OCTAVE®-S Implementation Guide, Version 1.0

Volume 2: Preparation Guidance

Christoper Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

Carnegie Mellon
Software Engineering Institute

OCTAVE®-S Implementation Guide, Version 1.0

Volume 2: Preparation Guidance

Chrstopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

Networked Systems Survivability Program

This report was prepared for the

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

Table of Contents

List of Tables

About This Document

This document is Volume 2 of the *OCTAVE-S Implementation Guide*, a 10-volume handbook supporting the OCTAVE-S methodology. This volume provides guidance and worksheets for an organization preparing to conduct an OCTAVE-S evaluation.

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.

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 Overview of Preparation

Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE[®])-S preparation activities are important because they set the stage for a successful evaluation. During preparation, you determine how your organization will conduct OCTAVE-S. In addition, you directly address the following key success factors:

- getting senior management sponsorship for the evaluation

- selecting the analysis team to lead the evaluation

- setting the scope of the evaluation

There are many ways in which organizations can prepare to conduct OCTAVE-S. In this section, we focus on a likely scenario for many organizations and make the following assumptions:

- There is a champion – someone internal to the organization with an interest in conducting OCTAVE-S.

- OCTAVE-S is an appropriate choice for the organization.

- The analysis team does *not* exist prior to gaining senior management approval.

If your circumstances are different, you may need to adjust the activities or the order in which they occur to suit your organization. The champion should help the organization's senior managers understand the benefits of OCTAVE-S and gain their sponsorship for conducting the evaluation. After the managers decide to use OCTAVE-S, they work with the champion to select members of the analysis team. The analysis team then becomes the focal point for completing all evaluation activities. Table l summarizes the preparation activities. Later sections in this document describe these activities in detail.

The next section begins to examine how an organization prepares for the evaluation by presenting a few ideas about developing senior management sponsorship of OCTAVE-S.

[SM] Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University.
[®] OCTAVE is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

Table 1:   OCTAVE-S Preparation Activities

	Activity	Step	Description	Worksheet
S0.1	Obtain Senior Management Sponsorship of OCTAVE-S	---	A person or team from the organization (i.e., a champion for OCTAVE-S) works with the organization's senior managers to gain their sponsorship of the evaluation. This person or team is responsible for making the managers aware of the evaluation process, the expected outcomes, and what commitments of time and personnel must be made.	---
S0.2	Select and Train Analysis Team Members	---	The organization's senior managers designate someone in the organization to select analysis team members. Alternatively, the senior managers can select team members. Once analysis team members have been selected, they need to become familiar with OCTAVE-S through formal training or informal means.	*Preparation* worksheet
S0.3	Set the Scope of the Evaluation	---	The analysis team guides the organization's senior managers in selecting which operational areas to examine during OCTAVE-S.	*Preparation* worksheet
S0.4	Plan to Conduct OCTAVE-S		The analysis team develops a plan and schedule for conducting OCTAVE-S. The team also tailors the evaluation as needed during this activity.	*OCTAVE-S Checklist* worksheet
S0.5	Prepare to Conduct Each OCTAVE-S Process		Before starting any OCTAVE-S process, the analysis team must ensure that • all entry criteria for that process have been met • all team members understand their roles • any supplemental team members (i.e., people providing unique skills, experience, and expertise required by that process) understand their roles as well as the OCTAVE-S process in which they will participate • an approach for making decisions that is understood by all participants has been agreed upon • rooms for all meetings have been reserved • any required equipment (e.g., overhead projectors, flip charts) is available and has been reserved	*OCTAVE-S Checklist* worksheet

2 Obtain Senior Management Sponsorship of OCTAVE-S (Activity S0.1)

Senior management sponsorship is the top critical success factor for information security risk evaluations. A successful evaluation requires an investment of people's time. If senior managers support the process, people in the organization tend to participate actively. If senior managers do not support the process, then staff support for the evaluation will dissipate quickly. OCTAVE-S does require an investment of time on the part of analysis team members, and the organization's managers must ensure team members are able to participate as required by the process.

2.1 What Is Sponsorship?

 Sponsorship implies the following conditions:

- visible, continued support of OCTAVE-S activities

- active encouragement of staff participation

- delegation of responsibility and authority for accomplishing all OCTAVE-S activities

- commitment to allocate the necessary resources

- agreement to support implementation of the results of the evaluation

The last item is particularly important, because any evaluation loses its value if little or nothing is done with its results and recommendations. An evaluation that goes nowhere is, in fact, worse than no evaluation at all because staff and managers will be less inclined to do another one in the future.

2.2 Getting Sponsorship

Although sponsorship from senior managers is vital to conducting a successful OCTAVE-S, there is no simple formula for obtaining it. In some cases, an organization's senior managers will take the initiative in implementing OCTAVE-S in their organizations. In those cases, sponsorship already exits. However, this is not typical.

Often, one person in the organization learns about the OCTAVE approach and decides that OCTAVE-S is the appropriate version of OCTAVE to conduct in his or her organization. This person is referred to as the champion. To develop senior management sponsorship of OCTAVE-S,

the champion needs to set expectations for the evaluation by informing appropriate senior managers of the evaluation process, the expected outcomes, and the expected time and personnel commitments. An "appropriate senior manager" is defined as anyone high enough in the organization to commit the organization and its resources to this effort. These senior managers are often chief executive officers, directors, or members of an organization's governing board.

Part of setting expectations for OCTAVE-S requires developing a shared understanding of the goals of the evaluation. For example, the goal might be to comply with a regulation. In other cases, the evaluation might be a response to a recent security incident. The goal in that case might be to reduce the risk of a major incident occurring in the future. It is important that the managers express their goals for the evaluation early in the process. Doing this helps set expectations and provides valuable information when the analysis team subsequently sets the scope of the evaluation.

2.2.1 Regulations and Standards of Due Care

Regulations are becoming more common in many industry segments these days. For example, the Health Insurance Portability and Accountability Act (HIPAA) [HIPAA 98] establishes a standard of due care for information security for healthcare organizations, while Gramm-Leach-Bliley [Gramm 01] legislation does the same for financial organizations. Most information security standards of due care require an organization to conduct an information security risk evaluation and to manage its risks. If your organization must perform an information security risk evaluation because of regulations, you can bring this to the attention of your organization's managers. Senior managers in some organizations have sponsored information security risk evaluations after learning about regulations and the requirements for complying with those regulations.

