently doing well and which security practices they need to maintain. The current security practices used by the organization also form the basis upon which a protection strategy for the organization can be built.

**Notes**

Activity P1.2 consists of two distinct components: a knowledge elicitation component and a consolidation component. The knowledge elicitation component requires staff members from across the organization to contribute their understanding of the current security practices used by the organization. The analysis team then consolidates the individual perspectives, creating an organization-wide view of current security practices.

This activity is directly related to Activity P1.3, Identify Current Organizational Vulnerabilities, where staff members focus on the organizational vulnerabilities present in the organization (the flip side of security practices). Because of the link between security practices and organizational vulnerabilities, Activities P1.2 and P1.3 are usually performed together. Note that Activities P1.1, P1.2, and P1.3 can be conducted together during a single knowledge elicitation session.

Because people from different areas of the organization (e.g., business and information technology areas) and from multiple organizational levels (e.g., senior management, operational area management, and staff) contribute their unique perspectives during this activity, it is important to structure the knowledge elicitation component of the activity carefully. The analysis team should make sure that open communication is encouraged. For example, if a workshop format is being used to elicit information, the analysis team might want to assign people to workshops according to organizational level. People tend to discuss issues more openly when there are no real or perceived reporting relationships among the participants in the workshop.

## P1.3 Identify Current Organizational Vulnerabilities

**Activity Description**

The goal of Activity P1.3 is to create an organization-wide listing of the current organizational vulnerabilities present in the organization. The following key questions must be answered during this activity. The questions focus on what people in the organization believe they are not doing well to protect the organization's important information-related assets.

| Key Questions for P1.3: Identify Current Organizational Vulnerabilities |
|---|
| • What is the organization currently not doing well with respect to protecting its important information-related assets? |
| • Is the organization's protection strategy effective? Why? Why not? |

When people are answering the first key question, they must consider their organization's practices in relation to a catalog of practices. (See Attribute RA.3, Catalog of Practices, of the OCTAVE criteria.) This allows people to evaluate their organization's security practices against a known and accepted measure of security practice.

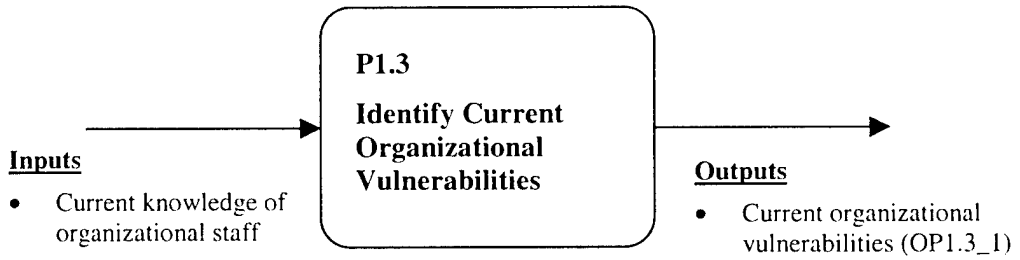
During Activity P1.3, current organizational vulnerabilities that are present in the organization are identified. People from different areas of the organization (e.g., business and information technology areas) and from multiple organizational levels (e.g., senior management, operational area management, and staff) contribute their unique perspectives about which organizational vulnerabilities are present in the organization. The analysis team consolidates the individual perspectives, creating an organization-wide view of current organizational vulnerabilities. It is important to solicit the multiple perspectives about current organizational vulnerabilities present in the organization. People from different parts of the organization often have different opinions about issues related to what the organization is currently doing to protect its assets. Before a global perspective of organizational vulnerabilities can be created, the individual perspectives must be identified.

**Participants**

A representative group of staff members from across the organization participates in this activity. This group includes people from both the business and information technology areas of the organization. In addition, multiple organizational levels (senior management, operational area management, staff) must be represented. The analysis team members facilitate the activity, ensuring that the activity is completed satisfactorily.

**Diagram**

The following diagram shows the inputs and outputs of Activity P1.3: Identify Current Organizational Vulnerabilities.




- Current knowledge of organizational staff
- Organizational data (IP1.2_1)
- Laws and regulations (IP1.2_2)
- Catalog of practices (IP1.2_3)
- Assets (OP1.1_1)

**Importance**

An organizational vulnerability is a weakness in organizational policy or practice that can result in the occurrence of unauthorized actions. Organizational vulnerabilities are indications of missing or inadequate security practices. It is important for people in an organization to understand which organizational vulnerabilities are present in the organization. This helps them understand where they need to improve with respect to security practices. The current organizational vulnerabilities indicate areas of improvement that can be incorporated into an organization's protection strategy and risk mitigation plans.

**Notes**

Activity P1.3 consists of two distinct components: a knowledge elicitation component and a consolidation component. The knowledge elicitation component requires staff members from across the organization to contribute their understanding of the current organizational vulnerabilities present in the organization. The analysis team then consolidates the individual perspectives, creating an organization-wide view of current organizational vulnerabilities.

This activity is directly related to Activity P1.2, Identify Current Security Practices, where staff members focus on the security practices used by the organization (the flip side of organizational vulnerabilities). Because of the link between security practices and organizational vulnerabilities, Activities P1.2 and P1.3 are usually performed together. Note that Activities P1.1, P1.2, and P1.3 can be conducted together during a single knowledge elicitation session.

Because people from different areas of the organization (e.g., business and information technology areas) and from multiple organizational levels (e.g., senior management, operational area management, and staff) contribute their unique perspectives during this activity, it is important to structure the knowledge elicitation component of the activity carefully. The analysis team should make sure that open communication is encouraged. For example, if a workshop format is being used to elicit information, the analysis team might want to assign people to workshops according to organizational level. People tend to discuss issues more openly when there are no real or perceived reporting relationships among the participants in the workshop.

## P1.4 Identify Critical Assets

**Activity Description**

The goal of Activity P1.4 is to select those assets that are the most important to the organization. The following key questions must be answered during this activity. The questions focus on violations of the assets' security requirements. As such, each question is framed around a specific threat outcome.

| Key Questions for P1.4: Identify Critical Assets |
| --- |
| • Which assets will cause a large adverse impact on the organization if they are disclosed to unauthorized people? |
| • Which assets will cause a large adverse impact on the organization if they are modified without authorization? |
| • Which assets will cause a large adverse impact on the organization if they are lost or destroyed? |
| • Which assets will cause a large adverse impact on the organization if access to them is interrupted? |

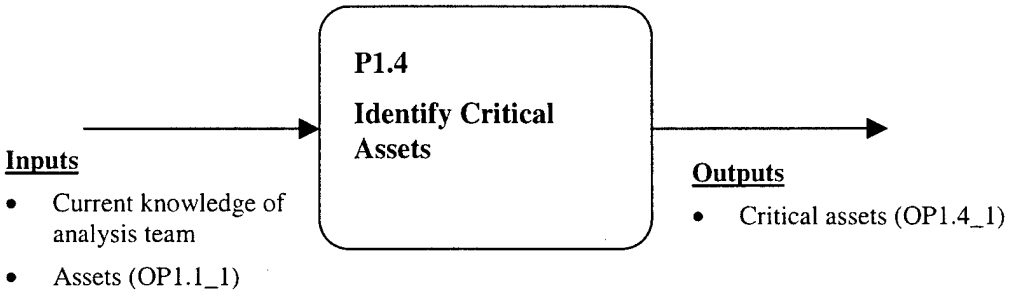
During Activity P1.4, the critical assets of the organization are selected. The analysis team first reviews all information-related assets that have been identified by participants from the organization. The team then selects those assets that are most important to meeting the mission and business objectives of the organization. The number of critical assets is small (often no more than five).

**Participants**

The analysis team members are the key participants in this activity. If appropriate, the analysis team can include selected personnel to augment its skills.

**Diagram**

The following diagram shows the inputs and outputs of Activity P1.4: Identify Critical Assets.




**Importance**

Critical assets are those that are believed to be the most important assets to the organization. The organization will suffer a large adverse impact if the security requirements of these assets are violated. The critical assets are used to focus all future evaluation activities.

## P1.5 Describe Security Requirements for Critical Assets

**Activity Description**

The goal of Activity P1.5 is to describe the security requirements for each critical asset. The following key questions must be answered during this activity. The questions focus on the important qualities of the assets.

| Key Questions for P1.5: Describe Security Requirements for Critical Assets |
|---|
| • Is the critical asset proprietary or sensitive? Does it contain personal information? Should it be inaccessible to anyone who is not authorized to see it? If the answer to any of these questions is yes, what is the specific confidentiality requirement? |
| • Are authenticity, accuracy, and completeness important for the critical asset? If yes, what is the specific integrity requirement? |
| • Is accessibility of the critical asset important? If yes, what is the specific availability requirement? |
| • Are there any other security-related requirements that are important to the critical asset? What are they? |

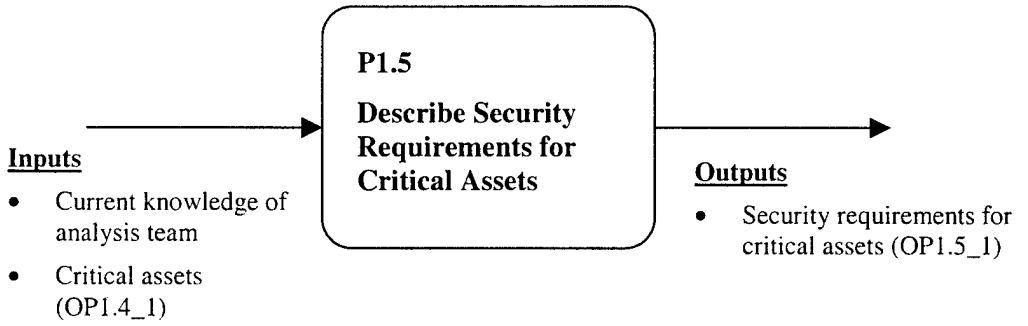
During Activity P1.5, the security requirements for the critical assets are described from the organizational perspective. The analysis team creates a set of security requirements for each critical asset. In creating the security requirements for a critical asset, the analysis team considers the confidentiality, integrity, and availability of that asset. The team also considers tradeoffs among the security requirements, identifying which requirement is ultimately most important for each critical asset.

**Participants**

The analysis team members are the key participants in this activity. If appropriate, the analysis team can include selected personnel to augment its skills.

**Diagram**

The following diagram shows the inputs and outputs of Activity P1.5: Describe Security Requirements for Critical Assets.




**Importance**

Security requirements for critical assets outline the qualities of the critical assets that are important to an organization. Security requirements also provide a basis for developing the protection strategy and risk mitigation plans during Phase 3.

