OCTAVE[SM] Method Implementation Guide Version 2.0

Volume 2: Preliminary Activities

Christopher J. Alberts
Audrey J. Dorofee

June 2001

Carnegie Mellon
Software Engineering Institute
Pittsburgh, PA 15213-3890

OCTAVE[SM] Method Implementation Guide Version 2.0

Volume 2: Preliminary Activities

Christopher J. Alberts
Audrey J. Dorofee

June 2001

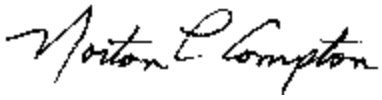
Networked Systems Survivability Program

This report was prepared for the

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

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

FOR THE COMMANDER



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

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

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

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

Table of Contents for Volume 2: Preliminary Activities

Overall Table of Contents for OCTAVE Method Implementation Guide

Introduction To Preliminary Activities

Before an Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE[SM]) can be conducted, there are preliminary activities that need to occur, or should occur. This volume provides materials to support those activities. In general, it is assumed that an internal champion and the analysis team would be involved in these activities. An internal champion is assumed to be someone who is interested, motivated, and influential enough to convince management to proceed with an OCTAVE. The following items are included in this section:

- **OCTAVE Method Preparation Guidelines**: the directions for preparing to perform an OCTAVE, including defining the overall schedule and plans for the workshops. These guidelines are to be used first by an internal champion to gain senior management sponsorship and select an analysis team. Once the analysis team is ready to proceed, they would use the guidelines to
  - facilitate setting the scope of the evaluation
  - facilitate the selection of participants from various levels of the organization
  - set the schedule for workshops and activities
  - coordinate logistics
- **Preparation Example Results**: an introduction to the example organization used in all of the example results as well as their preparation activities and decisions.
- **Tailoring Guidelines**: a set of guidelines for tailoring the overall evaluation to your organization as well as a summary of the possible process tailoring.
- **Senior Management Briefing**: The internal champion can use this briefing to gain senior management sponsorship and, as needed, to brief those involved in preparation. This briefing contains an overview of the OCTAVE Method as well as general descriptions of the resource and time requirements.
- **Participants Briefing**: The analysis team can use this briefing to familiarize all of the OCTAVE participants about the method and their roles in the evaluation. This briefing contains a general description of the OCTAVE Method and should be supplemented with the actual schedule of activities and assignments of personnel.

The following table lists the entry and exit criteria for OCTAVE Preparation, a suggested temporal flow of events or activities, and a checklist for the types of skills needed by the analysis team for these activities. The entry/exit criteria can be used by the analysis team to check their progress. Note

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

that, in some cases, the person or group doing the activities at this early stage may be the champion or a group of managers.

OCTAVE Preparation

Entry/Exit Criteria

Entry Criteria

❑ Senior management sponsorship of OCTAVE exists (OPR.1).

❑ Analysis team members have been identified (OPR.2).

Analysis Team Skills

Skills Required for OCTAVE Preparation	Analysis Team Members and Roles	Additional People to Augment the Analysis Team
• good communication skills • understanding of the organization's business environment • ability to develop plans and schedules	_____ _____ _____ _____ _____ logistics coordinator _____	_____ _____ _____ _____ _____

Suggested Temporal Flow of Events	Suggested Time Span
• Gain senior management sponsorship	• 1-2 hour briefing and discussion
• Select analysis team	• 1-2 hour discussion
• Train analysis team	• 2-3 days for training or 1 week for familiarization
• Select senior managers for Process 1 • Scope evaluation (select operational areas) • Select operational area managers • Select general and IT staff	• 2-3 hour meeting
• Set schedule	• 3-4 hours, spread out over a few days
• Brief all participants	• 1-2 hour briefing

OCTAVE Preparation **Entry/Exit Criteria (cont.)**
Exit Criteria
❑ Analysis team members understand the OCTAVE Method (OPR.3).
❑ Senior managers and the analysis team have selected operational areas to participate in OCTAVE (OPR.4).
❑ Senior managers, operational area managers, and the analysis team have selected participants for the process (OPR.5).
❑ The analysis team has developed a detailed schedule for OCTAVE (OPR.6).
❑ Participants have been briefed about OCTAVE and understand their roles in the evaluation (OPR.7)

Note: The numbers in parentheses are references to specific inputs, outputs, worksheets, or activities as defined in the OCTAVE Data Flow in Appendix B, Volume 16. For example, (OPR.4) is the fourth output of Preparation.

OCTAVE Method Preparation Guidelines

The Preparation Guidelines can be used by the organization's managers and the analysis team in preparing to do an Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). This section reflects the most probable scenario for preparation. It is assumed that the analysis team does **not** exist prior to gaining senior management approval and that there is a champion – someone internal to the organization with an interest in seeing the OCTAVE Method implemented.

Contents

1 Introduction

The Preparation Guidelines can be used by the organization's managers and the analysis team in preparing to do an Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). It also provides a convenient place to document all of the participants, team members, and logistics. There are many ways that the OCTAVE Method can scoped and be implemented. These guidelines reflect the most probable scenario for preparation. OCTAVE Method activities are led by an interdisciplinary analysis team whose members are from the organization being assessed. However, before the evaluation is performed, senior management sponsorship must be gained, the evaluation needs to be scoped, and personnel need to be selected. It is assumed, for the purposes of these guidelines, that the analysis team does **not** exist prior to gaining senior management approval. It is also assumed that there is a champion – someone internal to the organization with an interest in seeing the OCTAVE Method implemented. The champion should be willing to do the initial work of gaining senior management understanding and sponsorship. This is just one scenario, obviously, your experience may be different. It can be safely assumed, however, that all of these activities need to be done.

