

OCTAVESM Method Implementation Guide Version 2.0

Volume 1: Introduction

Christopher J. Alberts
Audrey J. Dorofee

June 2001

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE JUN 2001		2. REPORT TYPE		3. DATES COVERED 00-00-2001 to 00-00-2001	
4. TITLE AND SUBTITLE OCTAVE Method Implementation Guide Version 2.0. Volume 1: Introduction				5a. CONTRACT NUMBER	
				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 Same as Report (SAR)	18. NUMBER OF PAGES 34	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

OCTAVESM Method Implementation Guide Version 2.0

Volume 1: Introduction

Christopher J. Alberts
Audrey J. Dorofee

June 2001

Networked Systems Survivability Program

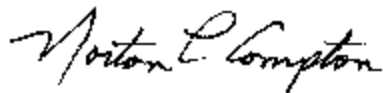
Unlimited distribution subject to the copyright.

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.

Copyright 2001 by Carnegie Mellon University.

Operational Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University. CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use. Requests for permission to reproduce this document or prepare derivative works of this document for external and commercial use should be addressed to the SEI Licensing Agent.

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>).

Preface

This is a Method Implementation Guide for the Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) Method, Version 2.0. The OCTAVE Method is based on a set of criteria, which define the essential elements of an asset-driven, comprehensive, self-directed security risk evaluation for an organization. The OCTAVE Method is the first step in what should be a continuous focus on managing information security risks. The method is a self-directed security evaluation but it also lends itself to using outside experts for specific activities, if necessary. The OCTAVE Method is a complex activity requiring a team with a diverse set of skills and experiences. It is led and performed by an interdisciplinary analysis team made up of people from your business units and information technology (IT) department. While the OCTAVE Method was developed with larger organizations (200+ employees) in mind, it can be tailored to suit a smaller organization.

This Method Implementation Guide contains everything we believe you will need to understand and implement the self-directed information security risk evaluation in your own organization. This is a complete set of reference material for all of the preparation and evaluation activities. We expect this guide to be useful and to provide meaningful results to your organization, whether you use it as is or tailor the materials to suit your organization.

To achieve rapid testing, adoption, and use across a broad spectrum of organization types, sizes, and business domains, we are publicly releasing the guide contents in a format that readers with a range of interests and needs can use. We impose no restrictions on internal use of this material by an organization. See the wording on the copyright and licensing page at the front of this volume for confirmation.

If you make use of this material, in part or in whole, we'd like to hear from you to better understand:

- what worked
- what didn't work
- what needs improvement
- what kind of tailoring you tried, if any

The feedback form at the end of this volume can be mailed or FAXed to us. It can also be found on the World Wide Web (WWW) under www.cert.org/octave/. If you have any questions, please send them to the email address found in the same area on the web. We will periodically post answers and good suggestions for changes and improvements.

The remainder of the OCTAVE Method is detailed in 17 other volumes, which were designed for convenience of use or as references. While the overall Method Implementation Guide is large, quite a few “navigational aids” are provided in the form of introductions, overviews, and embedded tables of content for individual volumes and sections. The authors chose to err on the side of providing as

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

much information as possible on the assumption it would be easier for users of this method to delete material rather than develop it.

In this volume you will find the Introduction, which includes a description of the contents, a brief description of OCTAVE, instructions for how to use this guide, and the feedback form. Start with this volume. It will tell you what you need to know to get started.

Table of Contents for Volume 1: Introduction

Preface	i
Acknowledgements	v
1 Introduction	I-1
2 What Is a Method Implementation Guide?	I-3
3 What Is OCTAVE?	I-7
4 How to Use This Guide	I-13
5 Analysis Team Training	I-17
6 Feedback Form	I-19