## P1.6 Create Threat Profiles for Critical Assets

**Activity Description**

The goal of Activity P1.6 is to identify the range of threats that can affect each critical asset. The following key questions must be answered during this activity. The questions focus on how the critical assets are threatened.

| Key Questions for P1.6: Create Threat Profiles for Critical Assets |
| --- |
| • For which potential threats is there a non-negligible possibility of a threat to the critical asset? |
| • For which potential threats is there a negligible possibility or no possibility of a threat to the critical asset? |

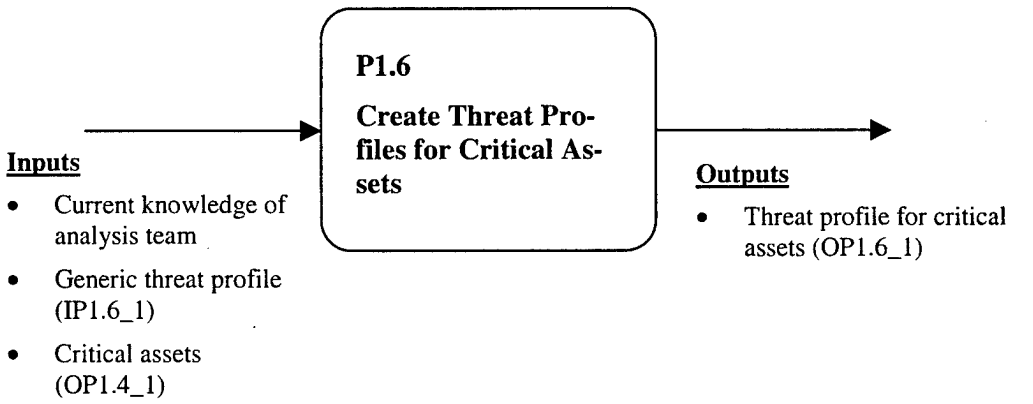
During Activity P1.6, threats to each critical asset are identified. The analysis team examines each critical asset in the context of the potential threats in the generic threat profile. The team then decides which of the threats in the profile applies to each critical asset, creating a unique threat profile for each critical asset. The generic threat profile provides the range of common threat scenarios to consider when developing a threat profile for a critical asset. When creating a threat profile for a critical asset, the analysis team also considers unique threats that might not be in the generic threat profile.

**Participants**

The analysis team members are the key participants in this activity. If appropriate, the analysis team can include selected personnel to augment its skills.

**Diagram**

The following diagram shows the inputs and outputs of Activity P1.6: Create Threat Profiles for Critical Assets.




**Importance**

Threats to critical assets are potential situations that can adversely affect an organization's critical assets. The threat profiles created during this activity help to form the basis for examining the information infrastructure for vulnerabilities during Phase 2 and for identifying and analyzing risks during Phase 3.

**Notes**

In some cases, perceived threat information could have been gathered during Activity P1.1. This information can be used as an input to Activity P1.6.

## A.2 Phase 2 (Identify Infrastructure Vulnerabilities) Activities

Phase 2 of OCTAVE is entitled Identify Infrastructure Vulnerabilities. It is a technological evaluation that focuses on the organization's computing infrastructure. During Phase 2, the analysis team and key information technology (IT) staff members

- select specific infrastructure components to examine for technology vulnerabilities
- select an approach for evaluating each infrastructure component
- develop a summary of the technology vulnerabilities affecting each critical asset
- refine the threat profile for each critical asset based upon the evaluation of that asset's key infrastructure components

Phase 2 is composed of the following three activities:

| | |
|---|---|
| P2.1 | Select Infrastructure Components to Evaluate |
| P2.2 | Run Vulnerability Evaluation Tools |
| P2.3 | Review Vulnerabilities and Summarize Results |

We describe each activity in the remainder of this section.

## P2.1 Select Infrastructure Components to Evaluate

**Activity Description**

The goals of Activity P2.1 are to select specific infrastructure components to examine for technology vulnerabilities by examining network access to each critical asset and to select an approach for the vulnerability evaluation. When selecting components and an approach, the analysis team must balance the comprehensiveness of the evaluation with the effort required to evaluate the components. The following key questions must be answered during this activity. The questions focus on identifying typical components and on selecting approaches for evaluating components.

| **Key Questions for P2.1: Select Infrastructure Components to Evaluate** |
|---|
| • Which specific component(s) will be evaluated for technology vulnerabilities?<br>- Is the infrastructure component typical of its class?<br>- How accessible is the infrastructure component? Is it "owned" by another organization? Is it a home machine?<br>- How critical is the infrastructure component to business operations? Will business operations be interrupted when the component is evaluated?<br>- What is the rationale for selecting this specific component(s)?<br>• What approach will be used to evaluate each selected component?<br>- Who will perform the evaluation?<br>- Which vulnerability evaluation tool(s) will be used?<br>- Will special permission or scheduling be required to evaluate the component? |

During Activity P2.1, specific infrastructure components are selected for evaluation. For each critical asset, the analysis team and key IT staff members review the threats for *human actors using network access*. These threats affect a critical asset due to deliberate exploitation of technology vulnerabilities or accidental actions by people. Based on the specific threats of this type to the critical asset, the team determines infrastructure components that are used by legitimate users to access the critical asset. They also identify which components threat actors could use to access the critical asset.

For organizations with large computing infrastructures, an optional first step is to identify key classes of infrastructure components. Individual components from each key class are then selected for evaluation. Then, individual components from each key class are selected for evaluation, making the infrastructure vulnerability evaluation a more manageable activity. The following questions could be answered during this optional step. These questions focus on components that are part of or related to the critical assets.

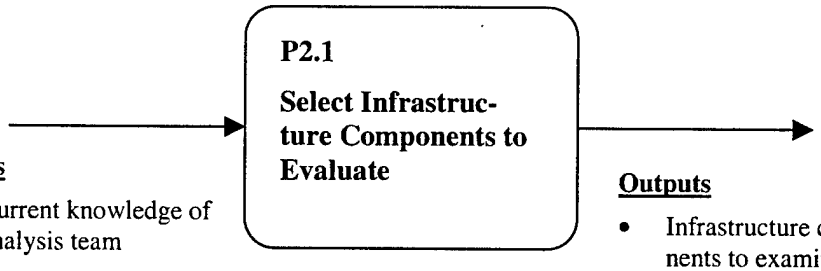
| **Optional Key Questions for P2.1: Select Infrastructure Components to Evaluate (Key Classes of Components)** |
|---|
| • Which system(s) is most closely linked to the critical asset? In which system(s) is the critical asset stored and processed?<br>- Which types of components are part of the system of interest? Consider servers, networking components, security components, desktop workstations, home machines, laptops, storage devices, wireless components, and others.<br>- Which types of components are related to the system of interest? From which types of hosts can the system of interest be legitimately accessed? Consider desktop machines, home machines, laptops, cellular phones, handheld devices, and others.<br>- How could threat actors access the system(s)? Via the Internet? Via the internal network? Shared external networks? Wireless devices? Others?<br>- Which types of components could a threat actor use to access the system of interest? Which could serve as intermediate access points? Consider physical and network access to servers, networking components, security components, desktop workstations, home machines, laptops, storage devices, wireless components, and others. |

**Participants**

The analysis team members participate in this activity. In addition, key IT staff members can be included if the analysis team needs to enhance its knowledge and skills in information technology. These additional people can be a part of the organization, or they can be from an external organization. It is important to ensure that the overall team participating in this activity has both an understanding of the legitimate business uses of the critical assets and an understanding of the underlying computing infrastructure for the organization.

**Diagram**

The following diagram shows the inputs and outputs of Activity P2.1: Select Infrastructure Components to Evaluate.




**Inputs**

- Current knowledge of analysis team
- Current knowledge of key IT personnel
- Current network topology diagram (IP2.1_1)
- Technology information (IP2.1_2)
- Critical assets (OP1.4_1)
- Threat profile for critical assets (OP1.6_1)

**Outputs**

- Infrastructure components to examine (OP2.1_1)
- Selected approach for evaluating each infrastructure component (OP2.1_2)
- Key classes of components (OP2.1_3)*

* Note: Key classes of components is optional. Infrastructure components can be selected without first identifying key classes.

**Importance**

Selected infrastructure components are those that are being evaluated for technology vulnerabilities. This activity is important because it sets the requirements for and the scope of the vulnerability evaluation in Activity P2.2.

## P2.2 Run Vulnerability Evaluation Tools

**Activity Description**

The goal of Activity P2.2 is to identify the technology vulnerabilities present on each selected infrastructure component and to create a preliminary summary of the vulnerabilities that are found. The following key questions must be answered during this activity. The questions focus on summarizing technology vulnerabilities according to when they need to be addressed.

| Key Questions for P2.2: Run Vulnerability Evaluation Tools |
| --- |
| • Which technology vulnerabilities are present on each evaluated infrastructure component? |
| • For each evaluated component, how many technology vulnerabilities must be addressed immediately? |
| • For each evaluated component, how many technology vulnerabilities must be addressed soon? |
| • For each evaluated component, how many technology vulnerabilities can be addressed later? |

To answer the first key question, the people who conduct the vulnerability evaluation must evaluate the organization's computing infrastructure in relation to a catalog of vulnerabilities. (See Attribute RA.5, Catalog of Vulnerabilities, of the OCTAVE criteria). This allows an organization to evaluate its technology base against known technology vulnerabilities, providing the organization with information about how vulnerable its computing infrastructure currently is.

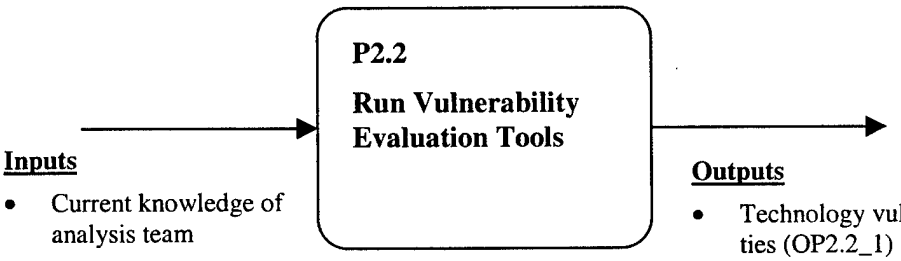
During Activity P2.2, specific infrastructure components are evaluated for technology vulnerabilities. The people leading this activity (members of the analysis team with an IT background or supplemental personnel) run vulnerability evaluation tools on each selected infrastructure components identified during Activity P2.1. Those individuals then review the detailed vulnerability information generated by the tool(s), interpret the results, and create a preliminary summary of the technology vulnerabilities for each key component.

**Participants**

The analysis team members participate in this activity. In addition, key information technology staff members can be included if the analysis team needs to enhance its knowledge and skills in information technology. These additional people can be a part of the organization or can be from an external organization. It is important to ensure that the individuals leading this activity have an in-depth understanding of information technology and computer security issues.

**Diagram**

The following diagram shows the inputs and outputs of Activity P2.2: Run Vulnerability Evaluation Tools.




**Inputs**

- Current knowledge of analysis team
- Current knowledge of key IT personnel
- Catalog of vulnerabilities (IP2.2_1)
- Current network topology diagram (IP2.1_1)
- Technology information (IP2.1_2)
- Infrastructure components to examine (OP2.1_1)
- Selected approach for evaluating each infrastructure component (OP2.1_2)

**Outputs**

- Technology vulnerabilities (OP2.2_1)
- Proposed technology vulnerability summary (OP2.2_2)

**Importance**

Technology vulnerabilities are weaknesses in systems that can directly lead to unauthorized action. These vulnerabilities are present in and apply to network services, architecture, operating systems, and applications. This activity is important because it helps organizations to identify specific weaknesses in their computing infrastructure that could be exploited by threat actors.

## P2.3 Review Vulnerabilities and Summarize Results

**Activity Description**

The goals of Activity P2.3 are to develop a summary of the technology vulnerabilities affecting each critical asset and to refine the threat profile for each critical asset based upon the evaluation of that asset's key infrastructure components. The following key questions must be answered during this activity. The questions focus on the vulnerability summaries and their effect on the organization.

| Key Questions for P2.3: Review Vulnerabilities and Summarize Results |
|---|
| • Are there any changes to the proposed vulnerability summary for each critical asset? What are these changes? |
| • Are there any specific actions or recommendations for addressing the technology vulnerabilities affecting each critical asset? What are these actions or recommendations? |
| • Do the technology vulnerabilities associated with each critical asset's key infrastructure components indicate the existence of threats that were previously believed to be negligible? What are these threats? |

During Activity P2.3, a technology vulnerability summary is created for each critical asset. The people who conducted the vulnerability evaluation (either members of the analysis team with an information technology background or supplemental personnel) review the proposed summary for each critical asset with the analysis team, ensuring that all analysis team members understand the results. Changes to the summary can be proposed and incorporated, if appropriate. In addition, the team identifies and records specific actions and recommendations for addressing the technology vulnerabilities. Finally, the team performs a gap analysis of the threat profile for each critical asset, refining the threat profile based upon the evaluation of the critical asset's key infrastructure components.