This section will help organizations prepare for each phase of OCTAVE and assist the champion and the analysis team in performing the up-front preparation and selection of personnel. It is divided into three main parts:

- **Sponsorship** (Section 2) – Gain senior management sponsorship for the OCTAVE Method. This activity is likely done by a champion.
- **Preparation** (Section 3) – Select the analysis team, scope the evaluation, and select personnel. These activities are usually done by senior and mid-level managers, and the analysis team.
- **Logistics support** (Section 4) – Schedule the workshops and handle the equipment requirements. These activities are usually done by the analysis team's logistics coordinator.

These Preparation Guidelines can be used to help you schedule the evaluation before you get started in the actual process. The champion and the analysis team should both use this guide. Some coordination or hand-off of responsibility between the champion and the analysis team will occur once the analysis team is ready to go.

Note that OCTAVE is organized into a series of workshops; therefore some logistics and scheduling support is also required. It is the analysis team's responsibility to ensure that this is done, whether by someone on the team or by another person with logistics responsibility. Logistics support information for all activities, including preparation, is provided in this guide.

2 Obtain Senior Management Sponsorship of OCTAVE

At some point, someone within the organization will decide that OCTAVE is needed. For the purposes of this guide, this person is referred to as the champion. The specifics about who makes this decision and how it is made will vary with each organization and situation; they are not covered here. The primary point made in this guide is that senior management must sponsor the activity. In order for that to occur, the appropriate senior managers must be aware of the evaluation process, the expected outcomes, and what commitments of time and personnel must be made. Senior managers could be a chief executive officer, a director, a governing board, or anyone high enough in the organization to commit the organization and its resources to this effort.

Before starting an OCTAVE, senior managers must be convinced to support it. Several methods can be used to achieve early buy-in, which is necessary to start any type of preparation and scheduling. The Senior Manager's Briefing slides, provided later in this volume, can be used for that purpose. Other materials, such as the Complete Example Results in Appendix C (Volume 16), can also be used. The individual trying to get OCTAVE started will need to pull together the necessary materials and brief the appropriate senior manager(s) to get their approval.

A typical schedule for an OCTAVE is provided later in this guide, in Section 4.0. The requirements for personnel and rough estimates of staff time can also be used to help senior managers understand what they will be supporting. These guidelines can also be used in acquiring sponsorship.

Sponsorship implies the following:

- visible, continued support of the OCTAVE activities
- active encouragement of staff participation
- delegation of responsibility and authority for accomplishing all OCTAVE activities
- commitment to allocate the necessary resources
- agreement to review the results and decide on appropriate actions

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

3 Preparation

Preparation can be done in one or more meetings, usually with senior managers in attendance or providing oversight. The order of activities provided here is but one example of how events can proceed. You may need a different order of activities to accommodate your particular circumstances.

Once sponsorship is acquired, the analysis team should be selected and trained. The analysis team will then lead the remaining activities to determine the exact scope of the evaluation and to help select the participants. Senior management and operational area managers will be involved to provide scoping direction and to assist in the selection of personnel. Finally, all participants should be briefed about what will be happening and what their roles will be.

3.1 Select Analysis Team Members

The first step is the selection of the interdisciplinary analysis team, who will be responsible for carrying out most of the activities during OCTAVE. The core analysis team should consist of three to five personnel, selected from the various operational areas in the organization as well as from the Information Technology (IT) Department. Supplemental team members, such as an operational area manager or a vulnerability assessment tool expert, may be added to particular workshops as needed to provide additional skills. Logistics support can be accomplished by one of the core team members, or an additional person can be assigned to the team for that specific purpose.

The analysis team will lead the scoping and personnel selection, facilitate the initial set of workshops, and gather and analyze information. This team will also be responsible for performing or helping with vulnerability evaluations of selected infrastructure components, and for developing protection strategies for the organization and mitigation plans for information security risks.

Overall, the analysis team needs to

- include between three to five people in the core group
- represent both business/mission and IT perspectives
- have knowledge of the business and IT processes
- have good communication and facilitation skills
- be committed to the effort

3.1.1 Analysis Team Roles and Responsibilities

The roles and responsibilities of the analysis team are to

- work with managers to scope the evaluation, select participants, and schedule OCTAVE activities
- coordinate with senior and operational area managers and IT support for vulnerability evaluations
- gather, analyze, and maintain data and results during the OCTAVE process
- enable the assessment activities. One of the major functions is to ensure that designated personnel attend their specific workshops.
- provide logistics support (See Section 3.1.4 and Section 4 for details.)

3.1.2 Skill Requirements for the Analysis Team

OCTAVE is a complex process. However, it does not require extensive or unique skills on the part of the analysis team. OCTAVE is not a typical vulnerability evaluation, focused on technological aspects with heavy automated tool use. It is much closer to a typical business process or management evaluation, since it involves gathering information from personnel and the technological infrastructure and analyzing both. So it is helpful if someone on the analysis team is familiar with or has done assessments or evaluations. Although audits are usually looking strictly for compliance with regulations or standards, familiarity with those might also be helpful. For the IT member of the analysis team, some familiarity with the realities of security is needed. This should not be someone who believes any one tool or firewall is the silver bullet that solves all security problems. The IT representative needs to have a more pragmatic viewpoint – they don't have to understand all aspects of security, just be able to see their own limits and look for more expertise as needed.

