Introduction to the OCTAVE® Approach

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

August 2003

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
AUG 2003		**00-00-2003 to 00-00-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Introduction to the OCTAVE Approach	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**37**	

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

Introduction to the OCTAVE® Approach

Christopher Alberts
Audree Dorofee
James Stevens
Carol Woody

August 2003

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

Christos Scondras
Chief of Programs, XPK

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 252.227-7013.

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).

Table of Contents

List of Figures

List of Tables

1 Purpose and Scope

This document describes the Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE[®]), an approach for managing information security risks. It presents an overview of the OCTAVE approach and briefly describes two OCTAVE-consistent methods developed at the Software Engineering Institute (SEI).

The overall approach embodied in OCTAVE is described first, followed by a general description of the two methods: the OCTAVE Method for large organizations and OCTAVE-S[1] for small organizations. Information is provided to assist the reader in differentiating between the two methods, including characteristics defining the target organization for each method as well as any constraints and limitations of each method. A series of questions is also provided to help readers determine which method is best for them. Readers are then directed to the appropriate Web site to download the method of their choice.

It should be noted that some organizations may need a hybrid or a combination of the two methods, or a completely different version of OCTAVE. A final chapter discusses some of the possible alternate versions.

® OCTAVE is registered in the United States Patent and Trademark Office by Carnegie Mellon University.

SM Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University.

1 This paper is based on Version 2.0 of the OCTAVE Method and OCTAVE Criteria and the preliminary or beta version (Version 0.9) of OCTAVE-S. OCTAVE-S is not as extensively documented as the OCTAVE Method. Only the minimal set of materials needed to perform OCTAVE-S is provided in Version 0.9. Additional materials will be developed and provided with OCTAVE-S Version 1.0 at a later date.

2 What Is the OCTAVE Approach?

2.1 Overview

An effective information security risk evaluation considers both organizational and technological issues, examining how people use their organization's computing infrastructure on a daily basis. The evaluation is vitally important to any security-improvement initiative, because it generates an organization-wide view of information security risks, providing a baseline for improvement.

2.2 What Is OCTAVE?

For an organization looking to understand its information security needs, OCTAVE is a risk-based strategic assessment and planning technique for security. OCTAVE is self-directed, meaning that people from an organization assume responsibility for setting the organization's security strategy. The technique leverages people's knowledge of their organization's security-related practices and processes to capture the current state of security practice within the organization. Risks to the most critical assets are used to prioritize areas of improvement and set the security strategy for the organization.

Unlike the typical technology-focused assessment, which is targeted at technological risk and focused on tactical issues, OCTAVE is targeted at organizational risk and focused on strategic, practice-related issues. It is a flexible evaluation that can be tailored for most organizations. When applying OCTAVE, a small team of people from the operational (or business) units and the information technology (IT) department work together to address the security needs of the organization, balancing the three key aspects illustrated in Figure 1: operational risk, security practices, and technology.

The OCTAVE approach is driven by two of the aspects: operational risk and security practices. Technology is examined only in relation to security practices, enabling an organization to refine the view of its current security practices. By using the OCTAVE approach, an organization makes information-protection decisions based on risks to the confidentiality, integrity, and availability of critical information-related assets. All aspects of risk (assets, threats, vulnerabilities, and organizational impact) are factored into decision making, enabling an organization to match a practice-based protection *strategy* to its security risks. Table 1 summarizes key differences between OCTAVE and other evaluations.