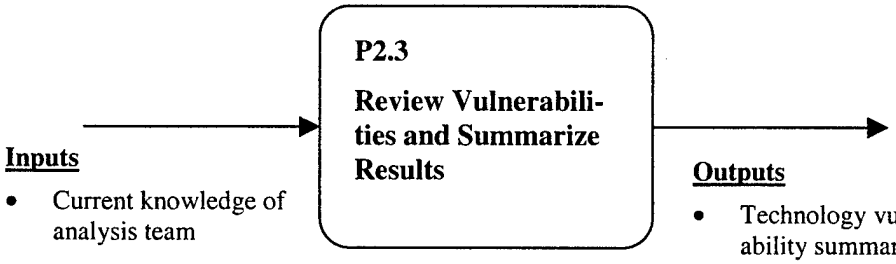
**Participants**

The analysis team members participate in this activity. In addition, key IT staff members can be included if the analysis team needs to enhance its knowledge and skills in information technology. These additional people can be a part of the organization, or they can be from an external organization. It is important to ensure that the individuals leading this activity have an in-depth understanding of in-

formation technology and computer security issues. The people who led Activity P2.1 must be involved in this activity.

**Diagram**

The following diagram shows the inputs and outputs of Activity P2.3: Review Vulnerabilities and Summarize Results.




**Inputs**

- Current knowledge of analysis team
- Current knowledge of key IT personnel
- Current network topology diagram (IP2.1_1)
- Technology information (IP2.1_2)
- Threat profiles for critical assets (OP1.6_1)
- Infrastructure components to examine (OP2.1_1)
- Selected approach for evaluating each infrastructure component (OP2.1_2)
- Proposed technology vulnerability summary (OP2.2_2)

**Outputs**

- Technology vulnerability summary (OP2.3_1)
- Threat profile for critical assets (OP2.3_2)

**Importance**

A technology vulnerability summary contains a description of the types of vulnerabilities found, when they need to be addressed, and specific actions or recommendations for addressing them. This activity is important because it captures the present state of the computing infrastructure with respect to technological weaknesses that could be exploited by human threat actors.

## A.3 Phase 3 (Develop Security Strategy and Plans) Activities

Phase 3 of OCTAVE is entitled Develop Security Strategy and Plans. During this part of the evaluation, the analysis team identifies risks to the organization's critical assets and decides what to do about them. The team analyzes the information generated during the evaluation and proposes a protection strategy for organizational improvement and risk mitigation plans to address the risks to the critical assets. The organization's senior managers review the proposed strategy and plans and refine them as appropriate, based on organizational resources and constraints. The senior managers then determine the next steps required to implement the protection strategy and the mitigation plans. During Phase 3, the analysis team

- identifies risks to the organization's critical assets
- develops priorities based on evaluating the risks against established evaluation criteria
- develops a proposed protection strategy for organizational security improvement
- develops proposed risk mitigation plans to address the risks to the critical assets

During Phase 3, the senior managers

- review and refine the proposed protection strategy
- review and refine proposed risk mitigation plans
- develop the next steps required to implement the protection strategy and the mitigation plans

Phase 3 is composed of the following seven activities:

| | |
|---|---|
| P3.1 | Identify Risks to Critical Assets |
| P3.2 | Create Risk Evaluation Criteria |
| P3.3 | Evaluate Risks to Critical Assets |
| P3.4 | Create Protection Strategy |
| P3.5 | Create Risk Mitigation Plans |
| P3.6 | Review Protection Strategy and Risk Mitigation Plans with Management |
| P3.7 | Identify Next Steps |

We describe each activity in the remainder of this section.

## P3.1 Identify Risks to Critical Assets

**Activity Description**

The goal of Activity P3.1 is to describe the potential impacts to the organization for the possible threat outcomes in each critical asset's threat profile. An optional goal is to gather probability data for the threats in each critical asset's threat profile. The following key questions must be answered during this activity. The questions focus on how threats affect the organization's business objectives and mission.

| Key Questions for P3.1: Identify Risks to Critical Assets (Impact) |
|---|
| For each critical asset, based on the threat outcomes:<br>• What is the potential impact to the organization's reputation?<br>• What is the potential impact on customer confidence?<br>• What is the potential impact to the customers' health?<br>• What is the potential impact to the organization's productivity?<br>• What fines or legal penalties could be imposed on the organization?<br>• What would be the financial impact to the organization? |

During Activity P3.1, risks are identified for each critical asset. The analysis team reviews the threat profile for each critical asset. For each threat outcome (disclosure, modification, loss/destruction, interruption) present in the profile, the team creates a narrative description of the potential impacts to the organization.

Using probability during the risk analysis is optional. If it is being used, then the analysis team describes the motive, means, and opportunity for human actors using either network or physical access, compiles any historical data for all threat types, and notes any unusual current conditions that can affect threats. If probability is used, then the following key questions must be answered during the activity. The questions focus on the factors that contribute to determining probability. See the *Notes* area below for additional thoughts about incorporating probability into the risk analysis.

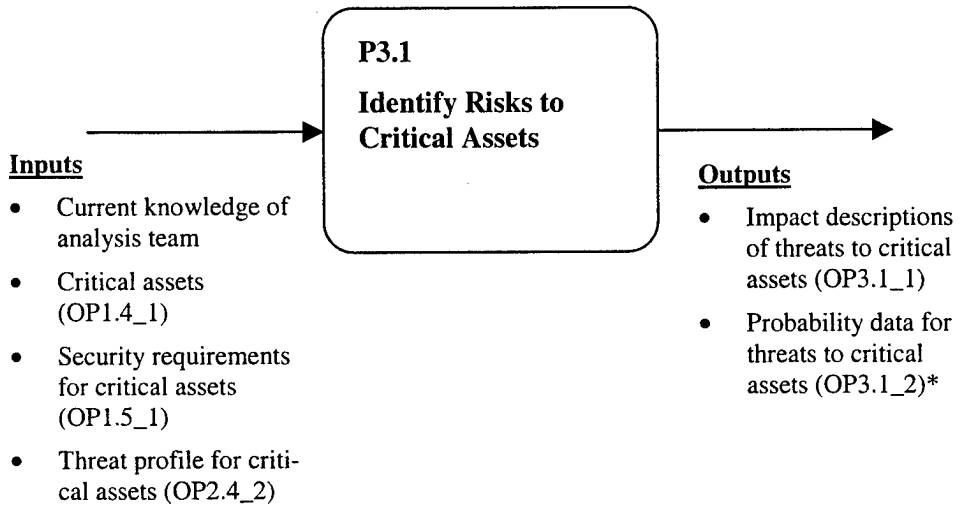
| Optional Key Questions for P3.1: Identify Risks to Critical Assets (Probability) |
|---|
| For each threat profile:<br>• Which critical assets are likely targets of human threat actors?<br>• What are the motives, means, and opportunities for each human threat actor that might use network access to violate the security requirements of the critical asset?<br>• What are the motives, means, and opportunities for each human threat actor that might use physical access to violate the security requirements of the critical asset?<br>• What historical data are available for the threats in the threat profile?<br>• What unusual current conditions or circumstances might affect the probability of the threats in the threat profile? |

**Participants**

The analysis team members are the key participants in this activity. If appropriate, the analysis team can include selected personnel to augment its skills.

**Diagram**

The following diagram shows the inputs and outputs of Activity P3.1: Identify Risks to Critical Assets.




* Note: Probability is optional. The risk analysis can be performed using only impact.

**Importance**

The essential risk property is impact, which describes the effect of threats on the organization's mission and business objectives. This activity is important because it focuses on the effect of threats on the organization by putting threats into the context of what the organization is trying to achieve. It forms the basis for setting priorities during later activities. If probability is also being used, the probability data gathered during this activity are important because they can be used to refine priorities. See the *Notes* area below for additional thoughts about incorporating probability into the risk analysis.

**Notes**

For information security risks, probability is a more complex and imprecise variable than is normally found in other risk management domains, because risk factors are constantly changing. Probability is highly subjective in the absence of objective data and must be used carefully during risk analysis. Impact values are used as the primary factor behind setting priorities in OCTAVE. Probability values can be factored into prioritization, but care must be taken when doing so. A subjective view of probability can refine the understanding of threat by focusing on information about motives, means, opportunities, historical data, and any unusual conditions.

## P3.2 Create Risk Evaluation Criteria

**Activity Description** The goal of Activity P3.2 is to define the risk evaluation criteria for the risk's impact, establishing a common understanding of the qualitative measures of impact. An optional goal is to define the risk evaluation criteria for probability, establishing a common understanding of the qualitative measures of probability. The following key questions must be answered during this activity. The questions focus on defining measures of impact.

| Key Questions for P3.2: Create Risk Evaluation Criteria (Impact) |
|---|
| • What defines a "high" impact to the organization? |
| • What defines a "medium" impact to the organization? |
| • What defines a "low" impact to the organization? |

During Activity P3.2, risk evaluation criteria are created. The analysis team determines what constitutes high, medium, and low impacts to the organization, considering a variety of potential impact areas.

Using probability during the risk analysis is optional. If it is being used, then the analysis team determines what constitutes high, medium, and low probabilities for threats. When establishing evaluation criteria for probability, the team considers information about motive, means, and opportunity for human actors using either network or physical access, any historical data for all threat types, and any unusual current conditions that can affect threats. If probability is used, then the following key questions must be answered during the activity. The questions focus on defining measures of probability.

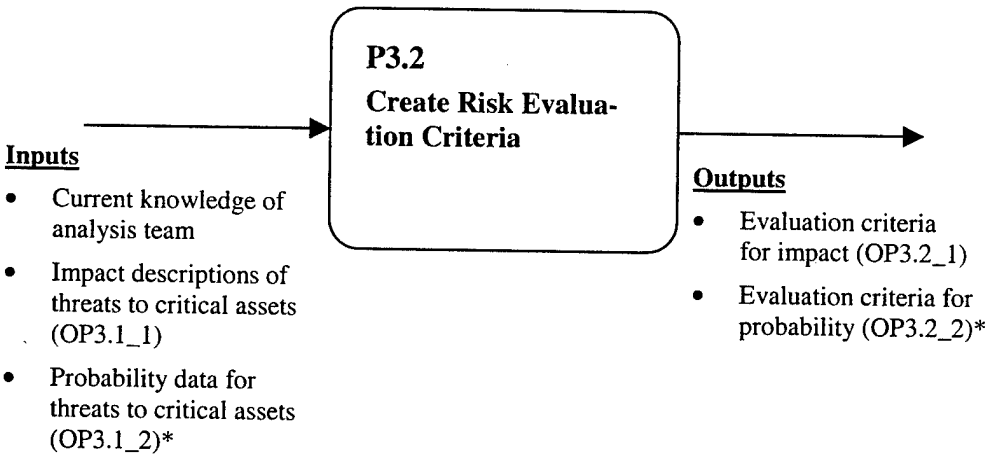
| Optional Key Questions for P3.2: Create Risk Evaluation Criteria (Probability) |
|---|
| • What defines a "high" likelihood of occurrence? |
| • What defines a "medium" likelihood of occurrence? |
| • What defines a "low" likelihood of occurrence? |

**Participants**

The analysis team members are the key participants in this activity. If appropriate, the analysis team can include selected personnel to augment its skills.