2.2.2 Anecdotal Information

 Although there is no substantial "return on investment" data currently available with respect to security improvement activities [Berinato 02, Braithwaite 01, Oberndorf 00, Proctor 03, SBQ 01], you can use anecdotal information to inform senior managers about the benefits of using information security risk evaluations.[1] You can emphasize how some organizations use these evaluations as the central component of a security improvement initiative. Those organizations often view a security improvement initiative as a competitive advantage.

2.2.3 Conducting a Limited Evaluation

One technique that has proven to build sponsorship in some organizations is conducting a limited evaluation. A limited evaluation focuses on one area of the organization (often on a single asset).

---

[1]   Some anecdotal information can be found at
      <http://www.cert.org/features/green/business_case.html#bib> from which the references in this
      document were drawn.

The analysis team performs a limited-scope evaluation and presents the results to senior managers. This approach enables senior managers to see what the results of the evaluation look like and can be a good way to get them interested in expanding the effort.

2.2.4 Using Example Results or Case Studies

Another possibility is using the example results to illustrate to senior managers the types of results that are expected from this evaluation. It is more beneficial to have results similar to your own domain; however, such example results are currently limited. Volume 10 of this method implementation guide contains the sample results for a small medical facility.

In the end, there is no universal way to get sponsorship for conducting an evaluation like OCTAVE-S. The ideas presented in this section should help you think about how to begin building sponsorship of OCTAVE-S in your organization. The next section examines the selection of analysis team members.

3 Select and Train Analysis Team Members (Activity S0.2)

The analysis team is the focal point for conducting OCTAVE-S. This team is responsible for the ultimate success of the evaluation. Because the analysis team plays a pivotal role, it is important to select a core team that has sufficient skills, experience, and expertise to lead the evaluation.

3.1 Who Is on the Analysis Team?

The general guidelines for selecting analysis team members for OCTAVE-S include the following:

- The core analysis team is generally three to five people in size.

- Supplemental team members can be added to any process to provide specific skills or knowledge.

- The team typically includes people from across the organization, including a mix of staff and, where possible, managers.

- The team must have broad insight into the organization's business and information technology processes and capabilities.

- Both business/mission and information technology perspectives are represented on the team to the extent possible.

The champion often assembles the analysis team after senior management sponsorship of the evaluation is obtained. Senior managers might also designate someone in the organization to work with the champion or to lead the selection of the analysis team. Note that when the evaluation is scoped, business units or operational areas are selected to be included in the evaluation. Some organizations decide to select people from these operational areas to be on the analysis team. In that case, this activity, *Select and Train Analysis Team Members*, is performed after the next activity, *Set Scope of Evaluation* (see Section 4).

In many small organizations, the information technology (IT) representatives on the analysis team are those people who work closely with service providers or work most closely with the technology. Many small organizations do not have full-time IT staff members. Analysis teams in these organizations must include people who are most familiar with the organization's technology base.

In OCTAVE-S, the analysis team is empowered to represent the global perspective of security for the organization. Only the analysis team members participate in activities during OCTAVE-S; there are no facilitated knowledge elicitation workshops like those used during the OCTAVE Method [Alberts 01a]. Thus, it is very important to select the appropriate team members.

3.1.1 Using Managers on the Analysis Teams

During the OCTAVE-S pilots, the analysis teams included both managers and staff members from the organizations. This type of composition provided insight from multiple organizational levels as well as a diverse set of team skills. These staff members and managers tended to work closely together on a routine basis. Because organizational positions did not get in the way of information sharing, it was possible to include both management and staff on the analysis team.

Mixing managers and staff on an analysis team might not work in all small organizations, especially in very hierarchical organizations. In some organizations, the presence of managers becomes a barrier to open communication of risks and issues. Some staff members might not be willing to share their concerns openly when their managers are present. This type of situation will adversely affect the results of the evaluation. Instead of managers, senior staff members or people who have been with the organization for a long time and are very familiar with the organization's plans and business goals are also good selections.

3.1.2 Roles and Responsibilities

The analysis team helps to set the scope of the evaluation. It also is responsible for identifying key issues and analyzing information. The roles and responsibilities of the analysis team include

- working with senior managers to set the scope of the evaluation

- scheduling OCTAVE-S activities

- conducting the evaluation activities

- gathering, analyzing, and maintaining evaluation data during the evaluation

- coordinating logistics for the evaluation

Logistics can be handled by one member of the core analysis team, or an additional person can be assigned to the analysis team specifically to address logistics. (Coordinating logistics for OCTAVE-S is discussed in Section 5 of this document.)

3.1.3 Skills and Knowledge Needed to Conduct OCTAVE-S

OCTAVE-S relies upon the experience and expertise of the analysis team members. For an effective evaluation, team members must have broad insight into

- how systems and information are used to support the organization's business processes across the organization

- organizational policies and processes

- the processes used to configure and maintain the organization's computing infrastructure

OCTAVE-S is not a typical vulnerability evaluation that focuses solely on technological issues. Because it addresses both business and technological issues, OCTAVE-S is an operational risk evaluation that is similar to typical business process or management evaluations. It is helpful if someone on the analysis team is familiar with or has done assessments or evaluations. At least one member of the analysis team must have some familiarity with the organization's computing infrastructure or must be the point of contact with the providers who configure and maintain the computing infrastructure. The person who has familiarity with the infrastructure needs to understand the organization's basic information security processes.

One characteristic of all successful analysis teams is that team members must have good working relationships, enabling them to openly share their concerns about security in the organization. Keep this in mind as you form your team.

