Carnegie Mellon
Software Engineering Institute

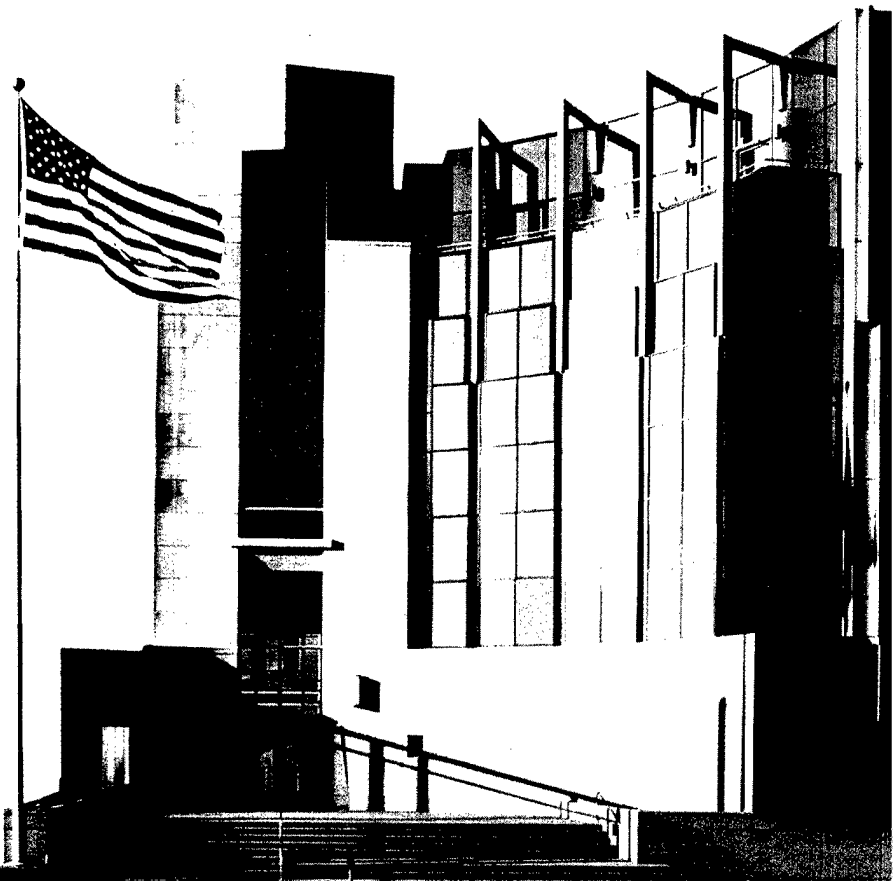
OCTAVE®-S Implementation Guide, Version 1.0

Volume 1: Introduction to OCTAVE-S

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

HANDBOOK
CMU/SEI-2003-HB-003



Carnegie Mellon
Software Engineering Institute
Pittsburgh, PA 15213-3890

OCTAVE®-S Implementation Guide, Version 1.0

Volume 1: Introduction to OCTAVE-S

CMU/SEI-2003-HB-003

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

Networked Systems Survivability Program

This report was prepared for the

SEI Joint Program Office
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

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

About This Document

This document is Volume 1 of the *OCTAVE-S Implementation Guide*, a 10-volume handbook supporting the OCTAVE-S methodology. This volume provides an overview of OCTAVE-S and is written for people who already have some familiarity with the basic concepts and principles of the OCTAVE approach.

The volumes in this handbook are

- ***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 Information Workbook* – This volume provides worksheets for all organizational-level information gathered and analyzed during OCTAVE-S.
- *Volume 5: Critical Asset Workbook for Information* – This volume provides worksheets to document data related to critical assets that are categorized as information.
- *Volume 6: Critical Asset Workbook for Systems* – This volume provides worksheets to document data related to critical assets that are categorized as systems.
- *Volume 7: Critical Asset Workbook for Applications* – This volume provides worksheets to document data related to critical assets that are categorized as applications.
- *Volume 8: Critical Asset Workbook for People* – This volume provides worksheets to document data related to critical assets that are categorized as people.
- *Volume 9: Strategy and Plan Workbook* – This volume provides worksheets to record the current and desired protection strategy and the risk mitigation plans.
- *Volume 10: Example Scenario* – This volume includes a detailed scenario illustrating a completed set of worksheets.