Overall Table of Contents for OCTAVE Method Implementation Guide

Volume 1: Introduction

Volume 2:	Preliminary Activities
Volume 3:	Phase 1, Process 1: Identify Senior Management Knowledge
Volume 4:	Phase 1, Process 2: Identify Operational Area Management Knowledge
Volume 5:	Phase 1, Process 3: Identify Staff Knowledge
Volume 6:	Phase 1, Process 4: Create Threat Profiles
Volume 7:	Phase 2, Process 5: Identify Key Components
Volume 8:	Phase 2, Process 6: Evaluate Selected Components
Volume 9:	Phase 3, Process 7: Conduct Risk Analysis
Volume 10:	Phase 3, Process 8, Workshop A: Develop Protection Strategy
Volume 11:	Phase 3, Process 8, Workshop B: Select Protection Strategy
Volume 12:	Asset Profile Workbook
Volume 13:	After the Evaluation
Volume 14:	Bibliography and Glossary
Volume 15:	Appendix A: Catalog of Practices
Volume 16:	Appendix B: OCTAVE Data Flow
Volume 17:	Appendix C: Complete Example Results
Volume 18:	Appendices D and E: White Papers

Acknowledgements

The method developers would like to acknowledge the following for their contributions to the OCTAVE Method Implementation Guide.

Additional technical development was provided by

- Julia Allen
- Sandra G. Behrens
- Rich Pethia
- Bradford Willke (especially for assistance with Processes 5 and 6)
- William R. Wilson

Editing support was provided by

- Suzanne Couturiaux

CD-ROM design support was provided by

- Matthew DeSantis
- Michael Durkota

Non-technical support was provided by

- Linda Pesante
- Jim Main
- Rita Briston
- Jill Hatch

And we would especially like to thank those reviewers who donated a large part of their time reading this guide end-to-end:

- Julia Allen
- Richard E. Barbour
- Jeff Collmann (Telemedicine and Advanced Technology Research Center (TATRC))
- Lynn Crane (Advanced Technology Institute (ATI))
- Eileen Forrester
- Klaus-Peter Kossakowski
- Steve Pellessier (Advanced Technology Institute (ATI))
- Robin Ruefle
- Carol A. Sledge

1 Introduction

This volume introduces the Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) Method Implementation Guide and the OCTAVE Method. Everyone interested in the method should read this section. It explains the organization and content of the 17 additional volumes and provides a brief description of the OCTAVE Method¹. This volume also provides guidance for using the Method Implementation Guide, based on who you are and what your purpose is. This guide is intended to provide enough material and guidance for most analysis teams to get started, with or without formal training. A short discussion on analysis team training is provided in this volume. Finally, a feedback form for comments and suggestions is provided. This form can be mailed or FAXed to the Software Engineering Institute.

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

¹ For a more detailed overview of the OCTAVE Method, refer to *Overview of the OCTAVE Method* in Appendix D (Volume 18).

2 What Is a Method Implementation Guide?

This is the Method Implementation Guide for the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), version 2.0. So what is a Method Implementation Guide? In short, this is everything we think you need to perform an OCTAVE for your organization. While there are many ways that the OCTAVE Method can be implemented, this guide reflects the most probable scenario.

There are 18 volumes in this guide, in its printed form. You could be reading this in either paper or electronic form. In general, the Method Implementation Guide includes

- overview material
- feedback form to return your experiences, critiques, and suggestions
- guidance for preparing to do an OCTAVE
- tailoring guidance
- process descriptions and guidance
- worksheets and instructions
- slides and notes for presentations
- surveys
- catalogs
- references
- a complete example of all results, based on our pilot tests and experience

If you are reading this, we assume you are either a potential “champion,” a manager, someone who may be getting ready to implement OCTAVE (an analysis team member), or someone who is just curious about the method. Champions, by our definition, are those who see something they think will help their organization, and proceed to do whatever is needed to get it started. A champion could be a manager, a senior staff member, or a recognized expert within the organization. Managers reading this are likely looking to see what this is going to cost in terms of people and time, and what role they might have to play. Analysis team members could be from the information technology (IT) department or other business units within the organization.

The Method Implementation Guide is divided into 18 volumes to make it easier to use. Each volume has its own table of contents and there are some variations in page numbering to make the individual sections easier to find. Each volume always has a list of the full set of volumes to remind readers where they are in the series.