The specific skills needed for each OCTAVE-S process are detailed in the *OCTAVE-S Checklist* in the appendix of this document. By reviewing the suggested skills for each process, you can determine whether it is necessary to supplement the skills of the core analysis team by including an additional person for a selected process. In general, the skills required for the core members of the analysis team are

- ability to manage group meetings

- good communication skills

- good analytical skills

- knowledge of the organization's business environment

- knowledge of the organization's information technology environment and how the business staff legitimately uses information technology in the organization

The analysis team can add supplemental team members to particular activities as needed (e.g., an operational area manager to help with planning, someone from a specific operational area during asset identification). These additional people augment the skills of the core team by providing unique abilities needed during designated activities. It is also important to consider team chemistry when you augment your team for a particular activity. Possible supplemental members may include those with

- knowledge of the organization's planning practices

- ability to develop plans

3.2 Guidance for Selecting an Analysis Team

Selecting an analysis team for OCTAVE-S requires you to identify people who have broad knowledge of business processes and how the computing infrastructure supports those processes. The analysis team should also be balanced to provide perspectives of people throughout the organization. You should consider including both managers and staff members if possible.

Use the *Preparation worksheet* when you are selecting analysis team members. (The *Preparation worksheet* can be found in the appendix of this document.) The worksheet breaks the selection of analysis team members into the following two parts:

- business-related areas

- information technology department

Start with the business-related areas of the organization (Part A of the worksheet). People from the business-related areas should have broad insight into how systems and information are used to support the organization's business processes and/or insight into organizational policies and processes. You can include up to 3 analysis team members from the business-related units.

Next, you must think about who has the most insight into the organization's computing infrastructure (Part B of the worksheet). Many small organizations do not have an IT department and many completely rely on third parties (e.g., contractors or service providers) for their information technology needs. In that case, you should include whoever works most closely with the third party. Depending on your organization's relationships with contractors and service providers, you could also include people third-party organizations on the analysis team.

IT-related analysis team members should have insight into your organization's computing infrastructure and/or how the systems and networks are configured and maintained. You may also select someone from a contracting organization or service provider who has insight into how systems and networks are configured and maintained *and* who could participate in the evaluation. You can include up to 3 IT-related analysis team members.

3.3 Training the Analysis Team

Once analysis team members have been selected, at least one team member needs to become familiar with OCTAVE-S. Ideally, all team members would become acquainted with the OCTAVE-S methodology. However, organizational constraints (e.g., funds available, size of organization) might limit the number of people who can invest time to become familiar with the process. Team members who are tasked with learning about OCTAVE-S can participate in formal training or become familiar with the process by working on their own. (For example, through reading and understanding the material in the *OCTAVE-S Method Implementation Guide*.)

If an analysis team decides to get started without training, there are some things it can do to facilitate the learning process. First, all team members should spend time reading about OCTAVE-S and discussing it among themselves. The team would then perform a very limited pilot by selecting one asset that team members consider to be critical to the organization. Once it completes the analysis for one asset, the team can then expand the evaluation to look at other critical assets.

Working through a limited pilot of the OCTAVE-S can go a long way toward understanding each evaluation process and how to work with information generated throughout the evaluation. As you complete your pilot, you should talk about what was easy and what was difficult. You should also review the guidance for the processes and begin to prepare and plan for an expanded evaluation. You can also use your results from the pilot to help convince senior managers to sponsor a more extensive evaluation. 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 that the evaluation might take longer than planned.

Once the analysis team has been selected and is trained in OCTAVE-S, it can set the scope of the evaluation. This topic is addressed in the next section.

4 Set the Scope of the Evaluation (Activity S0.3)

In OCTAVE-S, you can focus the evaluation on selected areas of the organization. Setting a manageable scope for the evaluation reduces its size, making it easier to schedule and perform the activities. It also allows you to prioritize the areas of an organization for the evaluation, ensuring that the highest risk or most important areas can be examined first or more frequently.

4.1 Setting the Scope of the Evaluation

In many small organizations, it is possible to evaluate the entire organization during OCTAVE-S. Organizations with a focused mission requiring most of its staff to support it directly may be able to evaluate the entire organization during an OCTAVE-S evaluation.

Small organizations with multiple business units, or operational areas, might be required to select a subset of those areas to evaluate. This is especially true if operational areas in the organization tend to be stove-piped. When selecting operational areas to evaluate, the analysis team typically works with the organization's senior managers. They consider the following guidelines when choosing operational areas:

- Select business units or operational areas that reflect the primary operational or business functions as well as the important support functions of the organization. Operational areas selected for the evaluation should represent those most critical to the success of the organization or those with the highest risk.

- At least four operational areas are generally recommended, one of which *must* be the information technology or information management department (or people familiar with the computing infrastructure if such a department does not exist).

- If the organization outsources most or all of its information technology or information management to service providers, select the person(s) who work most closely with the service providers or include representatives from the service providers on the analysis team.

- If the information technology or information management department is dispersed, or managed as separate support groups, select a cross section of those groups.

- Consider the time commitment that personnel will be required to contribute. Determine whether there will be significant conflicts with ongoing operations.

- Consider areas that require *electronic* information to accomplish their functions.

Remember that these are only guidelines. Senior managers and analysis team members need to use their best judgment when selecting areas to include in the evaluation.

4.2 Guidance for Setting the Evaluation's Scope

Use the *Preparation worksheet* when you are setting the scope of the evaluation. Turn to Part C of the worksheet. Consider the following questions as you select areas of the organization to include in the evaluation:

- Which operational areas of your organization are most critical to achieving its mission?

- Which operational areas would affect the organization's ability to function if those areas were unable to function?

- In which operational areas do you believe information and/or systems are most at risk?

Record the names of the selected operational areas on the worksheet. If the analysis team was selected prior to setting the scope of the evaluation, make sure that team members have an understanding of the operational areas being evaluated. If the team does not have sufficient insight into one or more areas, you might need to adjust the composition of the team.

At this point, you should be ready to plan how you intend to conduct the evaluation. The next section focuses on planning considerations.

5 Plan to Conduct OCTAVE-S (Activity S0.4)

You must plan for OCTAVE-S as you would plan for any project in your organization. An analysis team must work as a group during each OCTAVE-S activity, requiring each individual to set aside sufficient time for completing each evaluation activity.

5.1 Scheduling Considerations

You will find the *OCTAVE-S Checklist* in the appendix of this document. It consists of a collection of entry/exit criteria for each process, including preparation. The checklist comprises the following sections for each process:

- Entry Criteria – These are the items that a team should complete prior to starting a process.

- Skills Required – This area of the checklist documents the types of skills that the analysis team should have. This guidance can help a team determine whether it needs to augment its skills for any given activity.