Acknowledgements

OCTAVE-S was developed under the Technology Insertion, Demonstration, and Evaluation (TIDE) program, managed for the Software Engineering Institute by John Foreman. The authors would like to thank all those who participated in the early OCTAVE-S pilots as well as all those who reviewed and provided input on the method.

Abstract

The Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE®) approach defines a risk-based strategic assessment and planning technique for security. OCTAVE is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organizations (less than 100 people). OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organization's personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization's unique operational security risks. To conduct OCTAVE-S effectively, the team must have broad knowledge of the organization's business and security processes, so it will be able to conduct all activities by itself.

1 Purpose and Scope

This document is the first volume of the *OCTAVE-S Implementation Guide*. In all, the guide contains 10 volumes of material supporting the Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE®)-S methodology, including background materials, guidance, worksheets, and a detailed example scenario. The purpose of this document is to

- provide readers with a basic understanding of the OCTAVE-S, v0.9, methodology
- assist readers in determining whether OCTAVE-S, v0.9, is appropriate for their organizations

OCTAVE-S and the OCTAVE Method are two methods developed at the Software Engineering Institute (SEI[SM]) consistent with the OCTAVE criteria, the essential requirements of an asset-based, strategic assessment of information security risk. The OCTAVE Method was developed first and applies to large, hierarchical organizations. Volume 1 of the *OCTAVE Method Implementation Guide* [Alberts 01a] provides an introduction to that method. OCTAVE-S was developed to meet the needs of smaller, less hierarchical organizations. The document *Introduction to the OCTAVE Approach* [Alberts 03] provides a more comprehensive overview of the OCTAVE approach and SEI's OCTAVE-consistent methodologies.

People unfamiliar with the OCTAVE approach should read the *Introduction to the OCTAVE Approach* before deciding which method is best suited to their organization. This version of the *OCTAVE-S Implementation Guide* is written for people who already have some familiarity with the basic concepts and principles of OCTAVE. For example, anyone already familiar with the OCTAVE Method will likely find OCTAVE-S to be relatively easy to understand and use, since both methods share a common basis.

Note that there are only very minor differences between OCTAVE-S v0.9 and v1.0. These consist primarily of editorial changes. There was one correction to Volumes 9 and 10, step 25, Collaborative Security Management, Staff Awareness. The last sentence had the phrase "contingency, disaster recovery, and business continuity plans" changed to "collaborative security management policies and procedures."

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

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

2 What Is OCTAVE-S?

This section provides an overview of OCTAVE-S, highlighting the basic process, outputs, and scope of application. However, before looking specifically at OCTAVE-S, a brief overview of the OCTAVE approach is provided for additional context.

2.1 Overview of the OCTAVE Approach

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 typical technology-focused assessments, which are 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.

2.2 Overview of OCTAVE-S

OCTAVE-S is a variation of the OCTAVE approach that was developed to meet the needs of small, less hierarchical organizations. It is tailored to the more limited means and unique constraints typically found in smaller organizations. Although the "look and feel" of OCTAVE-S

differs from than of the OCTAVE Method, the technique produces the same types of results, including an organization-wide protection strategy.