The volumes of the Method Implementation Guide are organized as follows:

- **Volume 1: Introduction:** This volume (which you are currently reading) includes a description of OCTAVE, guidance on how to use this guide, some suggestions relative to analysis team training, and a feedback form.
- **Volume 2: Preliminary Activities:** This 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. Each process is documented in its own volume and generally includes an introduction, a summary of the process, example results, detailed process guidelines, worksheets, and a set of slides and notes. Process 8, which has 2 different types of workshops, is broken into two volumes, for convenience. In addition, an Asset Profile Workbook is in a separate volume and provides a complete set of all of the worksheets and results associated with a single critical asset. Volumes 3-12 define the OCTAVE Method and are the largest part of the guide.
- **Volume 13: After the Evaluation:** This is a short section providing guidance and an example of what to do after the evaluation is over.
- **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 the definitions for the key terms used throughout this guide.
- **Volume 15: Appendix A: OCTAVE Catalog of Practices:** This volume provides a set of good information security practices against which an organization measures itself for current practices and organizational vulnerabilities.
- **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.

OCTAVE is meant to be tailored to your organization and your domain. There are many aspects to this tailoring, which are discussed throughout this guide. You can tailor both the overall process and the smaller pieces, such as the templates and the catalog of practices. You could even use only part of the process to see if this is something you want to invest time in. See the Tailoring section in Volume 2 for specific guidance on tailoring this method.

Training for analysis teams may or may not be needed; it depends on who is selected, their experience with assessments, and their comfort level in trying something on their own. Some will want training;

some will not. If you need information about what training is available, see the OCTAVE Web site www.cert.org/octave/. Detailed training information is not included here, as we expect that to change over time. However, there are some training suggestions later in this volume that may be helpful.

The page numbering scheme used throughout this guide is intended to help you remember where you are. Check the table of contents for each volume for specific prefixes on page numbers. You will also note that the headers for each page contain a title for the section you are in.

A final note – throughout this guide you will see references such as (A1.1) or (W1.2). These refer to the specific activities, inputs, outputs and worksheets for OCTAVE, as defined in the OCTAVE Data Flow in Appendix B, Volume 16. For example, in the process guidelines for each process, all worksheets, outputs, and activities use the numbering scheme described in Table 1. Note that while a number is used to indicate a process, the letters “PR” are used to indicate the Preparation activity.

Table 1: Numbering Scheme for Data Flow Diagrams

Number	Definition	Example
Ax.y	y Activity in Process x	A4.1 is the first activity of Process 4.
Wx.y	y Worksheet in Process x	W3.1 is the first worksheet of Process 3.
IPR.y	y Input of Preparation	IPR.1 is the first input of OCTAVE Preparation
Ix.y	y Input of Process x	I5.2 is the second input of Process 5.
OPR.y	y Output of Preparation	OPR.2 is the first output of OCTAVE Preparation.
Ox.y	y Output of Process x	O5.2 is the second output of Process 5.
AB	Artifact ab	PG and WK are the Preparation Guidelines and the Asset Profile Workbook.
Dx.y	y data preparation or pre-work activity for Process x	D4.3 is the third data preparation or pre-work activity in Process 4. It occurs before the workshop for Process 4.
Xz.y	y post-workshop activity for Process z	X4.1 is the first post-workshop activity for Process 4.

These cross-references can be used to help you locate more specific or additional information on the activity or worksheet. The specific worksheets can be found with each process just after to the process guidelines. Additional information on activities can be found in the Process Guidelines using the table of contents for that section.

3 What Is OCTAVE?

Information systems are essential to most organizations today. However, many organizations form protection strategies by focusing solely on infrastructure weaknesses; they fail to establish the effect on their most important information assets. This leads to a gap between the organization's operational and information technology (IT) requirements, placing the assets at risk. Current approaches to information security risk management tend to be incomplete. They fail to include all components of risk (assets, threats, and vulnerabilities). In addition, many organizations outsource information security risk evaluations. The resulting evaluation may not be adequate or address their perspectives. Self-directed assessments provide the context to understand the risks and to make informed decisions and tradeoffs.