The specific skills needed for each OCTAVE process are detailed in the Process Guidelines. Refer to these to determine when it may be necessary to supplement the skill base of the core analysis team. (See Table 1 for a summary.) In general, the skills required for the core members of the analysis team are

- facilitation skills
- good communication skills
- good analytical skills
- ability to present to and work with senior managers, operational area managers, and staff
- understanding of the organization's business environment
- understanding of the organization's information technology environment and how the business staff legitimately uses information technology in the organization

In addition, at different times, the core team will need to have the following skills or should be able to acquire them through supplemental team members:

- understanding of the organization's information technology environment and knowledge of the organization's network topology
- understanding of common exploits of technology vulnerabilities
- knowledge of how to interpret the results of vulnerability evaluation software tools
- understanding of the organization's planning practices
- ability to develop plans

Table 1 lists the skills needed for each process. In addition, it can be used as a checklist to help select core and supplemental analysis team members.

Table 1: Analysis Team Skills Required for Each Process

Process	**Skills Required**
Preparation	• good communication skills • understanding of the organization's business environment • ability to develop plans and schedules
Process 1	• facilitation skills • ability to present to and work with senior managers
Process 2	• facilitation skills • ability to present to and work with operational area managers
Process 3	• facilitation skills • ability to present to and work with general and IT staff
Process 4	• understanding of the organization's business environment • understanding of the organization's information technology environment • good communication skills • good analytical skills
Process 5	• understanding of the organization's business environment and how business staff legitimately uses information technology in the organization • understanding of the organization's information technology environment and knowledge of the organization's network topology • good communication skills • good analytical skills • understanding of the common exploits of technology vulnerabilities

Table 1: Analysis Team Skills Required for Each Process (cont.)

Process	Skills Required
Process 6	• understanding of organization's information technology environment and knowledge of the organization's network topology • understanding of common exploits of technology vulnerabilities • knowledge of how to interpret the results generated by vulnerability evaluation software tools • good communication skills • good analytical skills
Process 7	• understanding of the organization's business environment • understanding of the organization's information technology environment • good communication skills • good analytical skills
Process 8, Workshop A	• understanding of the organization's business environment • understanding of the organization's information technology environment • understanding of the planning practices of the organization • ability to develop plans • good communication skills • good analytical skills
Process 8, Workshop B	• facilitation skills • ability to present to and work with senior managers • good communication skills • good analytical skills

3.1.3 Logistics Support

The analysis team will have logistics to coordinate. One person should take the lead for coordinating logistics. This person can be a part of the core team or someone outside the analysis team. The logistics coordinator should be familiar with the organization, be familiar with the culture of the organization, be able to commit to the time required for this role, and be authorized to make things happen. This includes

- coordinating meeting rooms, viewgraph projectors, etc.
- scheduling all meetings
- handling unexpected events such as scheduling additional meetings and/or substituting personnel in meetings

3.1.4 Estimated Time Requirements for Analysis Team Members

Table 2 summarizes the time commitments needed for the analysis team. See Section 3.4 for time requirements of additional personnel who might be needed to supplement the analysis team. If any members of the core team members are involved in running the vulnerability evaluation tools, they may need to spend one or more days running the tools and analyzing the results.

Table 2: Estimated Time Requirements for the Analysis Team

Processes	Staff	Estimated Time Requirement
All	Core Members	• 1 to 2 days for preparation • 7 days for workshops (more if additional workshops are needed) • 2 - 4 days for work outside of the workshops • 1 - 5 days to run vulnerability tools • ½ day for wrap-up and briefing all participants
All	Logistics Coordination	• 2-3 hours per workshop for coordinating logistics and handling any issues during the workshop • being "on-call" or easily reached during the entire assessment

3.1.5 List the Analysis Team Members

Consider all of the above requirements and list the names of the analysis team members in Table 3. One person should also be responsible for scribing or making sure all information is recorded. If known, supplemental team members should also be listed.

Table 3: Core and Supplemental Analysis Team Members

Name	Title	Responsibility
Core Team Members		

Table 3: Core and Supplemental Analysis Team Members (cont.)

Name	Title	Responsibility
Supplemental Members		

3.1.6 Supporting Documentation and Information

Some of the following types of site documents or information can be used (if it exists) to help scope the assessment and can be a source of information to the analysis team during some of the workshops. If possible, the analysis team should collect this information before the workshops begin.

- organization chart that outlines responsibilities
- list of computing equipment
- software used (operating systems, major applications)
- network diagram/topology
- security policy documents
- security procedure documents
- architecture documents
- security training materials
- router configuration tables
- logs and audit data
- tool configurations
- security newsletters
- list of available vulnerability evaluation tools/checklists/scripts for
  - operating systems
  - applications
  - physical security

3.2 Train Analysis Team

This guide assumes that the analysis team will be trained prior to the assessment or will have sufficient time to become familiar and comfortable with these materials. Training can be obtained from an internal or external source, or, at a minimum, the analysis team can use the OCTAVE Method Implementation Guide to learn "as they go." While all of the materials required to carry out the

OCTAVE Method are contained in the OCTAVE Method Implementation Guide, some tailoring may be required and team members may want to practice the activities before facilitating the workshops. In general, training in the method will take about three days, assuming training involves actually performing most of the processes as a team. If the team feels they can learn as they go, they should allow for a week to read and familiarize themselves with the material and practice using some of the worksheets or the Asset Profile Workbook. See also the section in the Volume 1 labeled "Analysis Team Training" for additional ideas on method training and tailoring.