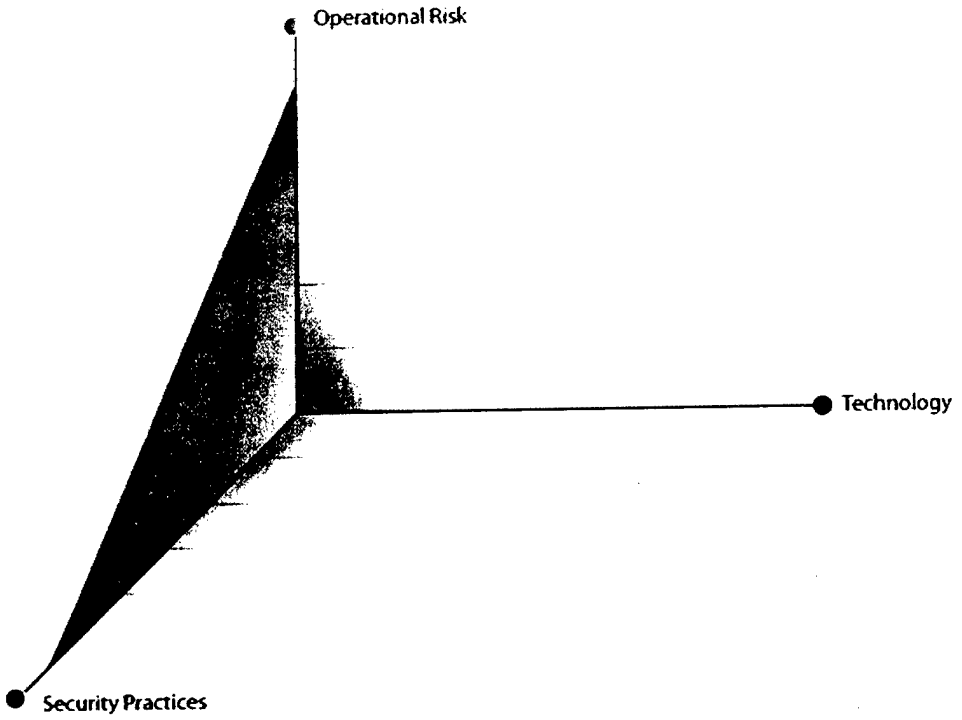


Figure 1: OCTAVE-S Emphasizes Operational Risk and Security Practices

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

Before attempting to use OCTAVE-S, you need to understand the following two unique aspects of the method:

1. A small interdisciplinary analysis team of three to five people leads OCTAVE-S. Collectively, analysis team members must have broad insight into the organization's business and security processes, sufficient to conduct all of the OCTAVE-S activities. For this reason, OCTAVE-S does not require formal data gathering workshops to kick-off the evaluation.

2. OCTAVE-S includes a limited exploration of the computing infrastructure during Phase 2. Since small organizations frequently outsource their IT services and functions, they typically have not developed organizational capabilities for running and interpreting the results of vulnerability evaluation tools. However, the lack of an organizational capability for running such tools does not preclude an organization from establishing a protection strategy. Rather than using vulnerability data to refine its view of its current security practices, an organization conducting an OCTAVE-S evaluation examines the processes employed to securely configure and maintain its computing infrastructure. Any deficiencies in organizational capability are noted and considered during Phase 3, when the organization develops its protection strategy.

2.3 OCTAVE-S Process

OCTAVE-S is a self-directed information security risk evaluation. It requires an analysis team to examine the security risks to an organization's critical assets in relation to its business objectives, ultimately yielding an organization-wide protection strategy and asset-based risk mitigation plans. By implementing the results of OCTAVE-S, an organization stands to better protect all information-related assets and improve its overall security posture.

OCTAVE-S is based upon the three phases described in the OCTAVE criteria [Alberts 01b], although the number and sequencing of activities differ from those used in the OCTAVE Method. This section provides a brief overview of the phases, processes, and activities of OCTAVE-S.

2.3.1 Phase 1: Build Asset-Based Threat Profiles

Phase 1 is an evaluation of organizational aspects. During this phase, the analysis team defines impact evaluation criteria that will be used later to evaluate risks. It also identifies important organizational assets and evaluates the security current practice of the organization. The team completes all tasks by itself, collecting additional information only when needed. It then selects three to five critical assets to analyze in depth based on relative importance to the organization. Finally, the team defines security requirements and defines a threat profile for each critical asset. Table 2 illustrates the processes and activities of Phase 1.