- Participants – The participants required for each process must be identified before the evaluation. Participants typically include only analysis team members. However, supplemental personnel can be selected to augment the analysis team's skills for any given process.

- Time Estimates – This area of the checklist provides a range of time estimates for completing each activity. The low end of the range provides an estimate of how long it would take someone with expertise in security and OCTAVE-S to complete that activity. The high end of the range provides an estimate of how long it would take less experienced practitioners to complete that activity.

- Exit Criteria – These are the items that a team should complete during a process.

During planning, you develop a schedule for the evaluation. You should review the information in the checklist for each process as you develop the overall plan for the evaluation. During planning, you must

- decide when the team will conduct each OCTAVE-S process

- decide whether additional personnel will be required for any processes or activities

- determine how much preparation time will be required for each process

- estimate the time required to complete each process (for both experienced and inexperienced teams)

When developing the project plan, you need to consider how familiar team members are with the OCTAVE-S process, information security, and operational risk management. Teams attempting to conduct the evaluation for the first time should reference times for inexperienced teams to avoid building an overly optimistic schedule.

OCTAVE-S is conducted using a series of meetings; the schedule for conducting those meetings is quite flexible. The shortest possible timeframe for completing an entire evaluation is approximately two days. This estimate assumes a full-time, dedicated analysis team that is experienced with the process and an evaluation that is narrowly scoped (e.g., for one to two operational areas). Practical constraints can extend the calendar time required to conduct OCTAVE-S. When scheduling evaluation activities, you should

- consider any organizational constraints

- allocate sufficient time to complete all preparation activities

- remember that all plans are estimates

- revise the project plan to reflect appropriate changes

5.2 Tailoring OCTAVE-S

During planning, a team must also determine the extent to which it will tailor OCTAVE-S to best meet the organization's needs. Section 7 provides a discussion of the tailoring options that can be considered. Depending upon the nature of the tailoring, the team could invest a considerable amount of time to update activities and artifacts before beginning the evaluation. Make sure you investigate the depth of tailoring you want to do before your plan and schedule are finalized.

5.3 Guidance for Developing a Project Plan for OCTAVE-S

You should document your project plan for conducting OCTAVE-S according to the practices and standards required by your organization. There is no standard worksheet or template provided for you to document the project plan for conducting OCTAVE-S in your organization.

As you develop your plan, review the information on the *OCTAVE-S Checklist*. Pay particular attention to

- whether additional personnel will be required for any processes or activities

- how much preparation time will be required for each process

- the time estimates for each process

For each process determine

- when it will occur

- who will participate

- any potential constraints or risks

Make sure that all team members agree to the plan's content. You may also need senior management review and approval of the plan before proceeding. At this point, you should be ready to start the evaluation.

6 Prepare to Conduct Each OCTAVE-S Process (Activity S0.5)

One key to conducting an effective evaluation is ensuring that the team is prepared for each evaluation activity. Preparation includes

- being ready to conduct each process

- ensuring that all logistics have been addressed

6.1 Preparing to Conduct a Process

Before starting any OCTAVE-S process, the analysis team must ensure that all entry criteria for that process have been completed. Completing these criteria indicates that the team is ready to start the process. In addition, analysis tem members must understand their roles and how to perform the activities required by the process.

If any supplemental members (i.e., people providing unique skills, experience, and expertise required by a process) are selected to augment the analysis team's skills, those participants must also understand their roles and the OCTAVE-S process in which they will participate.

Finally, team members must agree upon an approach for making decisions that is understood by all participants in a process. Doing this provides an unambiguous way for the team to resolve any conflicts and make decisions.

6.2 Addressing Logistics

The steps for coordinating logistics are straightforward and easy to understand, but they can present some of the bigger obstacles that you will face during the evaluation. Logistics includes scheduling workshops, making sure that equipment is available for meetings, and coordinating the schedules of team members.

One member of the analysis team should be the focal point for coordinating logistics for conducting OCTAVE-S. Be sure to consider the following types of items when you address evaluation logistics:

- Reserve rooms for all workshops.

- Ensure that any required equipment (e.g., overhead projectors, flip charts) is available.

- Allow time to complete all preparation activities.

- Address any unexpected events, such as scheduling additional meetings and notifying any supplemental personnel of meeting times and locations.

6.3 Guidance for Preparing for OCTAVE-S Process

Review the information on the *OCTAVE-S Checklist* for the process that you are about to conduct. The logistics coordinator for the team should reserve a meeting room and ensure that all participants know the time and location of the meeting. Any equipment required for the meeting should be signed out and ready to use by the team.

Review all entry criteria as you prepare to begin a process to ensure you have met them. The entry criteria for a process indicate the extent to which a team is ready to begin that process. If any criteria have not been completed, ensure that you address them before starting that process.

Ensure that all core analysis tem members understand their roles as well as how to perform the activities required by the process. Contact any supplemental personnel who have been selected to augment the analysis team's skills prior to the meeting. Ensure that all additional personnel understand their roles as well as the activities in which they will be participating.

Finally, select an approach for decision making (e.g., consensus, majority voting, multi-voting) and ensure that all team members understand the approach. This provides an unambiguous way in which the team will resolve any conflicts and make decisions. Note that this could be the same approach used for all processes or it could vary depending upon the process.

At this point, you should be ready to conduct the process. The last topic that is addressed in this document is a brief discussion of tailoring considerations.

7 OCTAVE-S Tailoring

An analysis team determines the extent to which it will tailor OCTAVE-S during planning. The ideas presented in this section provide a few tailoring options for OCTAVE-S, not an exhaustive list. As you read this section, you should think about your organization's unique needs and which aspects of the method you need to adjust to meet those needs. There are two optional tasks in OCTAVE-S for which an analysis team *must* make tailoring decisions: probability and approval for evaluation results. Those issues are addressed first.

7.1 Probability

Probability is the likelihood that an event (i.e., threat) will occur. Estimating the probability for each active threat is considered to be optional in OCTAVE-S. For information security risks, probability is a more complex and imprecise variable than is normally found in other risk management domains, because risk factors are constantly changing. Probability is highly subjective in the absence of objective data and must be used carefully during risk analysis.