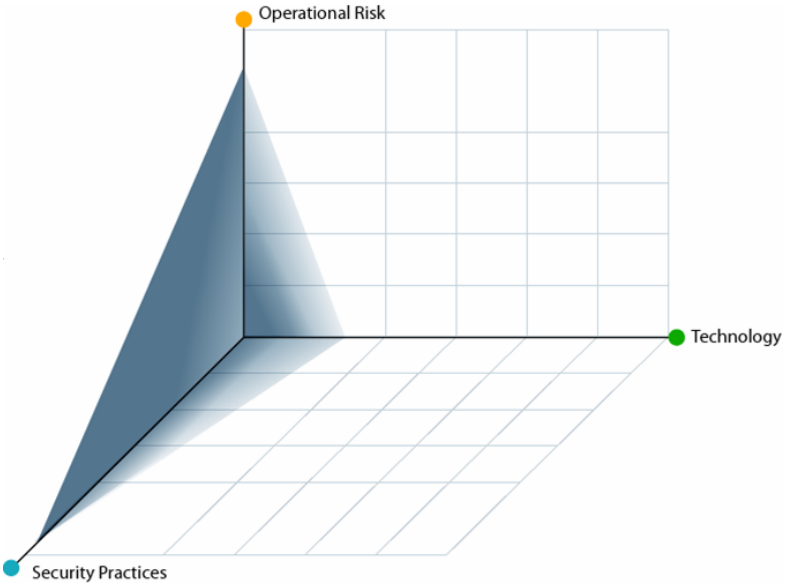

Figure 1: OCTAVE Balances Three Aspects

Table 1: Key Differences Between OCTAVE and Other Approaches

OCTAVE	**Other Evaluations**
Organization evaluation	System evaluation
Focus on security practices	Focus on technology
Strategic issues	Tactical issues
Self direction	Expert led

2.2.1 Key Characteristics of the OCTAVE Approach

OCTAVE is self directed, requiring an organization to manage the evaluation process and make information-protection decisions. An interdisciplinary team, called the analysis team, leads the evaluation. The team includes people from both the business units and the IT department, because both perspectives are important when characterizing the global, organizational view of information security risk.

OCTAVE is an asset-driven evaluation approach. Analysis teams

- 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
- consider the relationships among critical assets, the threats to those assets, and vulnerabilities (both organizational and technological) that can expose assets to threats

- evaluate risks in an operational context - how they are used to conduct an organization's business and how those assets are at risk due to security threats
- create a practice-based protection strategy for organizational improvement as well as risk mitigation plans to reduce the risk to the organization's critical assets

The organizational, technological, and analysis aspects of an information security risk evaluation are complemented by a three-phased approach. OCTAVE is organized around these three basic aspects (illustrated in Figure 2), enabling organizational personnel to assemble a comprehensive picture of the organization's information security needs. The phases are

- *Phase 1: Build Asset-Based Threat Profiles* – This is an organizational evaluation. The analysis team determines what is important to the organization (information-related assets) and what is currently being done to protect those assets. The team then selects those assets that are most important to the organization (critical assets) and describes security requirements for each critical asset. Finally, it identifies threats to each critical asset, creating a threat profile for that asset.
- *Phase 2: Identify Infrastructure Vulnerabilities* – This is an evaluation of the information infrastructure. The analysis team examines network access paths, identifying classes of information technology components related to each critical asset. The team then determines the extent to which each class of component is resistant to network attacks.
- *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.