2.3.2 Phase 2: Identify Infrastructure Vulnerabilities

During this phase, the analysis team conducts a high-level review of the organization's computing infrastructure, focusing on the extent to which security is considered by maintainers of the infrastructure. The analysis team first analyzes how people use the computing infrastructure to access critical assets, yielding key classes of components as well as who is responsible for configuring and maintaining those components.

Table 2: Processes and Activities of Phase 1

Phase	Process	Activity
Phase 1: Build Asset-Based Threat Profiles	Process S1: Identify Organizational Information	S1.1 Establish Impact Evaluation Criteria
		S1.2 Identify Organizational Assets
		S1.3 Evaluate Organizational Security Practices
	Process S2: Create Threat Profiles	S2.1 Select Critical Assets
		S2.2 Identify Security Requirements for Critical Assets
		S2.3 Identify Threats to Critical Assets
		S3.2 Analyze Technology-Related Processes

The team then examines the extent to which each responsible party includes security in its information technology practices and processes. The processes and activities of Phase 2 are shown in Table 3.

Table 3: Processes and Activities of Phase 2

Phase	Process	Activity
Phase 2: Identify Infrastructure Vulnerabilities	Process S3: Examine Computing Infrastructure in Relation to Critical Assets	S3.1 Examine Access Paths
		S3.2 Analyze Technology-Related Processes

2.3.3 Phase 3: Develop Security Strategy and Plans

During Phase 3, the analysis team identifies risks to the organization's critical assets and decides what to do about them. Based on an analysis of the information gathered, the team creates a protection strategy for the organization and mitigation plans to address the risks to the critical assets. The OCTAVE-S worksheets used during Phase 3 are highly structured and tightly linked to the OCTAVE catalog of practices [Alberts 01c], enabling the team to relate its recommendations for improvement to an accepted benchmark of security practice. Table 4 depicts the processes and activities of Phase 3.

2.4 OCTAVE-S Outputs

Information security risk management requires a balance between reactive and proactive activities. During an OCTAVE-S evaluation, the analysis team views security from multiple perspectives, ensuring that recommendations achieve the proper balance based on the organization's needs.

Table 4: Processes and Activities of Phase 3

Phase	Process	Activity
Phase 3: Develop Security Strategy and Plans	Process S4: Identify and Analyze Risks	S4.1 Evaluate Impacts of Threats
		S4.2 Establish Probability Evaluation Criteria
		S4.3 Evaluate Probabilities of Threats
	Process S5: Develop Protection Strategy and Mitigation Plans	S5.1 Describe Current Protection Strategy
		S5.2 Select Mitigation Approaches
		S5.3 Develop Risk Mitigation Plans
		S5.4 Identify Changes to Protection Strategy
		S5.5 Identify Next Steps

When forming recommendations for improving the organization's security practices, the team assumes a proactive point of view, analyzing security issues from both an organization-wide perspective and an asset-specific perspective. At any time during the evaluation, a team might also take a more reactive stand by identifying actions items intended to address specific weaknesses. These action items are considered to be more reactive in nature because they often fill an immediate gap rather than improving the organization's security practices.

The main results of OCTAVE-S are thus three-tiered and include

- organization-wide protection strategy – The protection strategy outlines the organization's direction with respect to its information security practice.
- risk mitigation plans – These plans are intended to mitigate risks to critical assets by improving selected security practices.
- action list – These include short-term action items needed to address specific weaknesses.

Other useful outputs of OCTAVE-S include

- a listing of important information-related assets supporting the organization's business goals and objectives
- survey results showing the extent to which the organization is following good security practice
- a risk profile for each critical asset depicting a range of risks to that asset

Each phase of OCTAVE-S produces usable results, so even a partial evaluation will produce information useful for improving an organization's security posture.