A qualitative version of probability is provided with OCTAVE-S. It depends upon your analysis team's ability to estimate the motive and history of different types of attacks or threats. You should review the *Risk Profile* worksheets in Volumes 5-8 to determine if you intend to use probability.

If you do choose to use probability, you should remember that the decision-making process of OCTAVE-S relies primarily on impact. You use impact to decide whether to mitigate or accept a risk. Probability, when used, helps determine which mitigation plans to implement first. You must determine the extent to which you will incorporate probability in your decision making.

For example, you might use scarce resources to address a medium-impact, high-probability risk in the near term. Later on, you might be able to free up enough resources to address a medium-impact, medium-probability risk. In this case, you are using probability to refine your priorities by determining *when* to implement mitigation plans. You are not using probability to drive the decision of whether to accept or mitigate the risk.

7.2 Approval of Evaluation Results

Depending on the composition of the analysis team and the degree to which it was empowered, the organization's senior managers might need to approve the results of the evaluation before any formal action is undertaken to implement those results.

For example, the analysis teams from the OCTAVE-S pilot organizations included representation from the organization's senior management. The managers on the team had the authority to approve all mitigation plans. However, if a team does not have such authority, it must determine how to present the results of OCTAVE-S to senior managers for their approval. This likely will require an additional meting with the organization's senior managers after the end of Process S5. This approach has proven to be effective for organizations that have conducted the OCTAVE Method.

7.3 Other Tailoring Activities

Other tailoring activities should be undertaken at the discretion of the analysis team. You should be aware that since OCTAVE-S worksheets are highly structured, tailoring is not always a simple proposition. The remainder of this section examines some potential items you might want to modify as you implement OCTAVE-S in your organization.

7.3.1 Catalog of Practices

The catalog of practices is a general catalog of accepted security practices. OCTAVE-S tightly integrates the catalog of practices with the following artifacts:

- Security practices survey – The practices in the survey are derived from the catalog of practices.

- Protection strategy – The content of the protection strategy used in OCTAVE-S is abstracted from the catalog of practices.

- Mitigation plan – Suggestions for potential mitigation activities were derived from the catalog of practices.

If you must comply with a specific standard of due care (e.g., HIPAA), you can modify the catalog to ensure that it addresses the range of practices in the standard. You can add specific practices unique to your domain or remove practices that are not relevant. You can also modify the catalog to make it consistent with the terminology used in your domain. The goal is to *have* a catalog of generally accepted, good security practices against which you can evaluate your current security practices. The catalog must be meaningful to your organization. If you modify the catalog of practices, you must ensure that all artifacts derived from the catalog are also modified in an appropriate manner.

7.3.2 Generic Threat Profile

Before you start OCTAVE-S, you can tailor the generic threat profile to meet your evaluation needs. As a general guideline, make sure that your organization's threat profile addresses the range of threats known to affect your operational environment. When tailoring the generic threat profile, you can

- add a new threat category

- add new threats to an existing category

- delete inapplicable threats from a category

- "decompose" or add depth to a threat category

For some organizations, the standard categories are sufficient. Other organizations might require additional categories of threat. Threat categories are contextual and are based on the environment in which an organization must operate. The standard categories are a good starting place. As you implement OCTAVE-S, you may start identifying unique threats that require the creation of new threat categories.

The following example addresses tailoring of the threat actors for the *Human Actors Using Network Access* category of threat. The basic threat tree for this category focuses on two types of threat actors: actors inside the organization and actors outside the organization. Depending on the evaluation needs of an organization, this classification of actors could be too broad. For example, an organization that deals with national security issues would probably want a more detailed classification of threat actors. The following list is an expanded classification of threat actors:

- non-malicious employees – people within the organization who accidentally abuse or misuse computer systems and their information

- disgruntled employees – people within the organization who deliberately abuse or misuse computer systems and their information

- attackers – people who attack computer systems for challenge, status, or thrill

- spies – people who attack computer systems for political gain

- terrorists – people who attack computer systems to cause fear for political gain

- competitors – people who attack computer systems for economic gain

- criminals – people who attack computer systems for personal financial gain

- vandals – people who attack computer systems to cause damage

The asset-based threat profile could be modified to include the above classifications and more detailed motives. In addition, other forms of tailoring can be applied to add detail to the access paths. Separate trees could be created for different means of network access or for

different means of physical access. If tailored in this manner, the trees do become more complicated, and the additional detail could make the subsequent analysis more complex. For many organizations, the generic set of trees will be sufficient.

7.3.3 Asset Categories

Asset categories are contextual for any organization and must be defined in order to conduct a meaningful evaluation. The categories considered in OCTAVE-S are

- systems

- information

- applications

- people

You can tailor the list by adding or deleting categories to meet your organization's needs. If you add asset categories, you must also tailor all critical-asset-specific worksheets for consistency with the new asset categories.

7.3.4 Security Requirements Categories

The categories of security requirements are contextual for any organization and must be defined in order to conduct a meaningful evaluation. The categories considered in OCTAVE-S are

- confidentiality

- integrity

- availability

You can tailor the list by adding or deleting categories to meet your organization's needs. For example, some organizations might want to add authenticity and/or non-repudiation to their list of security requirements. First, you need to decide what categories of security requirements you will incorporate into the evaluation, and then you need to use those categories consistently throughout all activities. You must add corresponding outcomes to the generic threat profile for any categories of security requirements you add. For example, the outcome associated with *confidentiality* is *disclosure*.

7.3.5 Impact Evaluation Criteria

Impact evaluation criteria are a set of qualitative measures against which an analysis team determines the extent of the potential impact on an organization resulting from each threat. Impact evaluation criteria define high, medium, and low impacts for an organization. These criteria are highly contextual. For example, while $1,000,000 may be a high impact to one

organization, it could be only a medium or low impact to another. Also, some organizations will have risks that result in a loss of life, but this is not true for all organizations. The contextual nature of evaluation criteria is the reason why every organization must define its own criteria.