**Diagram**

The following diagram shows the inputs and outputs of Activity P3.2: Create Risk Evaluation Criteria.




* Note: Probability is optional. The risk analysis can be performed using only impact.

**Importance**

Evaluation criteria are a set of qualitative measures against which impact and probability are evaluated. This activity is important because it establishes the criteria for what constitutes high, medium, and low impacts to an organization. In Activity P3.3, the impact descriptions from Activity P3.1 are evaluated against the criteria generated during this activity, yielding impact values. Impact values are used to establish priorities during risk mitigation. Thus, it is important to establish criteria that are meaningful to the organization. If probability is also being used, this activity also establishes what constitutes high, medium, and low probabilities for each threat. In Activity P3.3, the probability data from Activity P3.1 are evaluated against the criteria generated during this activity, yielding probability values. Probability values can be used to refine the priorities that were established using impact.

**Notes**

Evaluation criteria are qualitative measures against which impact and probability are evaluated. The evaluation criteria used to evaluate impact and probability are the same for all critical assets.

For impact, evaluation criteria are created for a broad range of impact types, or categories. Evaluation criteria are typically created for the following categories of impact:

- reputation/customer confidence
- safety/health issues
- fines/legal penalties
- financial impact
- productivity

The impact areas are contextual and should be tailored to meet the needs of each organization. Before conducting an evaluation, the analysis team needs to determine which impact areas to consider. One way to determine unique areas for an organization is to consider the organization's business objectives and make sure that impact areas are linked to those business objectives.

## P3.3 Evaluate Risks to Critical Assets

**Activity Description**

The goal of Activity P3.3 is to establish impact values (high, medium, or low) for each impact description, completing the risk profile for each critical asset. An optional goal is to establish probability values (high, medium, or low) for each threat. The following key questions must be answered during this activity. The questions focus on using the measures of impact to determine the value for each impact.

| **Key Questions for P3.3: Evaluate Risks to Critical Assets (Impact)** |
|---|
| For each impact description:<br>• Based on the evaluation criteria, is the impact to the organization "high?"<br>• Based on the evaluation criteria, is the impact to the organization "medium?"<br>• Based on the evaluation criteria, is the impact to the organization "low?" |

During Activity P3.3, impact values are established for each impact description. The analysis team reviews each impact description and then evaluates it against the evaluation criteria for impact, assigning the impact description a value (high, medium, or low).

Using probability during the risk analysis is optional. If it is being used, then the analysis team reviews the probability data for each threat and evaluates the data against the evaluation criteria for probability, assigning the threat a probability value (high, medium, or low). When the analysis team assigns an impact value to each impact description for a critical asset and, optionally, a probability value to each threat to the critical asset, it completes the risk profile for that critical asset. See the *Notes* area below for additional information about risk profiles. If probability is used, then the following key questions must be answered during the activity. The questions focus on using the measures of probability to determine the probability value for each threat.

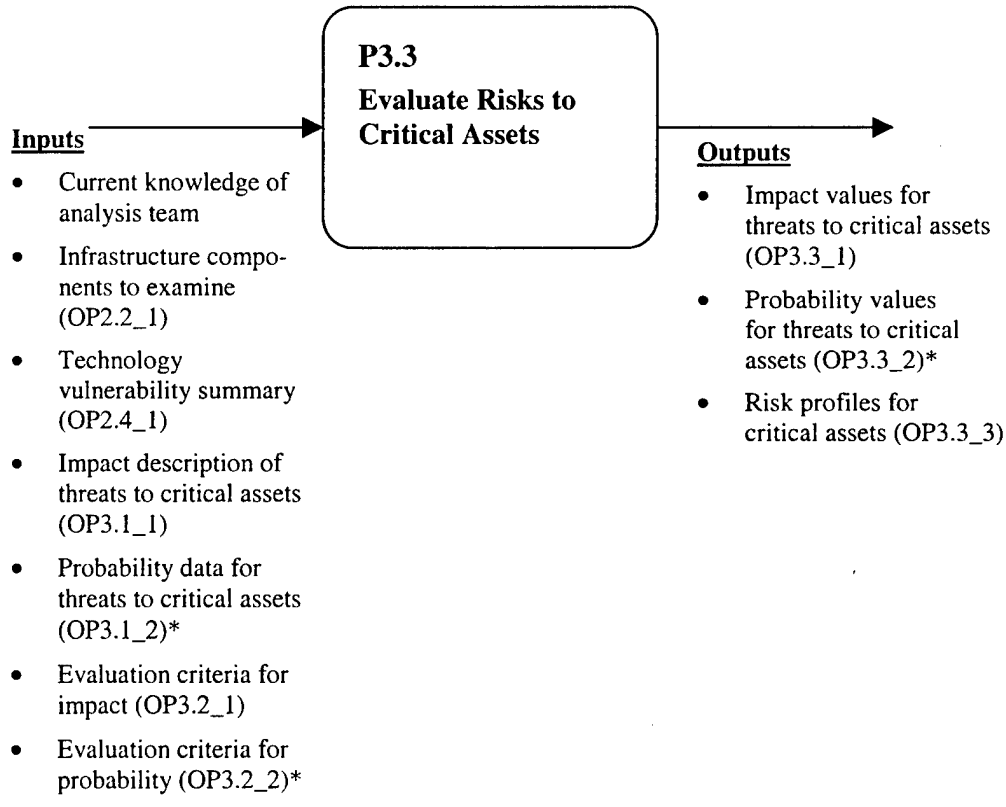
| Optional Key Questions for P3.3: Evaluate Risks to Critical Assets (Probability) |
|---|
| For each threat in the threat profile:<br>• Based on the evaluation criteria, is the threat probability "high?"<br>• Based on the evaluation criteria, is the threat probability "medium?"<br>• Based on the evaluation criteria, is the threat probability "low?" |

**Participants**

The analysis team members are the key participants in this activity. If appropriate, the analysis team can include selected personnel to augment its skills.

**Diagram**

The following diagram shows the inputs and outputs of Activity P3.3: Evaluate Risks to Critical Assets.




* Note: Probability is optional. The risk analysis can be performed using only impact.

**Importance**

Impact values are qualitative measures of a risk's impact to the organization (high, medium, or low). This activity is important because it requires the analysis team to establish an impact value for each impact description that was generated during Activity P3.1. Impact values are used to establish priorities when developing risk mitigation plans. If probability is also being used, this activity requires the analysis team to establish a probability value for each threat. Probability values can be used to refine the priorities established using impact.

**Notes**

A risk profile for a critical asset defines the range of risks that can affect that asset. The risk profile for a critical asset consists of the following information:

- the threat profile for that critical asset
- the security requirements for that critical asset
- the impact description of the threats in the threat profile
- probability data for the threats in the threat profile*
- impact values for threats in the threat profile
- probability values for threats in the threat profile*
- infrastructure components to examine for the critical asset
- technology vulnerability summary for each infrastructure component examined

* These items are optional. They are part of a risk profile only if probability is used during the risk analysis.

## P3.4 Create Protection Strategy

**Activity Description** The goal of Activity P3.4 is to create a proposed protection strategy for the organization. Key questions derived from the strategic practices in the catalog of practices must be used during this activity. The following key questions are examples of questions related to strategic security practices. The questions focus on developing a set of strategies framed around the catalog of practices.

| Key Questions for P3.4: Create Protection Strategy |
| --- |
| • What training and education initiatives could help the organization maintain or improve its security practices? |
| • What can be done to improve the way in which security issues are integrated with the organization's business strategy? |
| • What can be done to ensure that all staff members understand their security roles and responsibilities? |
| • What funding level is appropriate to support the organization's security needs? |
| • Are the organization's policies and procedures sufficient for its security needs? How could they be improved? |
| • Does the organization have policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners)? What can the organization do to improve the way in which it protects information when working with external organizations? |
| • What can the organization do to improve the way in which it verifies that outsourced security services, mechanisms, and technologies meet its needs and requirements? |
| • What can be done to ensure that the organization has defined and tested business continuity and disaster recovery plans? What can be done to ensure that staff members are aware of and understand the organization's business continuity and disaster recovery plans? |

During Activity P3.4, a proposed protection strategy for the organization is developed. The analysis team reviews the current security practices used by the organization, the current organizational vulnerabilities present in the organization, and the risk profile for each critical asset. The team starts to develop a protection strategy by considering the strategic practice areas of the catalog of practices. The team looks for strategies that help the organization maintain its cur-

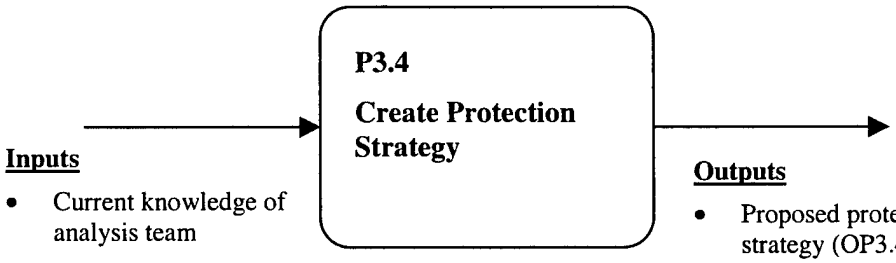
rent security practices, address its organizational vulnerabilities, and address its highest priority risks. The analysis team then looks at the major operational practice areas of the catalog and determines any additional strategies that could enable personnel in the organization to better understand and carry out their security responsibilities in those areas.

**Participants**

The analysis team members are the key participants in this activity. If appropriate, the analysis team can include selected personnel to augment its skills.

**Diagram**

The following diagram shows the inputs and outputs of Activity P3.4: Create Protection Strategy.




**Inputs**

- Current knowledge of analysis team
- Catalog of practices (IP1.2_3)
- Current security practices (OP1.2_1)
- Current organizational vulnerabilities (OP1.3_1)
- Risk profiles for critical assets (OP3.3_3)

**Outputs**

- Proposed protection strategy (OP3.4_1)

**Importance**

A protection strategy defines the strategies that an organization uses to enable, initiate, implement, and maintain its internal security. This activity is important because it requires the analysis team to create a strategy based on the information that it has gathered during the evaluation. The proposed protection strategy represents a proposal to the organization's management by the analysis team. The strategy is used to focus Activity P3.6, Review Protection Strategy and Risk Mitigation Plans with Management, where the organization's senior managers review and refine the proposed strategy.

**Notes**

After the risk mitigation plans are created in Activity P3.5, the analysis team should make sure that the strategies in the protection strategy and the actions in the risk mitigation plans complement each other. The team can also look at common themes among the protection strategy and mitigation plans to get a feel for high-priority strategies and actions to implement after the evaluation.