2.5 Scope of Application

OCTAVE-S was developed and piloted with small organizations, ranging from 20 to 80 people in size. The pilot organizations shared a couple of common characteristics. First, their

organizational structures were relatively flat, and people from different organizational levels were accustomed to working with each other. Second, people were often required to multi-task, exposing staff members to the processes and procedures used across the organization. Thus, those organizations were able to assemble a team of three to five people that

- included people from multiple organizational levels, including senior management
- had broad knowledge of the organization's business and security processes

The breadth of an analysis team's knowledge, rather than size of an organization, becomes a key differentiator between OCTAVE-S and the OCTAVE Method. No matter the size of an organization, if it can assemble a team of three to five people who have broad insight into the organization's business and security processes, then the organization is potentially a good candidate to conduct OCTAVE-S.

For example, a 200-person company with a flat organizational structure, where many people have rotated throughout the company's departments over the years, may be a candidate to conduct OCTAVE-S. That organization could plausibly assemble an analysis team whose members have sufficient knowledge of business processes employed across the company.

On the other hand, a company of 80 people dispersed across multiple sites and with an extremely stovepiped organizational structure (e.g., 9 distinct departments whose personnel do not have much interaction) might not be a candidate for OCTAVE-S. That organization probably will not be able to assemble an analysis team whose members have insight into all departments.

2.5.1 Should You Use OCTAVE-S?

The following set of questions should be used to help determine the applicability of OCTAVE-S to your organization:

- Is your organization small? Does it have a flat or simple hierarchical structure?
- 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
- 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 have limited familiarity with vulnerability evaluation tools within the context of information-related assets or are you unable to obtain the use of this expertise from current service provider to interpret results?

- Do you prefer a highly structured method as opposed an open-ended method that can be more easily tailored?

If you can answer "yes" to all of these questions, OCTAVE-S should work for you. A majority of "yes" answers implies that it will probably work for you, but caution is advised. While OCTAVE-S may still be useful outside of these boundaries, the results cannot be guaranteed.

2.5.2 Words of Caution

Some people might consider using OCTAVE-S within individual projects, lines of business, or departments, subsequently integrating the results to get the organization-wide perspective. Theoretically, using OCTAVE-S in this manner could work; however, we have neither empirical data to support this theory nor any guidance about what the "integration" process might require.

3 Available Materials

OCTAVE-S can be downloaded from the Web at <http://www.cert.org/octave>. The following list describes the materials that are provided:

- *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 Information Workbook* – This volume provides worksheets for all organizational-level information gathered and analyzed during OCTAVE-S.
- *Volume 5: Critical Asset Workbook for Information* – This volume provides worksheets to document data related to critical assets that are categorized as information.
- *Volume 6: Critical Asset Workbook for Systems* – This volume provides worksheets to document data related to critical assets that are categorized as systems.
- *Volume 7: Critical Asset Workbook for Applications* – This volume provides worksheets to document data related to critical assets that are categorized as applications.
- *Volume 8: Critical Asset Workbook for People* – This volume provides worksheets to document data related to critical assets that are categorized as people.
- *Volume 9: Strategy and Plan Workbook* – This volume provides worksheets to record the current and desired protection strategy and the risk mitigation plans.
- *Volume 10: Example Scenario* – This volume includes a detailed scenario illustrating a completed set of worksheets.

OCTAVE-S is *not* as completely documented as the OCTAVE Method. The materials provided for OCTAVE-S constitute the *minimal* set of materials needed to perform the evaluation.

3.1 Navigation Aid for Downloadable Materials

Each volume of the *OCTAVE-S Implementation Guide* contains an initial section describing the contents of that volume. The navigational aid contained in this introductory volume provides an overall map of the contents of the guide. The process chart, which begins on the next

page, is a cross-reference of the processes, activities, and steps of OCTAVE-S with the volumes in which you will find the associated worksheets. As you conduct an OCTAVE-S evaluation, you can use the process chart as a quick reference to worksheets or to reorient yourself should you lose track of where you are in the process.