3.3 Select Operational Areas to Participate in OCTAVE

In the spirit of targeted data collection, not all of the organization needs to be evaluated. Rather, key operational areas are selected for the evaluation. The analysis team should assist senior managers in deciding which operational areas are to be examined during OCTAVE. The following are rough guidelines for choosing operational areas. However, management should use its own judgment in selecting areas. The Senior Management Briefing slides can also be used to help with this activity.

- At least four operational areas are generally recommended, one of which **must** be the Information Technology (IT) or Information Management (IM) Group.
- Select a broad cross-section of operational areas.
- If the IT or IM Group is dispersed, or managed as separate support groups, select a cross section of those groups.
- Select operational areas that reflect the primary operational or business functions as well as the important support functions of the organization.
- Consider areas that are remote in location or different in terms of the type of work or support they need.
- Consider the time commitment necessary by the personnel in that area and any critical operations that may occur during OCTAVE.
- Consider areas that require *electronic* information to accomplish their functions.

Given the guidelines above, use Table 4 to list the selected operational areas. Also consider the questions in this table when selecting the key operational areas.

Table 4: Selected Operational Areas

Key Operational Areas	
Question	**Notes**
What areas of your organization are critical to achieving the mission of your organization?	
Have you considered your entire organization, including support functions? What additional areas are critical?	
Which areas would you like to participate in the risk assessment? Note: The Information Technology (IT) Group must, by default, participate in the assessment. You should select three additional operational areas. Optionally, additional areas can be selected if you believe you need them to adequately scope OCTAVE.	1. 2. 3. 4. (IT) 5. (optional) 6. (optional) 7. (optional)

3.4 Select Participants

The analysis team leads this activity, which will likely occur in more than one session. Senior managers select the operational areas and appropriate managers, and those operational area managers select participants from among their staff. Table 5 provides a summary of the participants for each activity in OCTAVE and the estimates for their time. In most cases, the people participating in Processes 1, 2, and 3 can provide the supplementary support to the analysis team in other processes. For example, one of the IT staff members from Process 3 could be the supplemental analysis team member for Processes 5, 6, and 8. The sections after the table provide additional guidance and a place to document the selections. The time required for running the vulnerability evaluation tools is only an estimate. The actual time will depend entirely upon the number of components selected for evaluation, the nature of the tools used, and the ability of the team to schedule time for running those tools.

Table 5: Participants in OCTAVE

Type of Participants	Participate In	Estimated Time	Notes
At least 3 senior managers	Process 1 Process 8, Workshop B	½ day up to a ½ day	
At least 4 operational area managers, including IT. From these, you may want to further select:	Process 2	½ day	
• 1 operational area manager (optional) • 1 operational area manager (optional)	Process 7 Process 8, Workshop A	1 day 1 day	Optional: to supplement the analysis team Optional: to supplement the analysis team
3-4 staff members from each operational area. In addition, you may need to select:	Process 3	½ day	
1 staff member (optional) 1 staff member (optional) 1 staff member (optional)	Process 4 Process 7 Process 8	1 day 1 day 1 day	Optional: to supplement the analysis team
3-4 members from IT. In addition, you may need to select:	Process 3	½ day	
1-3 IT staff members (optional) 1-2 IT staff members (optional) 1-3 IT staff members (optional)	Process 5 Process 6 Process 8, Workshop A	½ day ½ - 1 day ½ - 1 day	Optional: to supplement the analysis team in selecting key infrastructure components, running vulnerability assessment tools, and helping with risk mitigation plans

3.4.1 Select Senior Managers

The analysis team will coordinate this activity. The senior managers who originally sponsored OCTAVE should also decide who amongst them should participate in the Process 1 workshop. They will identify important information assets, the threats to those assets, the security requirements of the assets, the current protection strategy, and organizational vulnerabilities. At least three senior managers are needed who

- are familiar with the types of information assets used in your organization
- are able to commit to the time required for this assessment
- have the authority to select and authorize time for operational area managers
- preferably, have been in their role for at least a year

Senior managers in your organization will be asked to contribute the following amount of time:

- ½ day to attend a senior management workshop in Process 1
- ½ day to review and approve the protection strategy and risk mitigation plans in Process 8, Workshop B

Record the names of the senior management participants in Table 6. As you consider who might be appropriate, keep in mind those assets and functions believed to be critical to the organization.

Table 6: Senior Management Participants for Processes 1 and 8

Name	Title	Responsibility

3.4.2 Select Operational Area Managers

The analysis team will coordinate this activity. Senior managers will select managers from the previously selected operational areas to participate in the workshops. Operational area managers are needed to identify important information assets, the threats to those assets, the security requirements of the assets, the current protection strategy, and organizational vulnerabilities. There is usually only one operational area manager workshop (Process 2), although additional workshops can be held if needed. At least four operational area managers, including the IT manager, are needed. Select those who

- have key responsibilities for the selected operational areas
- are familiar with the types of information assets used in your organization
- are familiar with the ways in which these information assets are used
- are able to commit to the time required for this assessment
- preferably, have been in their role for at least a year
- have the authority to select and authorize time for staff members

Operational area managers in your organization will need to contribute the following amount of time:

- ½ day to attend the operational area managers workshop in Process 2
- for selected operational area managers, up to one additional day to participate in risk analysis (Process 7) and protection strategy development (Process 8, Workshop A). This is optional,

but recommended if the analysis team wants to add someone with experience in developing organization-level plans.