## P3.5 Create Risk Mitigation Plans

**Activity Description**

The goal of Activity P3.5 is to create proposed risk mitigation plans to reduce the risks to the critical assets. The following key questions must be answered during this activity for each category of threat as defined in the threat profile. The questions focus on the organization's ability to recognize, resist, and recover from threats to the organization's critical assets.

| Key Questions for P3.5: Create Risk Mitigation Plans |
| --- |
| For each critical asset:<br>• Which are the high-priority risks to the critical asset? Which threat types would cause the largest impact to the organization's mission and business objectives?<br>• Which risks will the organization actively mitigate by implementing actions intended to counteract the associated threat type? Which risks will the organization accept and take no action to address?<br>• What actions could be taken to help recognize or detect the threat types as they occur?<br>• What actions could be taken to help resist or prevent the threat types from occurring?<br>• What actions could be taken to help recover from the threat types if they occur?<br>• What other actions could be taken to address these threat types?<br>• What measures could be used to verify that this mitigation plan works and is effective? |

During Activity P3.5, proposed risk mitigation plans to reduce the risks to the critical assets are developed. The analysis team reviews the current security practices used by the organization, the current organizational vulnerabilities present in the organization, and the risk profile for each critical asset. For each critical asset, the team determines which risks the organization will actively mitigate by implementing actions intended to counteract the associated threat type and which risks the organization will accept and take no further action to address. The team uses impact values when it determines whether to accept or mitigate a risk. If probability is also being used, probability values can be factored into the decision as well. For risks that are

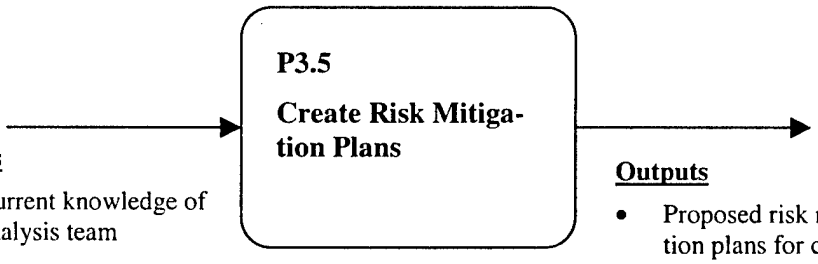
being mitigated, the team develops risk mitigation plans by identifying mitigation actions designed to counter the threats to the critical assets. The team uses impact values to establish mitigation priorities. It focuses on mitigating the threats that result in the largest impact to the organization's mission and business objectives. If probability is also being used in the analysis, probability values can be applied to refine the priorities established using impact.

**Participants**

The analysis team members are the key participants in this activity. If appropriate, the analysis team can include selected personnel to augment its skills.

**Diagram**

The following diagram shows the inputs and outputs of Activity P3.5: Create Risk Mitigation Plans.




**Inputs**

- Current knowledge of analysis team
- Catalog of practices (IP1.2_3)
- Current security practices (OP1.2_1)
- Current organizational vulnerabilities (OP1.3_1)
- Security requirements for critical assets (OP1.5_1)
- Evaluation criteria for impact (OP3.2_1)
- Evaluation criteria for probability (OP3.2_2)*
- Risk profiles for critical assets (OP3.3_3)

**Outputs**

- Proposed risk mitigation plans for critical assets (OP3.5_1)

* Note: Probability is optional. Risk mitigation plans can be created using only impact.

**Importance**

Risk mitigation plans for critical assets define the actions intended to reduce the risks to the critical assets. This activity is important because it requires the analysis team to create a risk mitigation plan for each critical asset based on the information that it has gathered during the evaluation. The proposed risk mitigation plans represent proposals to the organization's management by the analysis team. The plans are used to focus Activity P3.6, Review Protection Strategy and Risk Mitigation Plans with Management, where the organization's senior managers review and refine the proposed plans.

**Notes**

After this activity has been completed, the analysis team should make sure that the strategies in the protection strategy and the actions in the risk mitigation plans complement each other. The team can also look at common themes among the protection strategy and mitigation plans to get a feel for high-priority strategies and actions to implement after the evaluation.

## P3.6 Review Protection Strategy and Risk Mitigation Plans with Management

**Activity Description**

The goal of Activity P3.6 is for the organization's senior managers to review the proposed protection strategy and risk mitigation plans with the analysis team and to refine them as appropriate. The following key questions must be answered during the activity. The questions focus on the content of the protection strategy and risk mitigation plans in relation to the organizational resources and constraints.

| Key Questions for P3.6: Review Protection Strategy and Risk Mitigation Plans with Management |
|---|
| Based on organizational resources and constraints:<br>• What refinements, modifications, additions, or deletions must be made to the protection strategy?<br>• What refinements, modifications, additions, or deletions must be made to each risk mitigation plan? |

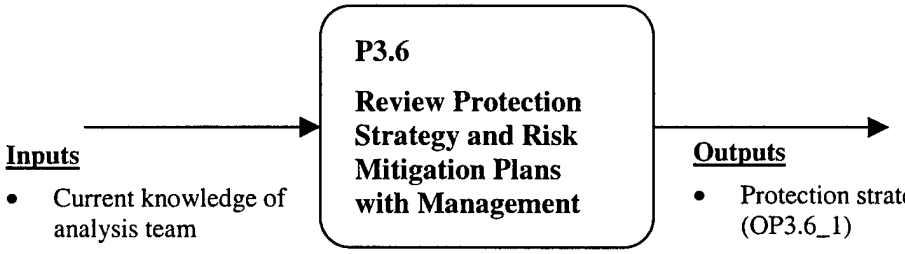
During Activity P3.6, the development of a protection strategy for the organization and risk mitigation plans to reduce the risks to the critical assets is completed. The analysis team presents the proposed protection strategy and proposed risk mitigation plans to the organization's senior managers. The senior managers then make any necessary refinements, modifications, additions, or deletions to the proposed protection strategy and risk mitigation plans, taking into account organizational resources and constraints. The result is the final version of the protection strategy and risk mitigation plans.

**Participants**

The organization's senior managers are the key participants in this activity. The analysis team members facilitate the activity, ensuring that the activity is completed satisfactorily. If appropriate, the analysis team can include selected personnel to augment its skills.

**Diagram**

The following diagram shows the inputs and outputs of Activity P3.6: Review Protection Strategy and Risk Mitigation Plans with Management.




**Inputs**

- Current knowledge of analysis team
- Current knowledge of management
- Current security practices (OP1.2_1)
- Current organizational vulnerabilities (OP1.3_1)
- Risk profiles for critical assets (OP3.3_3)
- Proposed protection strategy (OP3.4_1)
- Proposed risk mitigation plans for critical assets (OP3.5_1)

**Outputs**

- Protection strategy (OP3.6_1)
- Risk mitigation plans for critical assets (OP3.6_2)

**Importance**

A protection strategy defines the strategies that an organization uses to enable, initiate, implement, and maintain its internal security. Risk mitigation plans for critical assets define the mitigation actions intended to reduce the risks to the critical assets. This activity is important because it requires the organization's senior managers to review the proposed protection strategy and risk mitigation plans from the organizational perspective. The senior managers then refine the strategy and plans based on the managers' understanding of organizational resources and constraints. This activity is also important for developing senior management sponsorship of the protection strategy and risk mitigation plans.

## P3.7 Identify Next Steps

**Activity Description**

The goal of Activity P3.7 is for the organization's senior managers to identify next steps that will be taken to implement the protection strategy and the mitigation plans. The following key questions must be answered during this activity. The questions focus on management's role in enabling ongoing security improvement.

| Key Questions for P3. 7: Identify Next Steps |
| --- |
| • What will the organization do to build on the results of this evaluation? |
| • What else will management do to ensure that the organization improves its information security? |
| • What can management do to support this security improvement initiative? |
| • What are management's plans for ongoing security evaluation activities? |

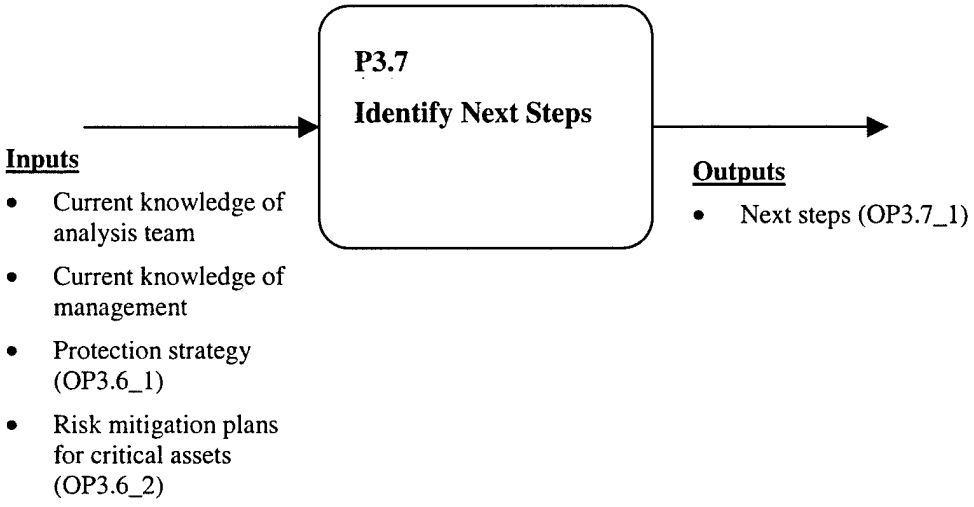
During Activity P3.7, the next steps required to implement the protection strategy and the mitigation plans are defined. The senior managers determine what the organization will do to implement the results of the evaluation and determine what the managers will do to enable security improvement in the organization. The managers also determine if there are any other security improvement activities that need to be addressed and determine how the organization will approach future assessments.

**Participants**

The organization's senior managers are the key participants in this activity. The analysis team members facilitate the activity, ensuring that the activity is completed satisfactorily. If appropriate, the analysis team can include selected personnel to augment its skills.

**Diagram**

The following diagram shows the inputs and outputs of Activity P3.7: Identify Next Steps.




**Importance**

The next steps define what the organization will do to implement the results of the evaluation. This activity is important because it requires management to identify actions that enable ongoing security improvement. Without the explicit definition of the steps required to implement the results of the evaluation and without strong sponsorship from senior management, the initiative to improve the organization's security posture will likely fail.

## A.4 Data Dictionary for Activity Inputs and Outputs

This section contains a data dictionary that defines each input and output in the diagrams that we presented in sections A.1-A.3. The data items are presented by activity. For an explanation of the numbering scheme, see the introduction to this appendix.

### General

**Current knowledge of organizational staff**

The current knowledge of the organizational staff includes the collective knowledge, skills, and abilities of the people who contribute their understanding of assets, current security requirements, and organizational vulnerabilities. This includes people from both the business and information technology areas of the organization. In addition, multiple organizational levels (senior management, operational area management, staff) must be represented.

**Current knowledge of analysis team**

The current knowledge of the analysis team includes the collective knowledge, skills, and abilities of the analysis team members and any supplemental personnel participating in a specific activity.

**Current knowledge of key IT personnel**

The current knowledge of key IT personnel includes the collective knowledge, skills, and abilities of the information technology personnel who participate in Phase 2 of OCTAVE. These people have an in-depth understanding of the organization's computing infrastructure as well as information security issues. These people can be a part of the organization or can be from an external organization.

## Activity P1.1 Identify Assets

**Assets (OP1.1_1)**

This is a listing of the information-related assets for the organization. An asset is something of value to the organization. The following categories of assets are typically considered during the evaluation:

- information – documented (paper or electronic) data or intellectual property used to meet the mission of the organization
- systems – information systems that process and store information. Systems are a combination of information, software, and hardware assets. Any host, client, or server can be considered to be a system
- software – software applications and services (operating systems, database applications, networking software, office applications, custom applications, etc.)
- hardware – information technology physical devices (workstations, servers, etc.)
- people – the people in the organization, including their skills, training, knowledge, and experience

## Activity P1.2 Identify Current Security Practices

**Organizational data (IP1.1_1)**

Organizational data include

- information about how the organization is structured
- the organization's currently documented policies and procedures related to security

**Laws and regulations (IP1.2_1)**

Laws and regulations define the legal obligations of the organization with respect to security.