When you are ready to begin an OCTAVE-S evaluation, you should start by looking at *Volume 2: Preparation Guidelines* to help you plan and structure the evaluation. You can use *Volume 3: Method Guidelines* to learn about how to conduct each process, activity, and step. You will find the OCTAVE-S worksheets in Volumes 4-9. Finally, you can use *Volume 10: Example Scenario* to better understand the type of results you should get from applying OCTAVE-S.

Process Chart

Process S1: Identify Organizational Information			
Activity	**Step**	**Description**	**Volume: Worksheet**
S1.1 Establish Impact Evaluation Criteria	1	Define a qualitative set of measures (high, medium, low) against which you will evaluate a risk's effect on your organization's mission and business objectives.	Volume 4: Impact Evaluation Criteria
S1.2 Identify Organizational Assets	2	Identify information-related assets in your organization (information, systems, applications, people).	Volume 4: Asset Identification
S1.3 Evaluate Organizational Security Practices	3a	Determine to what extent each practice in the survey is used by the organization.	Volume 4: Security Practices
	3b	As you evaluate each security practice area using the survey from Step 3a, document detailed examples of • what your organization is currently doing well in this area (security practices) • what your organization is currently *not* doing well in this area (organizational vulnerabilities)	Volume 4: Security Practices
	4	After completing Steps 3a and 3b, assign a stoplight status (red, yellow, or green) to each security practice area. The stoplight status should reflect how well you believe your organization is performing in each area.	Volume 4: Security Practices
	---	Document action items identified during Process S1.	Volume 9: Action List
	---	Document notes and recommendations identified during Process S1.	Volume 9: Notes and Recommendations

Process Chart (cont.)

Process S2: Create Threat Profiles			
Activity	**Step**	**Description**	**Volume: Worksheet**
S2.1 Select Critical Assets	5	Review the information-related assets that you identified during Step 2 and select up to five (5) assets that are most critical to the organization.	Volume 4: Critical Asset Selection
	6	Start a *Critical Asset Information Worksheet* for each critical asset. Record the name of the critical asset on the appropriate *Critical Asset Information Worksheet.*	Volumes 5-8: Critical Asset Information
	7	Record your rationale for selecting each critical asset on that asset's *Critical Asset Information Worksheet.*	Volumes 5-8: Critical Asset Information
	8	Record a description for each critical asset on that asset's *Critical Asset Information Worksheet.* Consider who uses each critical asset as well as who is responsible for it.	Volumes 5-8: Critical Asset Information
	9	Record assets that are related to each critical asset on that asset's *Critical Asset Information Worksheet.* Refer to the *Asset Identification Worksheet* to determine which assets are related to the critical asset.	Volumes 5-8: Critical Asset Information
S2.2 Identify Security Requirements for Critical Assets	10	Record the security requirements for each critical asset on that asset's *Critical Asset Information Worksheet.*	Volumes 5-8: Critical Asset Information
	11	For each critical asset, record the most important security requirement on that asset's *Critical Asset Information Worksheet.*	Volumes 5-8: Critical Asset Information

Process Chart (cont.)

Process S2: Create Threat Profiles (cont.)

Activity	Step	Description	Volume: Worksheet
S2.3 Identify Threats to Critical Assets	12	Complete all appropriate threat trees for each critical asset. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. As you complete this step, if you have difficulty interpreting a threat on any threat tree, review the description and examples of that threat in the *Threat Translation Guide*.	Volumes 5-8: Risk Profile Volumes 5-8: Threat Translation Guide
	13	Record specific examples of threat actors on the *Risk Profile Worksheet* for each applicable actor-motive combination.	Volumes 5-8: Risk Profile
	14	Record the strength of the motive for deliberate threats due to human actors. Also record how confident you are in your estimate of the strength of the actor's motive.	Volumes 5-8: Risk Profile
	15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.	Volumes 5-8: Risk Profile
	16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.	Volumes 5-8: Risk Profile
	---	Document action items identified during Process S2.	Volume 9: Action List
	---	Document notes and recommendations identified during Process S2.	Volume 9: Notes and Recommendations

Process Chart (cont.)