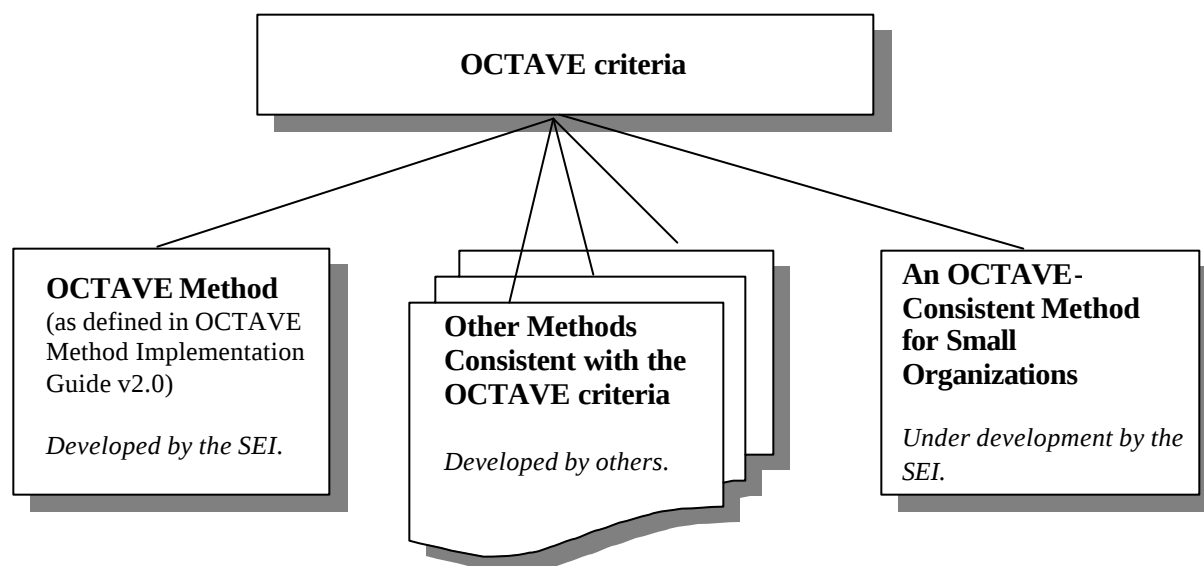
The first step in managing information security risk is to understand what your risks are. Once you have identified your risks, you can build mitigation plans to address those risks. The Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) enables you to do this.

OCTAVE is an approach to information security risk evaluations that is comprehensive, systematic, context-driven, and self-directed. The approach is embodied in a set of criteria that define the essential elements of an asset-driven information security risk evaluation [Alberts 2001a].

There can be many implementations (or methods) consistent with the OCTAVE criteria. For example, the criteria would be implemented differently in very a large organization than in a very small one. At this point, we have developed one method consistent with the OCTAVE criteria, called the OCTAVE Method.

The OCTAVE Method, documented in this Method Implementation Guide, was designed with larger organizations in mind. Another method for small organizations is in development. In addition, others might define methods for specific contexts that are consistent with the criteria. Thus, there can be many OCTAVE-consistent methods, but there is only one set of OCTAVE criteria. Figure 1 illustrates this point.

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

Figure 1: Multiple Methods Consistent with the OCTAVE Criteria

The OCTAVE criteria require the evaluation to be led and performed by a small, interdisciplinary analysis team of the organization's business and IT personnel. Team members work together to make decisions based on risks to critical information assets. Finally, the OCTAVE criteria require catalogs of information to measure organizational practices, analyze threats, and build protection strategies. These catalogs are

- catalog of practices – a collection of good strategic and operational security practices
- generic threat profile – a collection of major sources of threats
- catalog of vulnerabilities – a collection of vulnerabilities based on platform and application