**Catalog of practices (IP1.2_2)**

The catalog of practices defines the range of security practices that must be considered during the evaluation. The requirements for the catalog of practices are defined in the OCTAVE criteria. (See OCTAVE Attribute RA.3, Catalog of Practices, of the OCTAVE criteria.)

**Current security practices (OP1.2_1)**

Current security practices are those actions presently used by the organization to initiate, implement, and maintain its internal security. Security practices are used to protect an organization's information-related assets.

## Activity P1.3 Identify Current Organizational Vulnerabilities

**Current organizational vulnerabilities (OP1.3_1)**

Current organizational vulnerabilities are weaknesses in organizational policy or practice that can result in unauthorized actions occurring. They are indications of missing or inadequate security practices.

## Activity P1.4 Identify Critical Assets

**Critical assets (OP1.4_1)**

Critical assets are those that are believed to be the most important assets to the organization. The organization will suffer a large adverse impact if the security requirements of these assets are violated.

## Activity P1.5 Describe Security Requirements for Critical Assets

**Security requirements for critical assets (OP1.5_1)**

Security requirements for critical assets outline the qualities of the critical assets that are important to an organization. Security requirements considered during the evaluation typically include

- confidentiality
- integrity
- availability

## Activity P1.6 Create Threat Profiles for Critical Assets

**Generic threat profile (IP1.6_1)**

The generic threat profile defines the range of common threats that must be considered for each critical asset. The requirements for the generic threat profile are defined in the OCTAVE criteria. (See OCTAVE Attribute RA.4, Generic Threat Profile, of the OCTAVE criteria.)

**Threat profile for critical assets (OP1.6_1)**

The threat profile for a critical asset defines the range of threats that can affect that critical asset. Threat profiles contain categories that are grouped according to threat source. Attributes of a threat profile include asset, access, actor, motive, and outcome. (Examples of threat categories include human actors using network access, human actors using physical access, system problems, and other problems).

## Activity P2.1 Select Infrastructure Components to Evaluate

**Current network topology diagram (IP2.1_1)**

A current network topology diagram consists of electronic or paper documents used to display the logical or physical mapping of a network. These documents identify the connectivity of systems and networking components.

**Technology information (IP2.1_2)**

Technology information encompasses all detailed information about the organization's computing infrastructure. This includes the Internet Protocol (IP) addresses and fully qualified domain names for all infrastructure components.

**Infrastructure components to examine (OP2.1_1)**

Infrastructure components to examine are components that have been chosen for evaluation. These components are evaluated for technology vulnerabilities.

**Selected approach for evaluating each infrastructure component (OP2.1_2)**

The selected approach for evaluating each infrastructure component sets the requirements for and the scope of the vulnerability evaluation. The following are typically included in the approach:

- who will perform the evaluation
- which vulnerability evaluation tool(s) will be used

**Key classes of components (OP2.1_3)***

Key classes of components are types of devices that are important in processing, storing, or transmitting critical information. They represent related assets to critical assets. The following classes of components are typically considered during the evaluation:

- servers – hosts within your IT infrastructure that provide IT services to your organization
- networking components – devices important to your organization's networks. Routers, switches, and modems are all examples of this class of component.
- security components – devices that have security as their primary function (e.g., a firewall)
- desktop workstations – hosts on your networks that staff members use to conduct business
- home computers – home PCs that staff members use to access information remotely via your organization's networks
- laptops – portable PCs that staff members use to access information remotely via your organization's networks

## Activity P2.1 Select Infrastructure Components to Evaluate (cont.)

**Key classes of components (OP2.1_3)* (cont.)**

- storage devices – devices where information is stored, often for backup purposes
- wireless components – devices, such as cell phones and wireless access points, that staff members may use to access information (e.g., email)
- others – any other type of device that could be part of your threat scenarios, but does not fall into the above classes

* Note: Selecting key classes of components (OP2.1_3) is an optional first step useful for large computing infrastructures. It may not be necessary for smaller networks with limited components. The list of key classes can be used to help identify specific components (OP2.1_1).

## Activity P2.2 Run Vulnerability Evaluation Tools

**Catalog of vulnerabilities (IP2.2_1)**

The catalog of vulnerabilities is a collection of vulnerabilities based on platform and application. It is used to evaluate an organization's computing infrastructure for technology vulnerabilities. The requirements for the catalog of vulnerabilities are defined in the OCTAVE criteria. (See OCTAVE Attribute RA.5, Catalog of Vulnerabilities, of the OCTAVE criteria.)

**Technology vulnerabilities (OP2.2_1)**

Technology vulnerabilities are weaknesses in systems that can directly lead to unauthorized action. Technology vulnerabilities are present in and apply to network services, architecture, operating systems, and applications. Types of technology vulnerabilities include design, implementation, and configuration vulnerabilities.

**Proposed technology vulnerability summary (OP2.2_2)**

The proposed technology vulnerability summary for each component typically contains the following information for each infrastructure component that is evaluated:

- the number of vulnerabilities to fix immediately (high-severity vulnerabilities)
- the number of vulnerabilities to fix soon (medium-severity vulnerabilities)

- the number of vulnerabilities to fix later (low-severity vulnerabilities)

## Activity P2.3 Review Vulnerabilities and Summarize Results

**Technology vulnerability summary (OP2.3_1)**

The technology vulnerability summary for each component typically contains the following information for each infrastructure component that is evaluated:

- the number of vulnerabilities to fix immediately (high-severity vulnerabilities)
- the number of vulnerabilities to fix soon (medium-severity vulnerabilities)
- the number of vulnerabilities to fix later (low-severity vulnerabilities)

In addition, the summary for each critical asset contains specific actions or recommendations for addressing the technology vulnerabilities that were found.

**Threat profile for critical assets (OP2.3_2)**

The threat profile for a critical asset defines the range of threats that can affect that critical asset. Threat profiles contain categories that are grouped according to threat source. (Examples of threat categories include human actors using network access, human actors using physical access, system problems, and other problems).

## Activity P3.1 Identify Risk Properties for Threats to Critical Assets

**Impact descriptions of threats to critical assets (OP3.1_1)**

The impact description of a threat to a critical asset defines the effect(s) of the threat on the organization's mission and business objectives.

**Probability data for threats to critical assets (OP3.1_2)***

The probability data for a threat to a critical asset describe the motive, means, and opportunity for human actors using either network or physical access; compile any historical data for all threat types; and note any unusual current conditions that can affect threats.

* Note: Probability data for threats to critical assets (OP3.1_2) is an optional data item. See Activity P3.1: Identify Risk Properties for Threats to Critical Assets for more information.

## Activity P3.2 Create Risk Evaluation Criteria

**Evaluation criteria for impact (OP3.2_1)**

Evaluation criteria for impact are a set of qualitative measures against which a risk is evaluated. Evaluation criteria define high, medium, and low impacts for an organization. Evaluation criteria are typically created for the following categories of impact:

- reputation/customer confidence
- safety/health issues
- fines/legal penalties
- financial impact
- productivity

**Evaluation criteria for probability (OP3.2_2)***

Evaluation criteria for probability are a set of qualitative measures against which a risk is evaluated. Evaluation criteria define high, medium, and low probabilities for threats to critical assets.

* Note: Evaluation criteria for probability (OP3.2_2) is an optional data item. See Activity P3.2: Create Risk Evaluation Criteria for more information.

## Activity P3.3 Evaluate Risks to Critical Assets

**Impact values for threats to critical assets (OP3.3_1)**

Impact values for threats to critical assets are qualitative measures (high, medium, or low) of the resulting impact to the organization's mission and business objectives.

**Probability values for threats to critical assets (OP3.3_2)***

Probability values for threats to critical assets are qualitative measures (high, medium, or low) of the likelihood of occurrence.

**Risk profiles for critical assets (OP3.3_3)**

A risk profile for a critical asset defines the range of risks that can affect that asset. The following items are typically included in the risk profile for a critical asset:

- the threat profile for that critical asset
- the security requirements for that critical asset
- the impact description of the threats in the threat profile
- impact values for threats in the threat profile
- infrastructure components to examine for the critical asset
- technology vulnerability summary for each infrastructure component examined

If probability is used during the risk analysis, then the following can also be included in the risk profile for a critical asset:

- probability data for the threats in the threat profile
- probability values for threats in the threat profile

* Note: Probability values for threats to critical assets (OP3.3_2) is an optional data item. See Activity P3.3: Evaluate Risks to Critical Assets for more information.

## Activity P3.4 Create Protection Strategy

**Proposed protection strategy (OP3.4_1)**

The proposed protection strategy defines the strategies that the organization could use to enable, initiate, implement, and maintain its internal security. It represents a proposal to the organization's management by the analysis team. The proposed protection strategy tends to incorporate long-term organization-wide initiatives and is structured using the practice areas defined in the catalog of practices. (See OCTAVE Attribute RA.3, Catalog of Practices, of the OCTAVE criteria.)

## Activity P3.5 Create Risk Mitigation Plans

**Proposed risk mitigation plans for critical assets (OP3.5_1)**

The proposed risk mitigation plans for critical assets define the mitigation actions intended to reduce the risks to the critical assets. They represent proposals to the organization's management by the analysis team. Risk mitigation plans tend to incorporate actions, or countermeasures, designed to counter the threats to the assets. The actions are based on the practices contained in the catalog of practices. (See OCTAVE Attribute RA.3, Catalog of Practices, of the OCTAVE criteria.)

## Activity P3.6 Review Protection Strategy and Risk Mitigation Plans with Management

**Protection strategy (OP3.6_1)**

The protection strategy defines the strategies that the organization could use to enable, initiate, implement, and maintain its internal security. It is the organization's strategy for protecting its critical assets, and the analysis team has incorporated considerations of organizational resources and constraints into the development of this strategy. The protection strategy tends to incorporate long-term organization-wide initiatives and is structured using the practice areas defined in the catalog of practices. (See OCTAVE Attribute RA.3, Catalog of Practices, of the OCTAVE criteria.)

**Risk mitigation plans for critical assets (OP3.6_2)**

The risk mitigation plans for critical assets define the mitigation actions intended to reduce the risks to the critical assets. During the development of these plans, the analysis team has considered organizational resources and constraints. Risk mitigation plans tend to incorporate actions, or countermeasures, designed to counter the threats to the assets. The actions are based on the practices contained in the catalog of practices. (See OCTAVE Attribute RA.3, Catalog of Practices, of the OCTAVE criteria.)

## Activity P3.7 Identify Next Steps

**Next steps (OP3.7_1)**

The next steps define what the organization will do to implement the results of the evaluation. Next steps typically include

- what the organization will do to implement the results of the evaluation
- what the senior managers will do to enable security improvement in the organization
- whether there are any other security improvement activities that need to be addressed
- how the organization will approach future assessments

# Appendix B: The Relationship Between the OCTAVE Criteria and the OCTAVE Method

In this appendix, we examine the relationship between the OCTAVE criteria and the OCTAVE Method. We begin by providing a brief description of the OCTAVE Method. You can find a more detailed description of the method in the *OCTAVE Method Implementation Guide, v2.0* [Alberts 01a].

## B.1 The OCTAVE Method

The OCTAVE Method uses a three-phase approach to examine organizational and technological issues, assembling a comprehensive picture of an organization's information security needs. The method uses workshops to encourage open discussion and exchange of information about assets, security practices, and solutions. Each workshop in the OCTAVE Method is led by an analysis team, which is an interdisciplinary team consisting of personnel from the business units and the information technology department of the organization.