An analysis team evaluates impact across multiple categories, or impact areas. These areas are related to an organization's mission and business objectives. The standard set of areas considered in OCTAVE-S is

- reputation/customer confidence

- safety/health issues

- fines/legal penalties

- financial

- productivity

- other

The impact areas are contextual and should be tailored to meet the needs of your organization. Before you conduct an evaluation, you should determine which impact areas to consider. One way to determine unique areas for your organization is to consider your organization's business objectives and make sure that impact areas are linked to your key business objectives. For example, a military organization may add combat readiness as an area of impact.

7.3.6 Worksheets

Any OCTAVE-S worksheet can be modified to suit the particular needs or standards of an organization or domain. Worksheets can be combined, split apart, and rearranged to be more efficient or adaptable to a particular database or other automated tool. Formatting and other types of simple "look-and-feel" changes will generally have little effect on the processes themselves. However, moving pieces of information from one worksheet to another or other content types of changes can be more difficult to make. Analysis teams should look for dependencies between worksheets in terms of information flow as well as other cascading effects that could be the result of content changes.

Appendix: OCTAVE-S Worksheets

This appendix contains the following worksheets that are used during preparation for OCTAVE-S:

- Preparation worksheet – This worksheet is used to help guide the selection of analysis team members and to set the scope of the evaluation.

- OCTAVE-S checklist – The entry/exit criteria are used to help the analysis team develop its project plan for the evaluation. They are also used as the team prepares to conduct each process to ensure that all entry criteria for that process have been met, that all personnel understand their roles as well as the activities they will be conducting, and that all logistics for the process have been addressed.

Preparation Worksheet

Description: *Selecting an analysis team for OCTAVE-S requires you to identify people who have broad knowledge of business processes and how the computing infrastructure supports those processes.*

Select analysis team members for the following:

A. business-related areas

B. information technology department

Directions are provided for each part.

A. Business-Related Areas

Directions: *1. Consider the two questions below when selecting analysis team members from the business units.*

Questions

1.   Who from your organization has broad insight into how systems and information are used to support the organization's business processes?

2.   Who from your organization has insight into organizational policies and processes?

B. Information Technology Department

Directions: *1. Consider the three questions below when selecting analysis team members from the information technology department.*

Questions

1.   Who from your organization has insight into how systems and networks are configured and maintained?

2.   Who from your organization has insight into your organization's computing infrastructure?

3.   Who from a contracting organization or service provider has insight into how systems and networks are configured and maintained *and* could participate in the evaluation?

A. Business-Related Areas

2. Select up to three business unit representatives for the analysis team.

Analysis Team Members

1. _____

2. _____

3. _____

B. Information Technology Department

2. Select up to three information technology representatives for the analysis team.

Analysis Team Members

1. _____

2. _____

3. _____

Description: *Setting the scope of OCTAVE-S requires you to complete the following:*

   C. Select key operational areas of the organization to participate in the OCTAVE-S evaluation.

   Directions are provided to guide the selection of operational areas.

C. Selecting Key Operational Areas

Directions: *1. Consider the three questions below.*

Questions

1. Which operational areas of your organization are most critical to achieving its mission?

2. Which operational areas would affect the organization's ability to function if those areas were unable to function?

3. In which operational areas do you believe information and/or systems are most at risk?

C. Selecting Key Operational Areas

2. Based on your answers to the questions, select up to five operational areas to assess in the evaluation.

Operational Areas

1. Information Technology Department

2. _____

3. _____

4. _____

5. _____

OCTAVE-S Checklist

OCTAVE-S Checklist

OCTAVE-S Preparation

Entry/Exit Criteria

Entry Criteria

- ☐ The organization's senior managers sponsor the OCTAVE-S evaluation and have allocated funds and staff for OCTAVE-S.

- ☐ A person in the organization is designated as the focal point for selecting analysis team members.

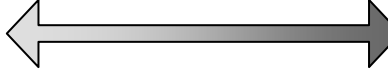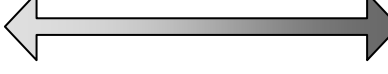**Skills Required for OCTAVE-S Preparation**

- ☐ An in-depth understanding of OCTAVE-S and the benefits it can provide

- ☐ Insight into the knowledge, skills, expertise, and experience of people throughout the organization who might serve as analysis team members

- ☐ The ability to work with senior managers and/or operational area managers to select analysis team members

- ☐ A broad understanding of the organization, its mission, and business objectives for setting the scope of the evaluation

- ☐ Knowledge of the organization's operational areas

- ☐ Project planning skills

- ☐ The ability to coordinate logistics for conducting the evaluation

- ☐ Good communication and presentation skills for building an awareness of OCTAVE-S

Analysis Team and Operational Areas

Core Analysis Team Members	Operational Areas Being Evaluated
Name	*Area*
_____	_____
_____	_____
_____	_____
_____	_____
Note: Designate specific roles if appropriate.	

OCTAVE-S Preparation

Entry/Exit Criteria (cont.)

OCTAVE-S Preparation Time Estimates

Activity		Estimated Time to Complete	
		Experienced Team	*Inexperienced Team*
S0.1	Obtain Senior Management Sponsorship of OCTAVE-S	1 hr	Never*
S0.2	Select and Train Analysis Team Members	3 days	1 week+
S0.3	Select Operational Areas to Evaluate	1 hr	1 day
S0.4	Develop Project Plan for Conducting OCTAVE-S	2 hr	4 hr+
S0.5	Prepare to Conduct Each OCTAVE-S Process	1 hr/process	4 hr+/process

Exit Criteria

❑ An analysis team for the organization has been selected. The team includes both business and information technology representation.

❑ At least one analysis team member has become familiar with OCTAVE-S through formal training or informal means.

❑ The scope of the evaluation has been decided – operational areas have been selected.

❑ A plan and approach for conducting OCTAVE-S has been developed, and it has been documented to the extent required by the organization.

❑ One member of the analysis team or some member of the organization has been assigned the responsibility for coordinating logistics for the evaluation.

❑ The analysis team has identified its preferred approach for decision making during the evaluation.

❑ The entry criteria for OCTAVE-S Process S1 have been met.

* Senior management sponsorship of OCTAVE-S is essential for a successful evaluation. If after using all available means you are unable to develop sponsorship from your organization's senior managers, you might want to consider discontinuing the evaluation.

Process S1: Identify Organizational Information
Entry/Exit Criteria

Entry Criteria

- ❑ All participants understand the activities and steps of Process S1.