Select the managers who will represent the operational areas and list them below in Tables 7 and 8. As you consider who might be appropriate, keep in mind those assets you believe to be critical to your organization.

Table 7: Operational Area Management Participants for Process 2

Name	Title/Operational Area	Responsibility

Table 8: Optional Operational Area Management Participants for Processes 7 and 8

Name	Title/Operational Area	Responsibility

3.4.3 Select Staff Members

Each of the operational area managers must select three to four key staff members from their areas to participate in the Process 3 workshops. They will identify important information assets, the threats to those assets, the security requirements of the assets, the current protection strategy, and organizational vulnerabilities. There should be at least three workshops involving staff – two for general staff and one for IT staff. Depending upon the number of operational areas selected, you may need more than two workshops for general staff. You should try to keep workshop participants to five staff members. If there are more than five, it will be difficult for all of them to participate actively and some may feel too overwhelmed to contribute. Higher numbers of participants can also be difficult to manage for a new analysis team.

Other staff may be needed to supplement the skills of the analysis team during the rest of the processes. Refer to the specific time requirements in Table 5 for these personnel, and list the ones you can identify in the table below.

3.4.3.1 Staff Members from Each Operational Area

List in Table 9 at least three to four people from each selected operational area who

- are familiar with the types of information assets used in their area
- are familiar with the ways in which the information assets are used
- are able to commit to the time required for this assessment
- preferably, have been in their role for at least a year

Table 9: Staff Participants for Process 3

Name	Title/Operational Area	Responsibility

3.4.3.2 Optional Staff Members

Additional members of the general staff may be needed to supplement the knowledge or skills of the analysis team during Processes 4, 7, and 8. During Process 4, additional help in performing the gap analysis on asset-based threat profiles might be needed. Record their names in Table 10 if known at this point. It is also possible that these individuals will be identified only after critical assets are

selected. They can then be brought in for a very short time to look at a particular asset. In Processes 7 and 8, additional help may be needed for analyzing risks, defining evaluation criteria, or developing mitigation plans. You may also find that you need to revisit this list as you progress.

Table 10: Optional General Staff Members

Process 4: Create Threat Profiles		
Name	**Title**	**Responsibility**
Process 7: Conduct Risk Analysis		
Name	**Title**	**Responsibility**
Process 8, Workshop A: Build Protection Strategy		
Name	**Title**	**Responsibility**

The technology evaluation will likely require additional IT staff commitment or external representatives to support the analysis team. They will help identify key components of the computing infrastructure and examine them for technology vulnerabilities. They may also assist in the analysis of the vulnerability assessment results. The IT manager should make these staff selections with assistance from the analysis team. Table 11 can be used to record their names. The selected staff should be

- familiar with the types of information assets used in their area
- familiar with the ways in which the information assets are used
- able to commit to the time required for this assessment
- preferably, have been in their role for at least a year

Table 11: Optional IT Staff or External Participants

Process 5: Identify Key Components		
Name	**Title**	**Responsibility**
Process 6: Evaluate Selected Components		
Name	**Title**	**Responsibility**
Process 8, Workshop A: Develop Protection Strategy		
Name	**Title**	**Responsibility**

3.5 Brief All Participants

Before any of the workshops begin, all participants should understand what the purpose of OCTAVE is and what their role will be. This is also a good opportunity for senior management to make their sponsorship visible. The Participants Briefing provided at the end of this volume can be used for this purpose.

4 Coordinate Logistics

This section describes all of the necessary scheduling and logistics support. It can be used as guidance and also as a checklist for ensuring that everything is ready before participants show up for their workshop. Logistics includes

- setting up the initial schedule
- coordinating meeting rooms, viewgraph projectors, etc.
- handling unexpected events such as scheduling additional meetings and/or substituting personnel in meetings

A general schedule of activities is provided in Figures 1 and 2. Figure 1 shows the preparation activities, while Figure 2 shows the activities during the evaluation itself. There is likely to be some time lag between the two sets of events. There are several assumptions with this example schedule. It is assumed that a three-day training class will be needed for the analysis team and that two general staff workshops will be needed during Process 3. It is also assumed that a week of elapsed time will be needed to run the vulnerability tools (not a total of a week's effort, rather a week with the tools run at different times and shifts to avoid interrupting key operations). The shortest possible timeframe for performing the workshop portion of OCTAVE is a bit less than two weeks. Coordination of people usually adds to the time as does running the vulnerability evaluation tools.

The OCTAVE Method activities are largely a series of short workshops. While the order of the activities is fixed, the actual schedule can be quite flexible. The analysis team will need to devise a schedule that meets the needs of both the organization and the process. You will need to remember that some processes have pre- and post-workshop activities, and time should be allowed for those. Check the detailed process guidance and decide how you want to handle that time and where you might be able to double up some of the data processing work. The introduction to each process and the preliminary activities includes a temporal flow of events/activities and suggested times. These are only suggestions, but they can help you plan ahead.