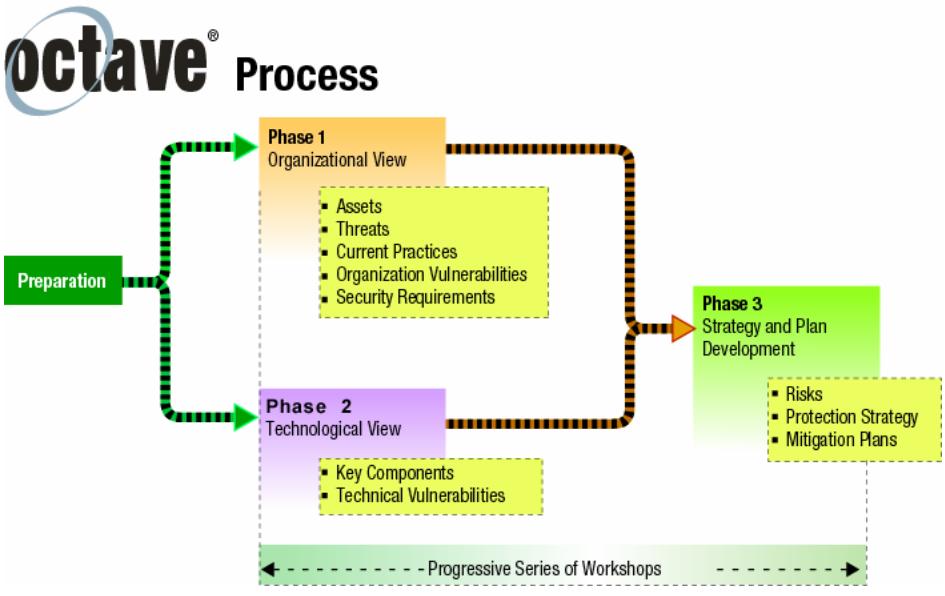

Figure 2: OCTAVE Phases

2.3 OCTAVE Criteria

The essential elements, or requirements, of the OCTAVE approach are embodied in a set of criteria [Alberts 01b]. There can be many methods consistent with these criteria, but there is only one set of OCTAVE criteria. At this point, two methods consistent with the criteria have been developed. The OCTAVE Method, documented in the *OCTAVE Method Implementation Guide, v2.0* [Alberts 01a], was designed with large organizations in mind, while OCTAVE-S was developed for small organizations. In addition, others might define methods for specific contexts that are consistent with the criteria. Figure 3 illustrates these points.