- ❑ The analysis team has defined roles and responsibilities for Process S1.

- ❑ Additional people to augment the analysis team have been identified (if necessary).

Skills Required for Process S1

- ❑ A broad understanding of the organization's business environment and the information-related assets used by the organization

- ❑ An understanding of the organization's information technology environment

- ❑ Good communication skills

- ❑ Good analytical skills

Analysis Team Members

Core Team Members and Roles	Supplemental Team Members
Name *Role*	*Name* *Skill/Expertise*
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
Note: Designate specific roles if appropriate.	

Process S1: Identify Organizational Information

Entry/Exit Criteria (cont.)

Process S1 Time Estimates		
Activity	**Estimated Time to Complete**	
	Experienced Team	*Inexperienced Team*
S1.1 Establish Impact Evaluation Criteria	1 hr	3 hr$^+$
S1.2 Identify Organizational Assets	1 hr	3 hr$^+$
S1.3 Evaluate Organizational Security Practices	2 hr	6 hr$^+$
Total	4 hr	12 hr$^+$

Exit Criteria
❑ Impact evaluation criteria for the organization have been documented.
❑ Impact evaluation criteria are based upon the organization's unique operational environment and reflect the organization's business objectives.
❑ The analysis team received sufficient input from the organization's management when creating impact evaluation criteria, and/or the criteria have been approved by the organization's management.
❑ A set of information-related assets have been identified and recorded.
❑ The set of information-related assets includes representation from all operational areas being evaluated.
❑ The security practices survey has been completed, and a stoplight status has been assigned to each security practice area.
❑ The results of the security practices survey adequately reflect the current state of the organization's security practices.
❑ All action items have been documented.
❑ All relevant notes and recommendations have been documented.

Process S2: Create Threat Profiles

Entry/Exit Criteria

Entry Criteria

❑ Process S1 exit criteria have been completed.

❑ All participants understand the activities and steps of Process S2.

❑ The analysis team has defined roles and responsibilities for Process S2.

❑ Additional people to augment the analysis team have been identified (if necessary).

Skills Required for Process S2

❑ A broad understanding of the organization's business environment and the information-related assets used by the organization

❑ An understanding of the organization's information technology environment

❑ Good communication skills

❑ Good analytical skills

Analysis Team Members

Core Team Members and Roles		Supplemental Team Members	
Name	*Role*	*Name*	*Skill/Expertise*
_____		_____	
_____		_____	
_____		_____	
_____		_____	
_____		_____	
Note: Designate specific roles if appropriate.			

Process S2: Create Threat Profiles
Entry/Exit Criteria (cont.)

Process S2 Time Estimates

Activity		Estimated Time to Complete	
		Experienced Team	*Inexperienced Team*
S2.1	Select Critical Assets	1 hr	2 hr[+]
S2.2	Identify Security Requirements for Critical Assets	1 hr	6 hr[+]
S2.3	Identify Threats to Critical Assets	2 hr	12 hr[+]
	Total	4 hr	20 hr[+]

Exit Criteria

❑ Up to five of the organization's information-related assets have been designated as critical assets.

❑ The rationale for selecting each critical asset has been documented.

❑ Security requirements have been documented for each critical asset.

❑ The most important security requirement for each critical asset has been documented.

❑ A threat profile has been created for each critical asset.

❑ Each threat profile contains the following information:

  • a set of completed threat trees

  • specific examples of all active human-based threats

  • the strength of the motive (where applicable) and the associated confidence level

  • the history of each threat and associated accuracy estimate, and areas of concern where appropriate

❑   All action items have been documented.

❑ All relevant notes and recommendations have been documented.

Process S3: Analyze Computing Infrastructure With Respect to Critical Assets
Entry/Exit Criteria

Entry Criteria

☐ Process S2 exit criteria have been completed.

☐ All participants understand the activities and steps of Process S3.

☐ The analysis team has defined roles and responsibilities for Process S3.

☐ Additional people to augment the analysis team have been identified (if necessary).

Skills Required for Process S3

☐ A broad understanding of the organization's business environment and how business staff legitimately uses information technology in the organization

☐ A basic understanding of the organization's information technology environment and knowledge of the organization's network topology

☐ Good communication skills

☐ Good analytical skills

Analysis Team Members

Core Team Members and Roles		Supplemental Team Members	
Name	*Role*	*Name*	*Skill/Expertise*
_____		_____	
_____		_____	
_____		_____	
_____		_____	
_____		_____	
Note: Designate specific roles if appropriate.			

Process S3: Analyze Computing Infrastructure With Respect to Critical Assets

Entry/Exit Criteria (cont.)

Process S3 Time Estimates		
Activity	**Estimated Time to Complete**	
	Experienced Team	*Inexperienced Team*
S3.1 Examine Access Paths	1 hr 30 min	4 hr$^+$
S3.2 Analyze Technology-Related Processes	1 hr 30 min	4 hr$^+$
Total	3 hr	8 hr$^+$

Exit Criteria
❑ A system or systems of interest have been identified for each critical asset.
❑ Network access paths to the system(s) of interest have been examined for each critical asset with network-based threats. The following have been identified: key components, intermediate access points, internal and external access points, backup sites for information, and other systems that can access the system of interest.
❑ The party responsible for managing and securing each key class of components has been identified.
❑ The extent to which each key class of components is resistant to network attacks has been documented.
❑ Any additional, contextual information relevant to the infrastructure analysis is documented.
❑ All action items have been documented.
❑ All relevant notes and recommendations have been documented.

Process S4: Identify and Analyze Risks
Entry/Exit Criteria

Entry Criteria

❑ Process S3 exit criteria have been completed.

❑ All participants understand the activities and steps of Process S4.

❑ The analysis team has defined roles and responsibilities for Process S4.

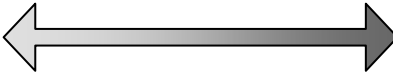❑ Additional people to augment the analysis team have been identified (if necessary).
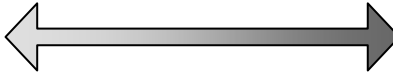
Skills Required for Process S4

❑ A broad understanding of the organization's business environment

❑ An understanding of the organization's information technology environment

❑ Good communication skills

❑ Good analytical skills

Analysis Team Members

Core Team Members and Roles		Supplemental Team Members	
Name	*Role*	*Name*	*Skill/Expertise*
_____		_____	
_____		_____	
_____		_____	
_____		_____	
_____		_____	
Note: Designate specific roles if appropriate.			