Process S3: Examine Computing Infrastructure in Relation to Critical Assets			
Activity	**Step**	**Description**	**Volume: Worksheet**
S3.1 Examine Access Paths	17	Select the system(s) of interest for each critical asset (i.e., the system most closely related to the critical asset).	Volumes 5-8: Network Access Paths
	18a	Review paths used to access each critical asset and select key classes of components related to each critical asset. Determine which classes of components are part of the system of interest.	Volumes 5-8: Network Access Paths
	18b	Determine which classes of components serve as intermediate access points (i.e., components that are used to transmit information and applications from the system of interest to people).	Volumes 5-8: Network Access Paths
	18c	Determine which classes of components, both internal and external to the organization's networks, are used by people (e.g., users, attackers) to access the system.	Volumes 5-8: Network Access Paths
	18d	Determine where information from the system of interest is stored for back-up purposes.	Volumes 5-8: Network Access Paths
	18e	Determine which other systems access information or applications from the system of interest and which other classes of components can be used to access critical information or services from the system of interest.	Volumes 5-8: Network Access Paths

Process Chart (cont.)

Process S3: Examine Computing Infrastructure in Relation to Critical Assets (cont.)			
Activity	**Step**	**Description**	**Volume: Worksheet**
S3.2 Analyze Technology-Related Processes	19a	Determine the classes of components that are related to one or more critical assets and that can provide access to those assets. Mark the path to each class selected in Steps 18a-18e. Note any relevant subclasses or specific examples when appropriate.	Volume 4: Infrastructure Review
	19b	For each class of components documented in Step 19a, note which critical assets are related to that class.	Volume 4: Infrastructure Review
	20	For each class of components documented in Step 19a, note the person or group responsible for maintaining and securing that class of component.	Volume 4: Infrastructure Review
	21	For each class of components documented in Step 19a, note the extent to which that class is resistant to network attacks. Also record how you came to that conclusion. Finally, document any additional context relevant to your infrastructure analysis.	Volume 4: Infrastructure Review
	---	Refine Phase 1 information based on the analysis of access paths and technology-related processes. Update the following, if appropriate: • Mark any additional branches of the threat trees when appropriate (Step 12). Be sure to document appropriate context for each branch you mark (Steps 13-16). • Revise documented areas of concern by adding additional details when appropriate. Identify and document new areas of concern when appropriate (Step 16) • Revise documented security practices and organizational vulnerabilities by adding additional details when appropriate. Identify and document new security practices and/or organizational vulnerabilities when appropriate (Step 3b). • Revise the stoplight status for a security practice when appropriate (Step 4).	Volumes 5-8: Risk Profile Volume 4: Security Practices
	---	Document action items identified during Process S3.	Volume 9: Action List
	---	Document notes and recommendations identified during Process S3.	Volume 9: Notes and Recommendations

Process Chart (cont.)

Process S4: Identify and Analyze Risks			
Activity	**Step**	**Description**	**Volume: Worksheet**
S4.1 Evaluate Impacts of Threats	22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) for each active threat to each critical asset.	Volumes 5-8: Risk Profile Volume 4: Impact Evaluation Criteria
S4.2 Establish Probability Evaluation Criteria	23	Define a qualitative set of measures (high, medium, low) against which you will evaluate the likelihood of a threat occurring.	Volume 4: Probability Evaluation Criteria Volumes 5-8: Risk Profile
S4.3 Evaluate Probabilities of Threats	24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) for each active threat to each critical asset. Document your confidence level in your probability estimate.	Volumes 5-8: Risk Profile Volume 4: Probability Evaluation Criteria Volume 4: Infrastructure Review
	---	Document action items identified in Process S4.	Volume 9: Action List
	---	Document notes and recommendations identified in Process S4.	Volume 9: Notes and Recommendations

Process Chart (cont.)