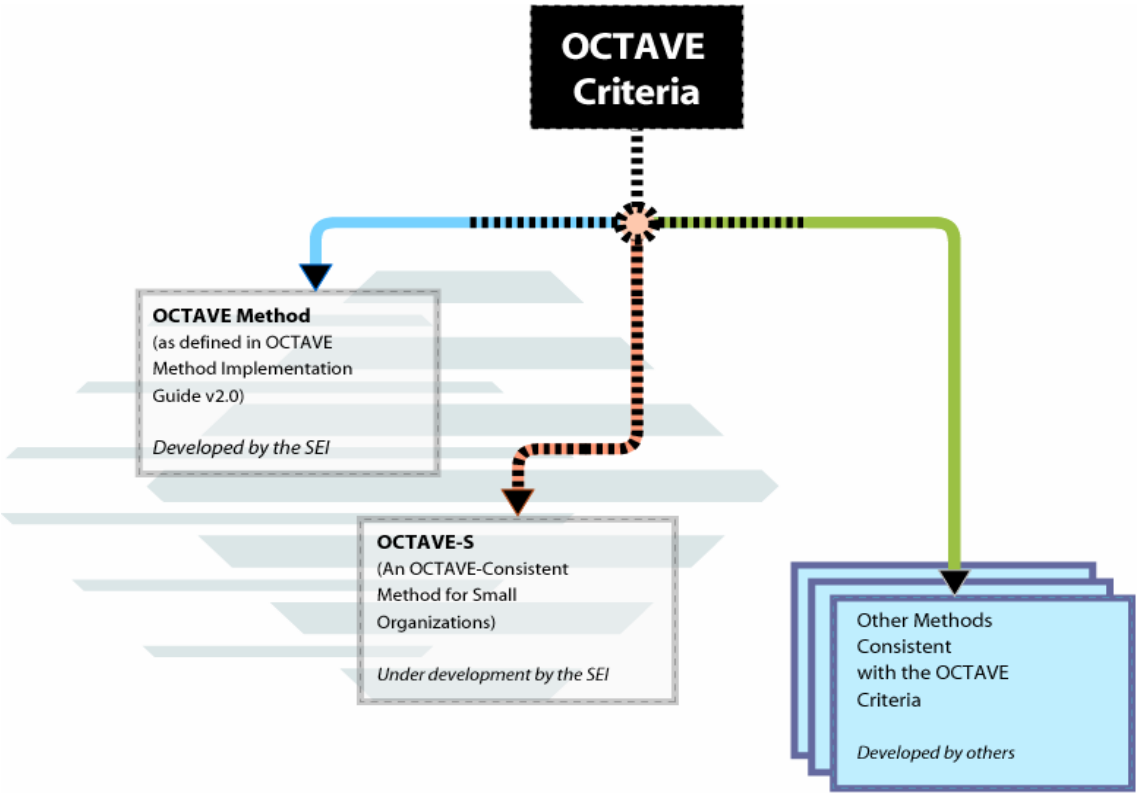

Figure 3: The OCTAVE Criteria Support Multiple Implementations

The OCTAVE criteria are a set of principles, attributes, and outputs. Principles are the fundamental concepts driving the nature of the evaluation, and defining the philosophy behind the evaluation process. They shape the evaluation approach and provide the basis for 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. There is more than one set of activities that can produce the outputs of OCTAVE; for this reason, a unique set of activities is not specified. The outputs define the outcomes that an analysis team must achieve during the evaluation and are organized according to the three phases. Tables 2 and 3 list the principles, activities, and outputs of the OCTAVE approach.

Table 2: OCTAVE Principles and 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

Principle	Attribute
Teamwork	RA.1 Analysis Team RA.2 Augment Analysis Team Skills RA.13 Business and Information Technology Participation RA.15 Collaborative Approach

Table 3: OCTAVE Outputs

Phase	Output
Phase 1	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
Phase 2	RO2.1 Key Components RO2.2 Current Technology Vulnerabilities
Phase 3	RO3.1 Risks to Critical Assets RO3.2 Risk Measures RO3.3 Protection Strategy RO3.4 Risk Mitigation Plans

2.4 OCTAVE Is Part of a Continuum

OCTAVE creates an organization-wide view of the current information security risks, providing 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 the organization's critical assets

An organization will not improve unless it implements its plans. The following 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

An information security risk evaluation is part of an organization's activities for managing information security risks. OCTAVE is an evaluation activity, not a continuous process. Thus, it has a defined beginning and end. Figure 4 shows the relationship among these activities and where OCTAVE fits in. Note that risk management activities define a *plan-do-check-act* cycle.

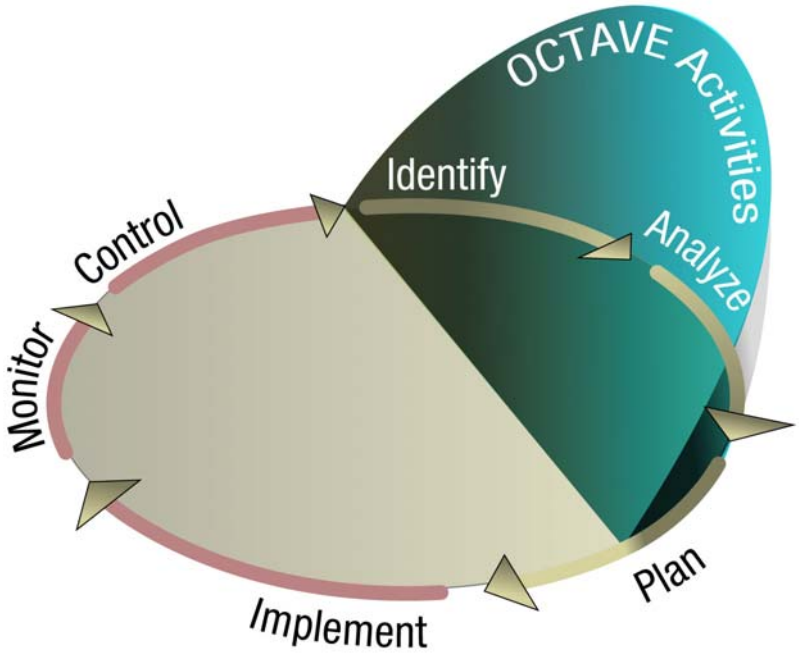

Figure 4: OCTAVE and Risk Management Activities

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). Between evaluations, an organization can periodically identify new risks, analyze these risks in relation to existing risks, and develop mitigation plans for them.