Some preparation activities are necessary to establish a good foundation for successfully completing the evaluation. The preparation activities for the OCTAVE Method are

- *Obtain senior management sponsorship of OCTAVE.* The planning activities for the OCTAVE Method start with senior management sponsorship. This could require briefings to senior managers to help them understand the process.
- *Select analysis team members.* Representatives from both the business and information technology parts of the organization will be on the analysis team. The size of the analysis team is three to five people. Senior managers should be involved in the selection of team members. In addition, it is helpful if some of the members come from the operational areas that will be participating in the evaluation.
- *Train analysis team.* The analysis team needs to be trained in the OCTAVE Method. Each member of the analysis team needs to understand his or her role during each workshop.
- *Select operational areas to participate in OCTAVE.* A key part of the planning process is selecting the operational areas that will participate in the OCTAVE Method. This scopes the evaluation. The analysis team will lead this activity with senior management input.
- *Select participants.* Participants for the knowledge elicitation workshops (Processes 1-3) need to be selected. Also, people with special skills to augment the analysis team at cer-

tain points in the process need to be selected. The analysis team members will lead the selection of participants. They need to get input from the senior managers and from the managers for each of the operational areas participating in the evaluation.

- *Coordinate logistics*. The analysis team members need to ensure that rooms and equipment are available for all workshops.
- *Brief all participants*. The analysis team should conduct a briefing for all participants prior to their participation in the process.

Once the preparation is completed, the organization is ready to start the evaluation. The three phases of the OCTAVE Method and their processes are described below.

**Phase 1: Build Asset-Based Threat Profiles**. This is an organizational evaluation. The analysis team determines which assets are most important to the organization (critical assets) and identifies what is currently being done to protect those assets. The processes of Phase 1 are

- Process 1: Identify Senior Management Knowledge – Selected senior managers identify important assets, perceived threats, security requirements, current security practices, and organizational vulnerabilities.
- Process 2: Identify Operational Area Management Knowledge – Selected operational area managers identify important assets, perceived threats, security requirements, current security practices, and organizational vulnerabilities.
- Process 3: Identify Staff Knowledge – Selected general and IT staff members identify important assets, perceived threats, security requirements, current security practices, and organizational vulnerabilities.
- Process 4: Create Threat Profiles – The analysis team analyzes the information from Processes 1 to 3, selects critical assets, refines the associated security requirements, and identifies threats to those assets, creating threat profiles.

**Phase 2: Identify Infrastructure Vulnerabilities** – This is an evaluation of the information infrastructure. The analysis team examines key operational components for weaknesses (technology vulnerabilities) that can lead to unauthorized action against critical assets. The processes of Phase 2 are

- Process 5: Identify Key Components – The analysis team identifies key IT systems and components for each critical asset. Specific instances are then selected for evaluation.
- Process 6: Evaluate Selected Components – The analysis team examines the key systems and components for technology weaknesses. Vulnerability tools (software, checklists, scripts) are used. The results are examined and summarized, looking for their relevance to the critical assets and their threat profiles.

**Phase 3: Develop Security Strategy and Plans** – During this part of the evaluation, the analysis team identifies risks to the organization's critical assets and decides what to do about them. The processes of Phase 3 are

- Process 7: Conduct Risk Analysis – The analysis team identifies the impact of threats to critical assets, creates criteria to evaluate the risks resulting from those threats, and evaluates the impacts based on those criteria. This produces a risk profile for each critical asset.
- Process 8: Develop Protection Strategy – The analysis team creates a protection strategy for organizational security improvement and mitigation plans to reduce the risks to critical assets based upon an analysis of the information gathered. Senior managers then review, refine, and approve the strategy and plans. Finally, the senior managers define the next steps that outline how the organization will build on the results of the evaluation and who will be responsible.

In the next section, we show how the OCTAVE attributes are implemented in the OCTAVE Method.

## B.2 Attributes and the OCTAVE Method

Recall that attributes are the distinctive qualities, or characteristics, of the evaluation. They define the basic elements of an information security risk evaluation from both the process and organizational perspectives. Table 5 shows how each attribute is reflected in the OCTAVE Method.

*Table 5: Mapping of Attributes to the OCTAVE Method*

| Mapping of Attributes to the OCTAVE Method | |
|---|---|
| **Attribute** | **Implementation in the OCTAVE Method** |
| RA.1 Analysis Team | An interdisciplinary analysis team consisting of personnel from the business units and the information technology department leads the OCTAVE Method. |
| RA.2 Augmenting Analysis Team Skills | The activities for the OCTAVE Method are documented in the *OCTAVE Method Implementation Guide, V2.0.* Guidance about the types of skills required to conduct each process is provided. If an analysis team believes that it does not possess sufficient knowledge and skills to conduct a process, it must include supplementary personnel who possess the required knowledge and skills for that process. |
| RA.3 Catalog of Practices | The OCTAVE Method requires the organization's security practices to be evaluated against a defined catalog of practices. Worksheets that are consistent with the practices in the catalog must be used. |
| RA.4 Generic Threat Profile | The OCTAVE Method requires the threats to the organization's critical assets to be evaluated against a generic threat profile. Worksheets that are consistent with the threats in the generic threat profile must be used. |

*Table 5: Mapping of Attributes to the OCTAVE Method (cont.)*

| Attribute | Implementation in the OCTAVE Method |
|---|---|
| RA.5 Catalog of Vulnerabilities | The OCTAVE Method requires the organization's computing infrastructure to be evaluated against a defined catalog of vulnerabilities. The method requires the use of vulnerability evaluation tools that check for known technology vulnerabilities. |
| RA.6 Defined Evaluation Activities | The activities for the OCTAVE Method are documented in the *OCTAVE Method Implementation Guide, V2.0.* The following are included in the guide:<br>• guidance for setting the scope of the evaluation and for selecting participants<br>• guidance for conducting each process<br>• worksheets and templates for recording information gathered during each process<br>• catalogs of information required by the process |
| RA.7 Documented Evaluation Results | The OCTAVE Method requires the analysis team to document the results of the evaluation. |
| RA.8 Evaluation Scope | Guidance for setting the scope of the evaluation is provided in the Preparation Guidelines of the *OCTAVE Method Implementation Guide, V2.0.* |
| RA.9 Next Steps | The last activity in the OCTAVE Method requires senior managers to define actions to implement their organization's protection strategy and risk mitigation plans. The activity also requires the managers to assign responsibility for completing the actions. |
| RA.10 Focus on Risk | The OCTAVE Method is an information security risk evaluation. It addresses the three components of risk: assets, threats, and vulnerabilities. |

*Table 5: Mapping of Attributes to the OCTAVE Method (cont.)*

| Attribute | Implementation in the OCTAVE Method |
|---|---|
| RA.11 Focused Activities | Each process of the OCTAVE Method is focused on identifying and analyzing the most important information security issues to the organization. For example:<br>• In Processes 1-3, the facilitators focus the activities using assets believed to be most important by the participants.<br>• In Process 4, the analysis team focuses its analysis activities using the critical assets that it selects.<br>• In Phase 2, the analysis team sets the scope of the infrastructure vulnerability evaluation using the organization's critical assets and the threats to those assets.<br>• In Phase 3, the analysis team establishes risk priorities based on the organizational impact of risks. |
| RA.12 Organizational and Technological Issues | The OCTAVE Method is focused on both organizational and technological issues. Phase 1 is an organizational evaluation where people from across the organization identify organizational information. Phase 2 is an evaluation of the information technology infrastructure, resulting in the identification of technological issues. The organizational and technological data are then analyzed during Phase 3. |
| RA.13 Business and Information Technology Participation | An interdisciplinary analysis team that includes representatives from operational areas and the information technology department lead the evaluation. Personnel from both the business units and the information technology department (including representation from multiple organizational levels) of the organization participate in Processes 1-3. |
| RA.14 Senior Management Participation | In the OCTAVE Method, senior managers are required to participate in Process 1, where the managers contribute their perspectives about what assets are important to them and how well those assets are being protected. The senior managers also participate in Process 8, where they review, refine, and approve the protection strategy and mitigation plans. In that workshop, they also define the next steps for implementing the strategy and plans. |
| RA.15 Collaborative Approach | The OCTAVE Method consists of a progressive series of workshops. Each workshop requires interaction among the people who participate in that workshop. |

In the next section, we focus on how the outputs map to the OCTAVE Method.

## B.3 Outputs and the OCTAVE Method

Outputs are the required results of the evaluation. They define the results that an analysis team must achieve during the evaluation. Table 6 shows where in the OCTAVE Method each output is generated.

*Table 6: Mapping of Outputs to the OCTAVE Method*

| Mapping of Outputs to the OCTAVE Method | |
|---|---|
| **Output** | **Implementation in the OCTAVE Method** |
| RO1.1 Critical Assets | During *Processes 1-3*, staff members from across the organization contribute their perspectives about which assets are important for completing their jobs. In *Process 4*, the analysis team selects the assets that are most critical to the organization. |
| RO1.2 Security Requirements for Critical Assets | During *Processes 1-3*, staff members from across the organization define security requirements for their important assets. The analysis team uses this information during *Process 4* to describe the security requirements for the organization's critical assets. |
| RO1.3 Threats to Critical Assets | During *Processes 1-3*, staff members from across the organization identify scenarios that threaten their most important assets. The analysis team uses the areas of concern as input when it creates a threat profile for each critical asset during *Process 4*. |
| RO1.4 Current Security Practices | During *Processes 1-3*, staff members from across the organization contribute their perspectives about which security practices are currently being used by the organization. The participants fill out surveys and talk about key issues during a follow-on discussion. During *Process 8*, the analysis team consolidates security practices identified during the first three processes. |
| RO1.5 Current Organizational Vulnerabilities | During *Processes 1-3*, staff members from across the organization contribute their perspectives about missing or inadequate practices in the organization (organizational vulnerabilities). These are identified in conjunction with security practices using surveys and follow-on discussions. During *Process 8*, the analysis team consolidates organizational vulnerabilities identified during the first three processes. |
| RO2.1 Key Components | During *Process 5*, the analysis team identifies key components of the computing infrastructure. The team members use the critical assets and the threats to the critical assets to focus their selection of components to evaluate for technology vulnerabilities. |

*Table 6: Mapping of Outputs to the OCTAVE Method (cont.)*

| Output | Implementation in the OCTAVE Method |
|---|---|
| RO2.2 Technology Vulnerabilities | During *Process 6*, the analysis team evaluates each key component from Process 5 using vulnerability evaluation tools. The team interprets data generated by the tools, identifying the technological weaknesses (technology vulnerabilities) present in each component. |
| RO3.1 Risks to Critical Assets | During *Process 7*, the analysis team identifies potential impacts on the organization for the threats to critical assets, resulting in explicit statements of risk. |
| RO3.2 Risk Measures | During *Process 7*, the analysis team evaluates the impacts of risks based on a set of qualitative measures (high, medium, low). Probability is viewed as optional in the OCTAVE Method. |
| RO3.3 Protection Strategy | During *Process 8*, the analysis team creates a protection strategy for organizational security improvement. The team bases the strategy on the organizational and technological information that it identified throughout the OCTAVE Method. |
| RO3.4 Risk Mitigation Plans | During *Process 8*, the analysis team creates risk mitigation plans to reduce the risks to the organization's most critical assets. The team selects mitigation actions based on the organizational and technological information that it identified throughout the evaluation process. |