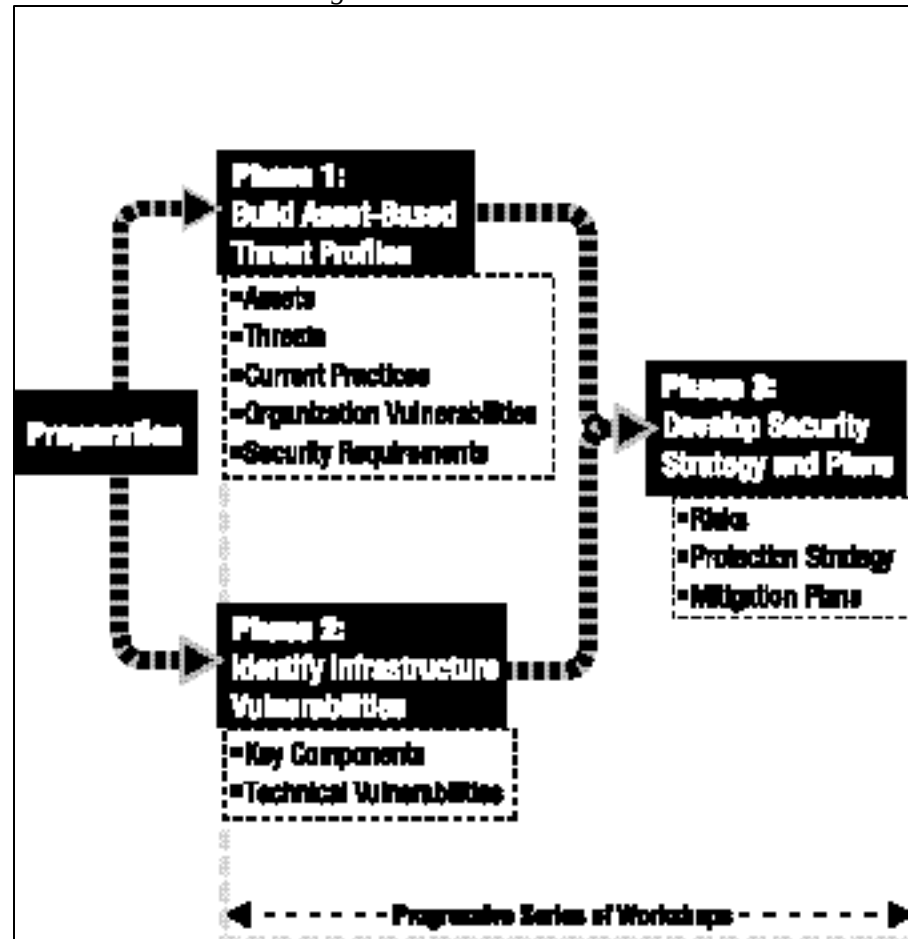
The rest of this section briefly describes preparing for the OCTAVE Method, the OCTAVE processes, and what happens after the evaluation. A longer, more complete discussion of the OCTAVE Method can be found in Appendix D, Volume 18.

The OCTAVE Method

The OCTAVE Method uses a three-phase approach to examine organizational and technology issues, assembling a comprehensive picture of the organization's information security needs (see Figure 2). The method uses workshops to encourage open discussion and exchange of information about assets, security practices, and strategies.

Each phase consists of several processes and each process has one or more workshops led or conducted by the analysis team. Some preparation activities are also necessary to establish a good foundation for successfully completing the evaluation.

Figure 2: OCTAVE Method



Preparing for OCTAVE creates the foundation for a successful evaluation. Some keys to a successful evaluation are

- Get senior management sponsorship – This is the most critical success factor. If senior managers support the process, people in the organization will actively participate.
- Select the analysis team – Team members need to have sufficient skills to lead the evaluation. They also need to know how to go outside the team to augment their knowledge and skills.
- Scope OCTAVE – The evaluation should include important operational areas. If the scope is too big, it will be hard to analyze all of the data. If it is too small, the results may not be as meaningful.
- Select participants – Staff members from multiple organizational levels will contribute their knowledge. It is important for these people to understand their operational areas.

These three phases 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 information technology 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 the 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 those risks, 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 the organization and mitigation plans for critical assets, based upon an analysis of the information gathered. Senior managers then review, refine, and approve the strategy and plans.