3 OCTAVE Method

The OCTAVE Method was developed with large organizations in mind (e.g., 300 employees or more). Size is not the only consideration when deciding to use the OCTAVE Method. Large organizations generally have a multi-layered hierarchy and are often stove-piped (disjoint) or geographically distributed. Formal data-gathering activities to determine what information-related assets are important, how they are used, and how they are threatened become an essential part of conducting OCTAVE in large organizations. Finally, a large organization is likely to maintain its own computing infrastructure and have the internal ability to run vulnerability evaluation tools and interpret the results in relation to its critical assets. This section introduces the OCTAVE Method. The materials that are available to conduct the OCTAVE Method are also described.

3.1 OCTAVE Method Processes

The OCTAVE Method comprises the three phases required by the OCTAVE criteria. The processes in those phases are described below:

- Phase 1: Build Asset-Based Threat Profiles – The two major functions of this phase are gathering information from across the organization and defining threat profiles for critical assets.
  - Process 1: Identify Senior Management Knowledge – The analysis team collects information about important assets, security requirements, threats, and current organizational strengths and vulnerabilities from a representative set of senior managers.
  - Process 2: Identify Operational Area Knowledge – The analysis team collects information about important assets, security requirements, threats, and current organizational strengths and vulnerabilities from managers of selected operational areas.
  - Process 3: Identify Staff Knowledge– The analysis team collects information about important assets, security requirements, threats, and current organizational strengths and vulnerabilities from general staff and IT staff members of the selected operational areas.
  - Process 4: Create Threat Profiles – The analysis team selects three to five critical information-related assets and defines the threat profiles for those assets.
- Phase 2: Identify Infrastructure Vulnerabilities – During this phase, the analysis team evaluates key components of systems supporting the critical assets for technological vulnerabilities.

  - Process 5: Identify Key Components – A representative set of key components from the systems that support or process the critical information-related assets are identified, and an approach for evaluating them is defined.
  - Process 6: Evaluate Selected Components – Tools are run to evaluate the selected components, and the results are analyzed to refine the threat profiles (for network-access threats) for the critical assets.
- Phase 3: Develop Security Strategy and Plans – The primary purpose of this phase is to evaluate risks to critical assets and develop an organizational protection strategy and risk mitigation plans.
  - Process 7: Conduct Risk Analysis – An organizational set of impact evaluation criteria are defined to establish a common basis for determining the impact value (high, medium, or low) due to threats to critical assets. All active risks are evaluated for impact. Note that probability is not currently included but can be added to this method.[2]
  - Process 8: Develop Protection Strategy – The team develops an organization-wide protection strategy focused on improving the organization's security practices as well as mitigation plans to reduce the important risks to critical assets.

3.2 Available Materials Supporting the OCTAVE Method

The OCTAVE Method is documented in the *OCTAVE Method Implementation Guide* (OMIG), available for downloading from the following web site <http://www.cert.org/octave> Web site. This guide contains 18 volumes of information in both Microsoft Word and PowerPoint. The following list briefly describes the contents of each volume (from Volume 1 of the OMIG).

- *Volume 1: Introduction*: This volume includes a description of OCTAVE, guidance on how to use the guide, some suggestions relative to analysis team training, and a feedback form.
- *Volume 2: Preliminary Activities*: This volume contains guidelines for preparing to do an OCTAVE, including selecting the analysis team and participants, scheduling, and logistics. Also in this volume you will find high-level tailoring guidance, and briefings for senior managers and participants.
- *Volumes 3 – 12: The OCTAVE Process*: These volumes provide a complete set of information for the three phases and eight processes of the OCTAVE Method.
- *Volume 13: After the Evaluation*: This is a short section providing guidance and an example of what to do after the evaluation is over.