After the sample schedule, the remaining part of Section 4 provides tables for documenting logistics and scheduling information associated with OCTAVE. Additional guidance on conducting the workshops is provided in the Process Guidelines for each OCTAVE process. Within these tables are

- the logistical requirements for the activity
- a place to list the participants and analysis team members for the activity
- a place to list the day and time that the meeting is scheduled
- a place to list the room number and any specific equipment that has been acquired for use

Figure PG-1: Sample Schedule for Preliminary OCTAVE Activities

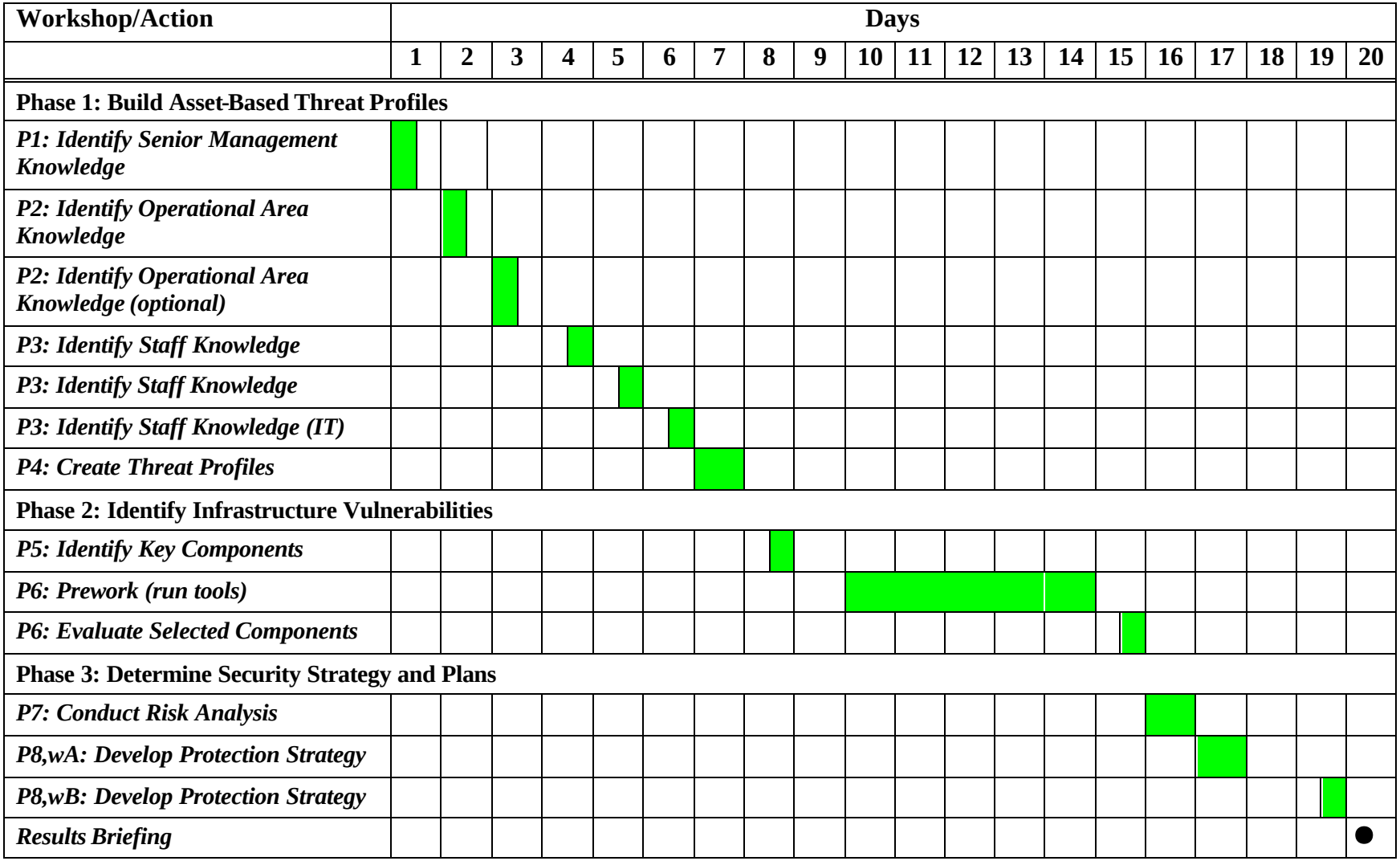
Preliminary Activities	**Days**													
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
Preparation sessions	■		■											
Select analysis team				●										
Train analysis team							■	■	■					
Select participants											●			
Participants briefing														●

Legend:

■ partial to several days for a workshop or other activities

● a briefing, usually 1 to 2 hours

Figure PG-2: Sample Schedule for OCTAVE Workshop Activities



4.1 Preparation Sessions

Note that part of the preparation session may have occurred before the analysis team was selected. This section refers to scoping OCTAVE and selecting participants. Generally, preparation will occur across multiple sessions as details are worked out, so the three hours set for the session could be broken into one or more sessions. Scheduling should occur after the analysis team is trained so that they can assist in developing a practical schedule. During the preparation session, the following is accomplished

- Brief participating senior managers on the OCTAVE Method (if needed).
- Agree on the scope and participants.
- Develop a general schedule of events, including identification of any known constraints on the schedule.