# Glossary

| | |
|---|---|
| **Access** | a property of threat that defines how a threat actor accesses an asset (network access, physical access). This applies only to human actors. |
| **Access path** | ways in which information or services can be accessed via an organization's network |
| **Action list** | actions that people in an organization can take in the near term without the need for specialized training, policy changes, etc. It is essentially a list of near-term action items. |
| **Activity** | the actual operations that are performed during the evaluation |
| **Actor** | a property of threat that defines who or what may violate the security requirements (confidentiality, integrity, availability) of an asset |
| **Analysis team** | an interdisciplinary team comprising representatives of both the mission-related and information technology areas of the organization. The analysis team conducts the evaluation and analyzes the information. The analysis team consists of about three to five people, depending on the size of the overall organization and the scope of the evaluation. |
| **Area of concern** | a situation or scenario where someone is concerned about a threat to important assets. Typically, areas of concern have a source and an outcome – a causal action that has an effect on the organization. |

| | |
|---|---|
| **Asset** | something of value to the organization. Information technology assets are the combination of logical and physical assets and are grouped into specific classes (information, systems, software, hardware, people). |
| **Attributes** | the distinctive qualities of the evaluation. Attributes are the requirements that define the basic elements of the OCTAVE approach and define what is necessary to make the evaluation a success from both the process and organizational perspectives. The attributes define the process and organizational requirements for the evaluation, creating the environment in which the activities are performed. |
| **Availability** | when or how often an asset must be present or ready for use |
| **Catalog of practices** | a collection of good strategic and operational security practices that an organization can use to manage its security |
| **Catalog of vulnerabilities** | a collection of vulnerabilities based on platform and application. It is used to evaluate an organization's computing infrastructure for technology vulnerabilities. |
| **Checklist** | a vulnerability evaluation tool that provides the same functionality as automated tools. However, because checklists are manual, not automated, they require a consistent review of the items being checked and must be routinely updated. |
| **Computer prioritization listings** | a listing of the computer inventory owned by an organization. This listing typically depicts a prioritized ordering of systems or networking components based on their importance to the organization (e.g., mission critical systems, high/medium/low priority systems, administrative systems, support systems). |

| | |
|---|---|
| **Confidentiality** | the need to keep proprietary, sensitive, or personal information private and inaccessible to anyone who is not authorized to see it |
| **Configuration vulnerability** | a weakness resulting from an error in the configuration and administration of a system or component |
| **Critical assets** | the most important assets to an organization. The organization will suffer a large adverse impact if something happens to critical assets. |
| **Desktop workstation** | hosts on an organization's networks that staff members use to conduct business |
| **Design vulnerability** | a weakness inherent in the design or specification of hardware or software whereby even a perfect implementation will result in a vulnerability |
| **Destruction** | the removal of an asset from existence; the asset cannot be recovered |
| **Disclosure** | the viewing of confidential or proprietary information by someone who should not see the information |
| **Evaluation criteria** | a set of qualitative measures against which a risk is evaluated. Evaluation criteria define high, medium, and low impacts for an organization. |
| **Hardware asset** | information technology physical devices (workstations, servers, etc.) |
| **Home computer** | home personal computers that staff members use to access information remotely via an organization's networks |

| | |
|---|---|
| **Hybrid scanner** | a vulnerability evaluation tool that targets a range of services, applications, and operating system functions. Hybrid scanners may address Web servers (CGI, JAVA), database applications, registry information (e.g., Windows NT/2000), and weak password storage and authentication services. These are also known as specialty and targeted scanners. |
| **Implementation vulnerability** | a weakness resulting from an error made in the software or hardware implementation of a satisfactory design |
| **Impact** | the effect of a threat on an organization's mission and business objectives |
| **Impact value** | a qualitative measure of a risk's impact to the organization (high, medium, or low) |
| **Information asset** | documented (paper or electronic) data or intellectual property that is used to meet the mission of the organization |
| **Integrity** | the authenticity, accuracy, and completeness of an asset |
| **Interruption** | the limiting of an asset's availability; interruption refers mainly to services. |
| **Key classes of components** | types of devices that are important in processing, storing, or transmitting critical information. They represent related assets to critical assets. |
| **Laptop** | portable personal computers that staff members use to access information remotely via an organization's networks |
| **Loss** | the limiting of an asset's availability; the asset still exists but is temporarily unavailable. |

| | |
|---|---|
| **Modification** | an unauthorized changing of an asset |
| **Motive** | a property of threat that defines whether an actor's intentions are deliberate or accidental. This applies only to human actors. Motive is also sometimes referred to as the objective of a threat actor. |
| **Networking component** | devices important to an organization's networks. Routers, switches, and modems are all examples of this class of component. |
| **Network infrastructure scanner** | a vulnerability evaluation tool that focuses on the components of the network infrastructure, such as routers and intelligent switches, DNS (domain name system) servers, firewall systems, and intrusion detection systems |
| **Network mapping tools** | software used to search a network, identifying the physical connectivity of systems and networking components. The software also displays detailed information about the interconnectivity of networks and devices (routers, switches, bridges, hosts). |
| **Network topology diagrams** | electronic or paper documents used to display the logical or physical mapping of a network. These documents identify the connectivity of systems and networking components. They usually contain less detail than network mapping tools provide. |
| **Operating system scanner** | a vulnerability evaluation tool that targets specific operating systems (OS) such as Windows NT/2000, Sun Solaris, Red Hat Linux, or Apple Mac OS |
| **Operational practices** | security practices that focus on technology-related issues. They include issues related to how people use, interact with, and protect technology. |
| **Organizational vulnerability** | a weakness in organizational policy or practice that can result in unauthorized actions occurring. They are indications of missing or inadequate security practices. |

| | |
|---|---|
| **Outcome** | a property of threat that defines the immediate outcome (disclosure, modification, destruction, loss, interruption) of violating the security requirements of an asset |
| **People asset** | the people in the organization, including their skills, training, knowledge, and experience |
| **Principles** | the fundamental concepts driving the nature of the evaluation. Principles define the philosophy that shapes the evaluation process. |
| **Protection strategy** | the strategy that an organization uses to enable, initiate, implement, and maintain its internal security. It tends to incorporate long-term organization-wide initiatives. |
| **Protection strategy practice** | action that helps initiate, implement, and maintain security within an organization. A protection strategy practice is also called a security practice. |
| **Risk** | the possibility of suffering harm or loss. It is the potential for realizing unwanted negative consequences of an event. Risk refers to a situation where a person could do something undesirable or a natural occurrence could cause an undesirable outcome, resulting in a negative impact or consequence. |
| **Risk management** | the ongoing process of identifying risks and implementing plans to address them |
| **Risk mitigation plan** | a plan that is intended to reduce the risks to a critical asset. Risk mitigation plans tend to incorporate actions, or countermeasures, designed to counter the threats to the assets. |
| **Risk profile** | the range of risks that can affect an asset. Risk profiles contain categories that are grouped according to threat source (human actors using network access, human actors using physical access, system problems, other problems). |

| | |
|---|---|
| **Script** | a vulnerability evaluation tool that provides the same functionality as automated tools. Scripts usually have a singular function. If a large number of items are being evaluated, a corresponding number of scripts will be required. Scripts require a consistent review of the items being checked and must be routinely updated. |
| **Security component** | device that has security as its primary function. A firewall is an example of a security component. |
| **Security practices** | actions that help initiate, implement, and maintain security within an organization. A security practice is also called a protection strategy practice. |
| **Security requirements** | requirements outlining the qualities of information assets that are important to an organization. Typical security requirements are confidentiality, integrity, and availability. |
| **Server** | hosts within the information technology infrastructure that provide information technology services to an organization |
| **Software asset** | software applications and services (operating systems, database applications, networking software, office applications, custom applications, etc.) |
| **Storage device** | devices where information is stored, often for backup purposes |
| **Strategic practices** | security practices that focus on organizational issues at the policy level. They include business-related issues as well as issues that require organization-wide plans and participation. |
| **System** | a logical grouping of components designed to perform a defined function(s) or meet a defined objective(s) |

| | |
|---|---|
| **System of interest** | the system that is most closely linked to the critical asset |
| **Systems asset** | information systems that process and store information |
| **Technology vulnerability** | a weakness in systems that can directly lead to unauthorized action. Technology vulnerabilities are present in and apply to network services, architecture, operating systems, and applications. Types of technology vulnerabilities include design, implementation, and configuration vulnerabilities. |
| **Threat** | an indication of a potential undesirable event. A threat refers to a situation in which a person could do something undesirable (an attacker initiating a denial-of-service attack against an organization's email server) or a natural occurrence could cause an undesirable outcome (a fire damaging an organization's information technology hardware). Threats have defined properties (asset, actor, motive, access, outcome). |
| **Threat profile** | the range of threats that can affect an asset. Threat profiles contain categories that are grouped according to threat source (human actors using network access, human actors using physical access, system problems, other problems). |
| **Vulnerability** | a weakness in an information system, system security practices and procedures, administrative controls, internal controls, implementation, or physical layout that could be exploited by a threat to gain unauthorized access to information or disrupt processing. There are two basic types of vulnerabilities (organizational and technology). |
| **Vulnerability evaluation approach** | an approach for evaluating each infrastructure component, including who will perform the evaluation and the selected tool(s) |

| | |
|---|---|
| **Vulnerability summary** | a summary of the technology vulnerabilities for each component that is evaluated. A vulnerability summary includes the types of technology vulnerabilities found, when they need to be addressed, their potential effect on the critical assets, and how they can be addressed. |
| **Wireless components** | devices, such as cell phones and wireless access points, that staff members may use to access information (for example, email) |

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. AGENCY USE ONLY | 2. REPORT DATE | 3. REPORT TYPE AND DATES COVERED |
|---|---|---|
| (Leave Blank) | December 2001 | Final |

| 4. TITLE AND SUBTITLE | 5. FUNDING NUMBERS |
|---|---|
| OCTAVE[SM] Criteria, Version 2.0 | F19628-00-C-0003 |

6. AUTHOR(S)

Christopher J. Alberts, Audrey J. Dorofee

| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) | 8. PERFORMING ORGANIZATION REPORT NUMBER |
|---|---|
| Software Engineering Institute<br>Carnegie Mellon University<br>Pittsburgh, PA 15213 | CMU/SEI-2001-TR-016 |

| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSORING/MONITORING AGENCY REPORT NUMBER |
|---|---|
| HQ ESC/XPK<br>5 Eglin Street<br>Hanscom AFB, MA 01731-2116 | ESC-TR-2001-016 |

11. SUPPLEMENTARY NOTES

| 12A DISTRIBUTION/AVAILABILITY STATEMENT | 12B DISTRIBUTION CODE |
|---|---|
| Unclassified/Unlimited, DTIC, NTIS | |

13. ABSTRACT (MAXIMUM 200 WORDS)

Today, we rely on access to digital data that are accessible, dependable, and protected from misuse. Unfortunately, this need for accessible data also exposes organizations to a variety of new threats that can affect their information. The Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE[SM]) enables organizations to understand and address their information security risks. OCTAVE is led by a small, interdisciplinary team of an organization's personnel and focuses on an organization's assets and the risks to those assets. It is a comprehensive, systematic, context-driven, and self-directed evaluation approach. The essential elements of the OCTAVE approach are embodied in a set of criteria that define the requirements for OCTAVE. This report describes the OCTAVE criteria. The goal of this report is to define a general approach for evaluating and managing information security risks. Organizations can then develop methods that are consistent with the OCTAVE criteria.

| 14. SUBJECT TERMS | 15. NUMBER OF PAGES |
|---|---|
| information security; information security risk; information security risk evaluation; OCTAVE[SM]; Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] | 138 |

16. PRICE CODE

| 17. SECURITY CLASSIFICATION OF REPORT | 18. SECURITY CLASSIFICATION OF THIS PAGE | 19. SECURITY CLASSIFICATION OF ABSTRACT | 20. LIMITATION OF ABSTRACT |
|---|---|---|---|
| Unclassified | Unclassified | Unclassified | UL |