[2] OCTAVE-S has a qualitative version of probability that can be integrated into the OCTAVE Method, if desired. Future revisions to the OCTAVE Method will likely contain some form of optional, qualitative probability estimation.

- *Volume 14: Bibliography and Glossary*: This provides a long, but not exhaustive, list of references, Web sites, and other sources of information relative to information security, practices, and standards. A glossary provides definitions for the key terms used throughout the guide.
- *Volume 15: Appendix A: OCTAVE Catalog of Practices*: This volume provides a set of good information security practices against which an organization evaluates itself during the OCTAVE Method.
- *Volume 16: Appendix B: OCTAVE Data Flow*: This volume contains a data flow diagram showing, in concise format, all of the activities, inputs, outputs, and worksheets in the OCTAVE Method.
- *Volume 17: Appendix C: Complete Example Results*: This provides the complete set of example results (which are also found in smaller pieces throughout the guide).
- *Volume 18: Appendices D and E: White Papers*: Two papers, *Overview of the OCTAVE Method* and *OCTAVE Threat Profiles*, are provided in this volume.

In addition to the no-cost download, a paper version and/or CD-ROM version of the OMIG can also be purchased. Refer to the <http://www.cert.org/octave> Web site for additional information.

4 OCTAVE-S

Note: This section is based on the preliminary or beta version (Version 0.9) of OCTAVE-S. Additional materials will be developed and provided with Version 1.0 at a later date. OCTAVE-S is not as extensively documented as the OCTAVE Method. The minimal set of materials needed to perform OCTAVE-S is provided in the beta version.

OCTAVE-S was developed and tested for small organizations, ranging from 20 to 80 people. It is designed for organizations that can empower a team of three to five people to conduct all evaluation activities, without the need for formal data-gathering activities. For example, a 200-person company that has a single location might be able to assemble a team of 5 people that has sufficient insight into the entire organization. On the other hand, a company with 90 people at multiple sites, with an extremely stove piped structure of 9 divisions may require the OCTAVE Method to ensure that sufficient data are gathered from across the organization.

Another defining difference in OCTAVE-S relates to the Phase 2 evaluation of the computing infrastructure. Small organizations often outsource, in part or in total, the maintenance of their computer systems. For these companies, running evaluation tools and making sense out of the results would be a significant burden on their resources. OCTAVE-S may identify the need for this type of analysis, but Phase 2 in OCTAVE-S is an abbreviated inspection and review of the processes used to secure the organization's computing infrastructure.

OCTAVE-S also includes an optional, qualitative version of probability. It requires some knowledge of an actor's motivation (when appropriate) as well as some history of previous security incidents and problems. While it is optional, organizations may be interested to see what types of data they should be collecting to establish a reasonably confident measure of probability for information security risks.

4.1 OCTAVE-S Processes

OCTAVE-S has the same three phases described in the OCTAVE approach and in the OCTAVE Method. However, the processes are somewhat different from the OCTAVE Method.

- Phase 1: Build Asset-Based Threat Profiles – During this phase, organizational information is identified and used to define threat profiles for three to five critical information-related assets.

  - Process S1: Identify Organizational Information – The analysis team identifies the organization's important information-related assets, defines a set of impact evaluation criteria, and defines the current state of the organization's security practices.
  - Process S2: Create Threat Profiles – The analysis team selects three to five critical information-related assets and defines the security requirements and threat profiles for those assets.
- Phase 2: Identify Infrastructure Vulnerabilities – During this phase, the analysis team takes a high-level review of their infrastructure and technology-related practices to refine the threat profiles.
  - Process S3: Examine the Computing Infrastructure in Relation to Critical Assets – The analysis team analyzes the access paths in the systems that support the critical assets and determines how well their technology-related processes are protecting those assets.
- Phase 3: Develop Security Strategy and Plans – During this phase, the risks to critical assets are evaluated and an organizational protection strategy and risk mitigation plans are defined.
  - Process S4: Identify and Analyze Risks – The analysis team evaluates all active risks for impact and, optionally, probability.
  - Process S5: Develop Protection Strategy and Mitigation Plans – The team develops an organization-wide protection strategy and risk mitigation plans based on security practices.