After OCTAVE – Finally, at the end of the evaluation, implementation details will need to be added to the protection strategy and risk mitigation plans. Managers should also define steps for continuously reviewing and improving their security posture.

4 How to Use This Guide

This guide is intended for managers or internal champions who are considering using the OCTAVE Method and for interdisciplinary analysis teams who will perform the majority of the activities. Training may not be needed for an analysis team with experience in doing assessments or process evaluations. However, if needed, information about OCTAVE Method Training can be found in the Volume 2, Preliminary Activities, the Analysis Team Training section and at the Web site <http://www.cert.org/octave/>.

As described in this Method Implementation Guide, the OCTAVE Method consists of a series of workshops. Some workshops are discussions facilitated by the analysis team, while others are conducted by the analysis team with additional experts if needed. OCTAVE is accomplished by the organization being evaluated, not by an independent assessment team. It is recognized, however, that outside expertise may be required at some key points in the process. This determination should be made early on during preparation.

The rest of this section provides some guidance on who should use what parts of this Method Implementation Guide. This is guidance only. Readers should feel free to explore any part. If you are reading this from the CD-ROM, it may be easier to browse the linked version and determine which parts are the most useful.

Curious or Casual Reader

If you just want to know what OCTAVE is and how it might be useful to you, look at the following:

1. Read the “What is OCTAVE?” section of this volume.
2. Read the white papers “An Overview of the OCTAVE Method ” and “OCTAVE Threat Profiles” in Appendix D (Volume 18).
3. Look through the Complete Example Results in Appendix C (Volume 17).
4. Read the Introduction sections for each process (Volumes 3-11).
5. Look through the Asset Profile Workbook (Volume 11), the catalog of practices (Appendix A, Volume 14), and the surveys in Processes 1 to 3 (Volumes 3-5).

Champions

Generally, there is a champion or a manager interested in seeing the OCTAVE Method implemented. That champion or manager should complete the following actions:

1. Read the “What is OCTAVE?” section of this volume.

2. Read the white paper “An Overview of the OCTAVE Method” in Appendix D (Volume 18) if more detail is desired.
3. Read the Preparation Guidelines (Volume 2), paying particular attention to the first parts dealing with sponsorship, selection of the analysis team, and selection of participants.
4. Identify the appropriate managers and use the senior management briefing to establish sponsorship.
5. Use the Preparation Guidelines (Volume 2) to work with senior management, selecting the analysis team.
6. Work with management to obtain training for the analysis team.

Sponsors and Other Managers

Sponsors and other managers who need to understand what OCTAVE is should look at the following:

1. Read the “What is OCTAVE?” section of this volume.
2. Read the white paper “An Overview of the OCTAVE Method” in Appendix D (Volume 18) if more detail is desired.

Analysis Team

The analysis team should do the following:

1. Read the “What is OCTAVE?” section of this volume and the papers in Appendices D and E, (Volume 18).
2. Be trained in or spend several days reviewing and discussing the method to reach a good level of understanding.
3. Read the Preparation Guidelines in Volume 2.
4. Read the rest of the Implementation Guide, focusing on the Process Guidelines, Worksheets, and Asset Profile Workbook. Note the Entry/Exit Criteria and suggested timelines found at the start of each Process.
5. Review the example results as a team and discuss any issues or uncertainties.
6. Read the Tailoring Guidelines in Volume 2.
7. Revise or replace the catalog of practices (Volume 14) and organizational practice surveys (Volumes 3-5), if necessary, and make any other tailoring changes.
8. Work with management to select the participants.
9. Define the plan for conducting OCTAVE, laying out the schedule and participants, and using the Preparation Guidelines in Volume 2.
10. Determine if and when you will need outside expertise and arrange for their assistance.
11. Hold an opening briefing with the participants.
12. Facilitate Workshops 1-3 (using Volumes 3-5) with the participants and record all data.

Analysis Team (cont.)