Process S4: Identify and Analyze Risks
Entry/Exit Criteria (cont.)

Process S4 Time Estimates

Activity	Estimated Time to Complete		
	Experienced Team		*Inexperienced Team*
S4.1 Evaluate Impacts of Threats	2 hr	⬅➡	10 hr[+]
S4.2 Establish Probability Evaluation Criteria (optional)	30 min	⬅➡	1 hr[+]
S4.3 Evaluate Probabilities of Threats (optional)	1 hr	⬅➡	8 hr[+]
Total	3 ½ hr	⬅➡	19 hr[+]

Exit Criteria

❑ Each active threat was assigned an impact value (high, medium, or low) for each applicable impact area based on the impact evaluation criteria defined for that area.

❑ Probability evaluation criteria for the organization have been documented (optional).

❑ Probability evaluation criteria were based upon a review of the known history of threats to the organization's critical assets (optional).

❑ Each active threat was assigned a probability value (high, medium, or low) and a confidence level for that probability value (optional).

❑ All action items have been documented.

❑ All relevant notes and recommendations have been documented.

Process S5: Develop Protection Strategy and Mitigation Plans
Entry/Exit Criteria

Entry Criteria

- ❑ Process S4 exit criteria have been completed.

- ❑ All participants understand the activities and steps of Process S5.

- ❑ The analysis team has defined roles and responsibilities for Process S5.

- ❑ Additional people to augment the analysis team have been identified (if necessary).
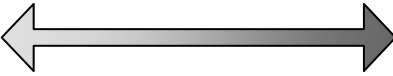
Skills Required for Process S5

- ❑ A broad understanding of the organization's business environment

- ❑ An understanding of the organization's information technology environment

- ❑ An understanding of the planning practices of the organization

- ❑ The ability to develop plans

- ❑ Good communication skills

- ❑ Good problem-solving and analysis skills

Analysis Team Members

Core Team Members and Roles		Supplemental Team Members	
Name	*Role*	*Name*	*Skill/Expertise*
_____		_____	
_____		_____	
_____		_____	
_____		_____	
_____		_____	
Note: Designate specific roles if appropriate.			

Process S5: Develop Protection Strategy and Mitigation Plans
Entry/Exit Criteria (cont.)

Process S5 Time Estimates

Activity		Estimated Time to Complete	
		Experienced Team	*Inexperienced Team*
S5.1	Describe Current Protection Strategy	1 hr	4 hr[+]
S5.2	Select Mitigation Approaches	30 min	6 hr[+]
S5.3	Develop Risk Mitigation Plans	2 hr	8 hr[+]
S5.4	Identify Changes to Protection Strategy	30 min	3 hr[+]
S5.5	Identify Next Steps	30 min	1 hr[+]
	Total	4 ½ hr	22 hr[+]

Exit Criteria

❑ The current protection strategy for the organization has been documented.

❑ The analysis team members agreed upon their decision-making factors for selecting mitigation areas.

❑ Up to three security practice areas were selected as mitigation areas.

❑ All risks that will be mitigated by the selected mitigation areas were designated as "mitigate" on all appropriate risk profiles.

❑ All risks that will *not* be mitigated by the selected mitigation areas were designated as "accept" or "defer" on all appropriate risk profiles.

❑ A mitigation plan was developed for each selected mitigation area.

❑ Changes to the protection strategy driven by mitigation plans are documented.

❑ Other changes to the organization's current protection strategy are supported by additional details documented in the appropriate mitigation plans.

❑ Next steps for implementing the results of the evaluation were documented.

❑ All action items were documented.

❑ Senior management approval of the evaluation results was obtained.

References

[Alberts 01]   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>.

[Berinato 02]   Berinato, Scott. "Calculated Risk." *CSO Magazine* (December 2002). <http://www.csoonline.com/read/120902/calculate.html>.

[Braithwaite 01]   Braithwaite, Timothy. "Executives Need to Know: The Arguments to Include in a Benefits Justification for Increased Cyber Security Spending." *Information Systems Security*, Auerbach Publications (September/October 2001):35-48.

[Gramm 01]   "Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness; Proposed Rule." *Federal Register*, vol. 65, no. 123 (June 2000): 39471-39489.

[HIPAA 98]   "Security Standards and Electronic Signature Standards; Proposed Rule." *Federal Register*, vol. 63, no. 155 (August 1998): 43242-43280.

[Oberndorf 00]   Oberndorf, Patricia.; Brownsword, Lisa.; Sledge, Carol. *An Activity Framework for COTS-Based Systems* (CMU/SEI-2000-TR-010, ADA385347). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2000. <http://www.sei.cmu.edu/publications/documents/00.reports /00tr010.html>.

[Proctor 03]   Proctor, Paul. "Talk the Talk, Walk the Walk: Five Tips to Win Friends and Influence C-level Execs in Your Organization." *Information Security Magazine* (February 2003). <http://www.infosecuritymag.com/2003/feb/talkthetalk.shtml>.

[SBQ 01]   *Secure Business Quarterly*, fourth quarter 2001. Cambridge, MA:
                               @stake, Inc. <http://www.sbq.com/sbq/rosi/index.html>.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this 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, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE January 2005	3. REPORT TYPE AND DATES COVERED Final
4. TITLE AND SUBTITLE OCTAVE-S Implementation Guide, Version 1.0, Volume 2		5. FUNDING NUMBERS F19628-00-C-0003
6. AUTHOR(S) Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213		8. PERFORMING ORGANIZATION REPORT NUMBER CMU/SEI-2003-HB-003
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116		10. SPONSORING/MONITORING AGENCY REPORT NUMBER
11. SUPPLEMENTARY NOTES		

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

13. ABSTRACT (MAXIMUM 200 WORDS)

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.

14. SUBJECT TERMS information security, risk management, OCTAVE	15. NUMBER OF PAGES 50
16. PRICE CODE	

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

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18 298-102