4.2 Available OCTAVE-S Materials

The OCTAVE Method is documented in the *OCTAVE-S Implementation Guide*, available for downloading from the following web site: <http://www.cert.org/octave>. This guide contains 10 volumes of information in both Microsoft Word and PowerPoint. The following list briefly describes the contents of each volume.

- *Volume 1: Introduction to OCTAVE-S* – This volume provides a basic description of OCTAVE-S and advice on how to use the guide.
- *Volume 2: Preparation Guidelines* – This volume contains background and guidance for preparing to conduct an OCTAVE-S evaluation.
- *Volume 3: Method Guidelines* – This volume includes detailed guidance for each OCTAVE-S activity.
- *Volume 4: Organizational Worksheets* – This volume contains worksheets for all organizational-level information that is gathered and analyzed during OCTAVE-S.
- *Volume 5: Critical Asset Worksheets for Information* – This volume provides worksheets to document data related to critical assets categorized as information.

- *Volume 6: Critical Asset Worksheets for Systems* – This volume provides worksheets to document data related to critical assets categorized as systems.
- *Volume 7: Critical Asset Worksheets for Applications* – This volume provides worksheets to document data related to critical assets categorized as applications.
- *Volume 8: Critical Asset Worksheets for People* – This volume provides worksheets to document data related to critical assets categorized as people.
- *Volume 9: Strategy and Plans Worksheets* – This volume contains worksheets to record the current and desired protection strategy and the risk mitigation plans.
- *Volume 10: Example Scenario* – This volume contains a detailed scenario illustrating a completed set of worksheets.

5 Choosing Between the Methods

The OCTAVE Method is structured for an analysis team with some understanding of IT and security issues, employing an open, brainstorming approach for gathering and analyzing information. On the other hand, OCTAVE-S is more structured. Security concepts are embedded in OCTAVE-S worksheets, allowing for their use by less experienced practitioners. Experienced teams may find OCTAVE-S too constraining, while inexperienced teams may become lost using the OCTAVE Method.

While only two methods have been developed by the SEI, some users may find that neither method is exactly what they need. Many methods that integrate pieces of the two methods for something that is "in-between" are possible. As long as the tailored methods still meet the OCTAVE criteria, they are still considered to be OCTAVE-consistent evaluations.

The following set of questions should be used to help you decide which method is best suited for your organization. These questions are guidelines only, not a black-and-white decision process. You may find that the results are not clear, in which case, both methods should be downloaded or obtained and reviewed in detail or pilot-tested for suitability. To use the table, consider each question. If your answer is *yes*, look to see which column is checked, the OCTAVE Method or OCTAVE-S.

Question	**OCTAVE Method**	**OCTAVE-S**
Size and complexity of the organization		
Is your organization small? Does your organization have a flat or simple hierarchical structure?		✓
Are you a large company (300 or more employees)? Do you have a complex structure or geographically-dispersed divisions?	✓	
Structured or Open-Ended Method		
Do you prefer a more structured method using fill-in-the-blanks, checklists, and redlines, but not as easy to tailor?		✓
Do you prefer a more open-ended methodology that is easy to tailor and adapt to your own preferences?	✓	