13. Conduct Workshop 4 (using Volumes 6 and 12), integrating and analyzing the data from Workshops 1-3.
14. Conduct Workshops 5 and 6 (using Volumes 7, 8, and 12), using any additional personnel as needed, then discuss the findings.
15. Conduct Workshops 7 and 8 (using Volumes 9-12), briefing senior management on the findings and recommended strategy and plans, and making changes as requested by the senior managers.
16. Brief all participants on the results.
17. Further refine, as needed, the protection strategy and mitigation plans.
18. Follow through with implementation of the strategy and mitigation plans and use the “After the Evaluation” material in Volume 13.

5 Analysis Team Training

5.1 Training Class Information

This Method Implementation Guide is intended to provide the information and guidance necessary to enable an analysis team to proceed on its own without formal training. If training is needed, see www.cert.org/octave for the most up-to-date information on training and training providers.

OCTAVE Method training is a three-day workshop that trains analysis teams in all of the OCTAVE processes by having them actually perform the processes using their own organization's information. Teams also learn to use all of the materials in the Method Implementation Guide. Formal method training can be useful to some analysis teams, particularly those that are new to evaluations or who want the assurance of having had formal training. However, some teams may find it just as easy to simply roll up their sleeves and get started on a small scale.

5.2 Just Getting Started

If you, the analysis team, want to get started without training, there are some things you can do to make it easier on yourselves. First, spend three to five days reading and discussing the materials, going through the preparation guidelines in Volume 2, and looking through the complete example results in Volume 17. Then get together and select one asset that you consider critical to the organization. For that asset, use the Asset Profile Workbook (Volume 12) to define security requirements, identify threats and risks, and create mitigation plans. You might also fill out the staff or IT staff surveys from Process 3 for yourselves and see what kind of organization-wide protection strategy you would recommend based on the results. Running vulnerability tools is not likely to be done without a recognized effort, but if such tools are routinely run, then perhaps the IT group can spend a some time with the analysis team discussing the results from any key components related to the critical asset.

Working through these processes with one of your assets can go a long way towards understanding the activities and how to work with the information. You should talk about what was easy and what was difficult, look back over the guidance for the processes, and then begin preparing and planning for the real evaluation. You can also use your results for the selected critical asset to help convince senior managers to sponsor OCTAVE.

As a final note, if you choose to proceed without formal training, make sure your managers understand that you are learning as you go, and the processes may take a bit longer than planned.

6 Feedback Form

If you have any comments, suggestions, or corrections, please fill in and either mail or FAX this form to the SEI, attention OCTAVE Feedback. This form can also be found on the WWW at www.cert.org/octave/.

We also request that you if you have any sanitized data or case study information that you could share with the SEI or the broader base of OCTAVE users, to please let us know and we will arrange a means to transfer the data.

Mailing address:

OCTAVE Feedback
Software Engineering Institute
4500 Fifth Ave.
Pittsburgh, PA 15213-3890

FAX number: (412) 268-5758

Attention: OCTAVE Feedback/Survivable Enterprise Management Group

Feedback Form for OCTAVE Method Implementation Guide v2.0

	← OFTEN		SOMETIMES		← RARELY →
1. Were the materials in the OCTAVE Method Implementation Guide					
1.1 easy to use?	☐	☐	☐	☐	☐
1.2 easy to understand?	☐	☐	☐	☐	☐
1.3 complete?	☐	☐	☐	☐	☐
1.4 well designed?	☐	☐	☐	☐	☐

2. Which, if any, topics, sections, worksheets, or other materials stand out as....
- 2.1 being particularly useful?

 2.2 needing improvements? (please describe)

Feedback Form for OCTAVE Method Implementation Guide v2.0

3. Overall, how can the OCTAVE Method Implementation Guide be improved to better satisfy your needs?

4. Is there any other feedback that you would like to provide to us?

Feedback Form for OCTAVE Method Implementation Guide v2.0	
Please provide us with any errors that you found in the OCTAVE Method Implementation Guide.	
Page Number	Description

Feedback Form for OCTAVE Method Implementation Guide v2.0	
Please provide us with any errors that you found in the OCTAVE Method Implementation Guide.	
Page Number	Description