Process S5: Develop Protection Strategy and Mitigation Plans			
Activity	**Step**	**Description**	**Volume: Worksheet**
S5.1 Describe Current Protection Strategy	25	Transfer the stoplight status of each security practice area to the corresponding area on the *Protection Strategy Worksheet*. For each security practice area, identify your organization's current approach for addressing that area.	Volume 9: Protection Strategy Volume 4: Security Practices
S5.2 Select Mitigation Approaches	26	Transfer the stoplight status of each security practice area from the *Security Practices Worksheet* to the "Security Practice Areas" section (Step 26) of each critical asset's *Risk Profile Worksheet*.	Volumes 5-8: Risk Profile Volume 4: Security Practices
	27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.	Volumes 5-8: Risk Profile
S5.3 Develop Risk Mitigation Plans	28	Develop mitigation plans for each security practice area selected during Step 27. As you complete this step, if you have difficulty coming up with potential mitigation activities for a security practice area, review examples of mitigation activities for that area in the *Mitigation Activities Guide*.	Volume 9: Mitigation Plan
S5.4 Identify Changes to Protection Strategy	29	Determine whether your mitigation plans affect your organization's protection strategy. Record any changes on the *Protection Strategy Worksheet*. Next, review the protection strategy, including proposed changes. Determine whether you intend to make any additional changes to the protection strategy. Record any additional changes on the *Protection Strategy Worksheet*.	Volume 9: Protection Strategy
	---	Document action items identified in Process S5.	Volume 9: Action List
S5.5 Identify Next Steps	30	Determine what your organization needs to do to implement the results of this evaluation and improve its security posture.	Volume 9: Next Steps

3.2 Additional Sources of Help

The OCTAVE approach and the two methods were developed to be self-directed (i.e., performed by an organization on itself, using external assistance only as required or desired). However, given that OCTAVE-S is a beta version, some organizations may need additional assistance. Training is recommended for those with little or no experience with the OCTAVE approach. Another source of additional information and background is the book, *Managing Information Security Risks* [Alberts 02]. Anyone who has already had OCTAVE Method training, used the OCTAVE Method, or read the book is in a better position to understand and use OCTAVE-S. For more information about training and the book, see <http://www.cert.org/octave>.

For other information, see also

- *OCTAVE Criteria* technical report [Alberts 01b]
- *Introduction to the OCTAVE Approach* [Web paper, see <http://www.cert.org/octave>]
- *OCTAVE Method Implementation Guide, V2.0* [Alberts 01a]

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-016, ADA3399229). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001. <http://www.sei.cmu.edu/publications/documents/01.reports/01tr016.html>.

[Alberts 01c] Alberts, Christopher; Dorofee, Audrey; and Allen, Julia. *OCTAVE Catalog of Practices, 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: The OCTAVE Approach.* Boston, MA: Addison-Wesley, 2002.

[Alberts 03] Alberts, Christopher; Dorofee, Audrey; Stevens, James; and Woody, Carol. *Introduction to the OCTAVE Approach.* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003. <http://www.cert.org/octave>.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	January 2005	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
OCTAVE-S Implementation Guide, Version 1.0, Volume 1	F19628-00-C-0003

6. AUTHOR(S)

Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2003-HB-003

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

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

The Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE®) approach defines a risk-based strategic assessment and planning technique for security. OCTAVE is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organizations (less than 100 people). OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organization's personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization's unique operational security risks. To conduct OCTAVE-S effectively, the team must have broad knowledge of the organization's business and security processes, so it will be able to conduct all activities by itself.

14. SUBJECT TERMS	15. NUMBER OF PAGES
information security, risk management, OCTAVE	24

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