Question	OCTAVE Method	OCTAVE-S
Analysis team composition		
Can you find a group of three to five people for the analysis team who have a broad and deep understanding of the company and also possess most of the following skills? • problem-solving ability • analytical ability • ability to work in a team • at least one member with leadership skills • ability to spend a few days working on this method		✓
Can you find a group of 3-5 people for the analysis team who have some understanding of at least part of the company and also possess most of the following skills? • problem-solving ability • analytical ability • ability to work in a team • at least one member with leadership skills • at least one member who understands the computing infrastructure and how to run and interpret vulnerability tools • ability to spend a few weeks working on this method	✓	
IT resources		
Do you outsource all or most of your information technology functions?		✓
Do you have a relatively simple information technology infrastructure that is well understood by at least one individual in your organization?		✓
Do you manage your own computing infrastructure and are familiar with running vulnerability evaluation tools?	✓	
Do you have a complex computing infrastructure that is well understood by one or more individuals in your organization?	✓	
Are you able to run, comprehend, and interpret the results of vulnerability evaluation tools within the context of information-related assets (i.e., can you tell if a particular vulnerability means a particular asset is exposed to unwanted modification or destruction)? Are you able to use the expertise of a current service provider to interpret results?	✓	
Using a Beta-version method		
Are you willing to use a beta-version of a method (that is, use a method that may not have all the guidance you might need)?		✓

You may not get a consistently clear indication of which method to use. If that is the case, select the one that is closest to what you need. You may also want to look at the other method to determine if some degree of tailoring will make the selected method more suitable to your organization.

A word of caution: Some might consider it possible to use OCTAVE-S within individual projects, lines of business, or departments, and then roll the information up to get an organization-wide perspective in place of using the OCTAVE Method. While this approach is theoretically possible, there is no experience at this time defining how this would be accomplished.

6 Other Derivative Methods

The Software Engineering Institute has developed two methods that meet the OCTAVE criteria. Other organizations are developing their own unique versions of OCTAVE-consistent methods. These may be specific to a domain, such as the medical community, specific to a standard or practice such as the Health Insurance Portability and Accountability Act (HIPAA) or ISO[3] 17799, or they may incorporate additional proprietary tools and processes that expand the scope of OCTAVE.

To the extent that these other OCTAVE-consistent methods are freely available, they will be referenced on the OCTAVE Web site. Proprietary methods may be obtained only from the specific developing organization.

[3] International Organization for Standardization

7 Additional Information

7.1.1 OCTAVE Training

The three-day training workshop, *OCTAVE Training*, provides the basic training needed to conduct an OCTAVE evaluation, using either the OCTAVE Method or OCTAVE-S. Since the OCTAVE Method has a broader scope and more complex activities, it is used as the core of the course. The different aspects of OCTAVE-S are discussed and the method materials are reviewed to instruct students on the different implementation. While it is not required for everyone, this course is recommended for people wanting in-depth experience at conducting the various OCTAVE activities before they conduct one in their own organization.

A two-day train-the-trainer course is also provided for transition partners and others licensed to teach and conduct OCTAVE evaluations for their customers.

7.1.2 Book: *Managing Information Security Risks*

The materials available for downloading for the OCTAVE Method and OCTAVE-S are reference materials for use while conducting the evaluation. For easier understanding and reading, the Addison-Wesley book, *Managing Information Security Risks* [Alberts 02], provides a solid basis for understanding the OCTAVE approach and the OCTAVE Method, as well as several optional variations. The book can provide basic understanding for OCTAVE users who opt not to take training. It is also used as the core text during the training class.

References

[Alberts 01a] Alberts, Christopher and Dorofee, Audrey. *OCTAVE Method Implementation Guide v2.0*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001. <http://www.cert.org/octave>.

[Alberts 01b] Alberts, Christopher and Dorofee, Audrey. *OCTAVE Criteria v2.0*. (CMU/SEI-2001-TR-020, ADA 396654). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001. <http://www.sei.cmu.edu/publications/documents/01.reports/01tr020.html>.

[Alberts 02] Alberts, Christopher and Dorofee, Audrey. *Managing Information Security Risks*. Boston, MA: Addison-Wesley, 2002.