Analysis team responsibilities

- Schedule the meeting and notify all participants.
- Facilitate the activities.
- Record or capture the results.
- As a post-activity, define the detailed schedule and review it with senior managers.

Table 12: Logistics for Preparations

Participants	Time	Facilities/Logistics
Analysis team members	• 3 hours • 2 hours for preparation	• A conference room • Overhead projector or equivalent • Briefing slides
Participants (at least 3 senior managers)	Meeting Day and Time	Room Equipment

4.2 Phase 1: Build Asset-Based Threat Profiles

Phase 1 of OCTAVE has at least four workshops and one briefing.

- The first workshop examines the senior management perspective.
- The second workshop examines the operational area perspective.
- The third workshop(s) examines the perspective of the general and IT staff levels of the organization.

- The fourth workshop integrates these perspectives to produce an organizational view of the assets, threats, protection strategies, organizational vulnerabilities, and security requirements.

4.2.1 Process 1: Identify Senior Management Knowledge

There should be one Process 1 workshop for senior managers. The analysis team leads the senior managers in this workshop. The senior managers identify information assets and determine which are most important to the organization. They then construct plausible scenarios outlining concerns about the threats to important information assets and define the security requirements for each important asset. Finally, they measure their security practices in relation to known good security practices.

Analysis team responsibilities

- Schedule the meeting and notify all participants.
- Facilitate the activities.
- Record or capture the results.

Table 13: Logistics for Process 1: Identify Senior Management Knowledge

Participants	Time	Facilities/Logistics
Analysis team members	½ day	• Direct display projector or overhead for slides • Flip charts or overhead to capture information
Participants (at least 3 senior managers)	Meeting Day and Time	Room Equipment

4.2.2 Process 2: Identify Operational Area Management Knowledge

There could be up to two workshops for operational area managers, depending on how many managers are selected to participate. The analysis team leads the participating managers in this workshop. The managers identify information assets and determine which are most important to the organization. They then construct plausible scenarios outlining concerns about the threats to important information assets and define the security requirements for each important asset. Finally, they measure their security practices in relation to known good security practices.

Analysis team's responsibilities

- Schedule the meeting and notify all participants.
- Facilitate the activities.

- Record or capture the results.

Table 14: Logistics for Process 2: Identify Operational Area Management Knowledge

Workshop	Participants	Time	Facilities/Logistics
First workshop	Analysis team members	½ day	• Direct display projector or overhead for slides • Flip charts or overhead to capture information
	Participants (at least 4 operational area managers)	Meeting Day and Time	Room Equipment
Second workshop, if needed	Analysis team members	½ day	• Direct display projector or overhead for slides • Flip charts or overhead to capture information
	Participants (at least 4 operational area managers)	Meeting Day and Time	Room Equipment

4.2.3 Process 3: Identify Staff Knowledge

There are usually no more than four staff workshops, depending upon how many staff members are selected. No more than five staff members should be in a workshop. IT staff members meet in a separate workshop. If IT is distributed across several departments, you might want more than three or four members and more than one IT Staff workshop. The analysis team runs the workshop with the participating staff. Staff members identify information assets and determine which are most important. They then construct plausible scenarios outlining concerns about the threats to important information assets and define the security requirements for each important asset. Finally, they measure their security practices in relation to known good security practices.

Analysis team's responsibilities

- Schedule facilities and participants.
- Facilitate workshops.
- Record results.

Table 15: Logistics for Process 3: Identify Staff Knowledge

Workshop	Participants	Time	Facilities/Logistics
General Staff Workshop 1	Analysis team members	½ day	• Direct display projector or overhead for slides • Flip charts or overhead to capture information
	Participants (up to 5 staff members)	Meeting Day and Time	Room Equipment
General Staff Workshop 2	Analysis team members	½ day	• Direct display projector or overhead for slides • Flip charts or overhead to capture information
	Participants (up to 5 staff members)	Meeting Day and Time	Room Equipment
IT Staff Workshop 3	Analysis team members	½ day	• Conference room with space to hang flip charts • Overhead projector or equivalent
	Participants (3-4 IT staff members)	Meeting Day and Time	Room Equipment

Table 15: Logistics for Process 3: Identify Staff Knowledge (cont.)

Workshop	Participants	Time	Facilities/Logistics
Optional General Staff Workshop (if needed)	Analysis team members	½ day	• Conference room with space to hang flip charts • Overhead projector or equivalent
	Participants (up to 5 staff members)	Meeting Day and Time	Room Equipment

4.2.4 Process 4: Create Threat Profiles

The information elicited from the previous workshops is consolidated by the analysis team to create an integrated view. They analyze the information and identify the assets that are most crucial to meeting the mission of the organization – called the critical assets. Finally, they describe the security requirements and build a threat profile for each critical asset.

Analysis team responsibilities

- Schedule conference room.
- Hold workshop.
- Record results.

Table 16: Logistics for Process 4: Create Threat Profiles

Participants	Time	Facilities/Logistics
Analysis team members	up to 1 day	• Conference room with table space • Overhead projector or equivalent
Supplemental team members	Meeting Day and Time	Room Equipment

4.3 Phase 2: Identify Infrastructure Vulnerabilities

Phase 2 includes two workshops and a vulnerability evaluation. It focuses on the information technology area to identify technology vulnerabilities that are exposing the organization's assets. It builds on the information identified during Phase 1 by identifying the high-priority infrastructure components.

Note: There is pre-work for the Process 6 workshop – running the vulnerability tools. Care should be taken that this is done before the scheduled workshop begins.

4.3.1 Process 5: Identify Key Components

The analysis team conducts the workshop with selected members of the IT staff. The analysis team must ensure that documentation of the present state of the computing infrastructure is available. The team will examine network access paths to identify the key classes of components for critical assets. Next, they will select specific components from the key classes to evaluate and determine an approach for conducting the vulnerability evaluations. Finally, they will schedule the vulnerability evaluations, acquire all necessary permissions, and notify any personnel who might be affected.

Analysis team responsibilities

- Schedule facilities and additional IT staff.
- Hold the workshop.
- Record results.
- Schedule vulnerability evaluations, acquire permissions, and notify all affected personnel.

Table 17: Logistics for Process 5: Identify Key Components

Participants	Time	Facilities/Logistics
Analysis team members	½ day	• Conference room with table space • Overhead projector or equivalent
Participants (additional IT staff members as needed)	Meeting Day and Time	Room Equipment

4.3.2 Process 6: Evaluate Selected Components

The participants in this process are the analysis team, selected members of the information technology staff, and, optionally, third party tool experts or contractors. Prior to the workshop, the vulnerability

evaluation(s), supported by software tools, checklists, or scripts, are performed. The people who conduct the vulnerability evaluation(s) must also review and analyze the results prior to the workshop. During the workshop, the people who conducted the vulnerability evaluation(s) discuss the summary of the results with the analysis team. Together, they must decide what actions need to be taken.

Pre-work

The pre-work activities are to run the vulnerability tools and summarize the results. Whether done by third parties, supplemental IT staff, or the analysis team members, these activities will require some logistics in order to schedule tool execution. The exact nature of the coordination depends on the tools, the components selected, the infrastructure, and the organization itself (see the Process Guidelines for specific details).

Analysis team responsibilities

- Schedule and participate in vulnerability evaluations.
- Hold the workshop to analyze results with respect to the organization and the critical asset threat profiles.
- Record results.

Table 18: Logistics for Process 6: Evaluate Selected Components

Workshop	Participants	Time	Facilities/Logistics
Process 6: Pre-work	Analysis team members	At least 1 day	• Access to the site's computing facilities • Small room for discussion
	Supplemental team members	Days and Times	Room(s) Equipment
Process 6: Workshop	Analysis team members	½ day	• Access to the site's computing facilities • Small room for discussion

Workshop	Participants	Time	Facilities/Logistics
	Supplemental team members	Meeting Day and Time	Room(s) Equipment

4.4 Phase 3: Develop Security Strategy and Plans

Phase 3 has three workshops to analyze asset, threat, and vulnerability information and to identify and prioritize the risks to the organization. In addition, a protection strategy and risk mitigation plans are developed for the organization.

4.4.1 Process 7: Conduct Risk Analysis

The analysis team creates a risk profile for each critical asset and establishes criteria by which risks are evaluated. Supplemental team members from previous workshops may also be called in to assist as needed.

Analysis team responsibilities

- Schedule facilities and additional participants.
- Participate in workshop.
- Record results.

Table 19: Logistics for Process 7: Conduct Risk Analysis

Participants	Time	Facilities/Logistics
Analysis team members	½ - 1 day	• Conference room with space to display information • Overhead projector or equivalent (optional)
Supplemental team members	Meeting Day and Time	Room Equipment

4.4.2 Process 8: Develop Protection Strategy

There are two workshops in Process 8. In Workshop A, the analysis team and supplemental members develop a protection strategy for the organization, mitigation plans for risks to critical assets, and an action item list. In Workshop B, the analysis team presents their findings and recommendations to senior managers. Senior managers can then revise, if necessary, and approve the plans.

Analysis team responsibilities

- Schedule facilities and additional participants.
- Hold workshops.
- Prepare for presentation and discussion with senior managers.
- Record results.
- Facilitate senior management discussions.

Table 20: Logistics for Process 7: Conduct Risk Analysis

Workshop	Participants	Time	Facilities/Logistics
Workshop A	Analysis team members	• 1 day	• Conference room with space to hang flip charts • Overhead projector or equivalent
	Supplemental team members	Meeting Day and Time	Room Equipment
Workshop B	Analysis team members	½ day	• Conference room with space to hang flip charts • Overhead projector or equivalent
	Senior managers and other attendees	Meeting Day and Time	Room Equipment

4.4.3 Results Briefing

The final, optional, OCTAVE activity is a briefing to all of the participants in the evaluation to inform them about the risks identified during the assessment, the protection strategy and the mitigation plans

developed to address the risks. Other personnel from the organization or third parties can be invited as well.

Analysis team responsibilities

- Schedule facilities and participants.
- Present the briefing or support senior management presenting the briefing.

Table 21: Logistics for Results Briefing

Participants	Time	Facilities/Logistics
Analysis team members	1-2 hours	• Large conference room/auditorium • Overhead projector or equivalent
Participants (everyone who participated in any part of OCTAVE)	Meeting Time	Room Equipment

Preparation Example Results

This is a section of the Complete Example Results contained in Appendix C, Volume 17. The section numbers as well as table and figure numbers used within this section are identical to those in Appendix C and may, therefore, appear to be non-sequential. This portion of the example results is provided in this volume to make it easier to understand this particular part of OCTAVE.

Contents

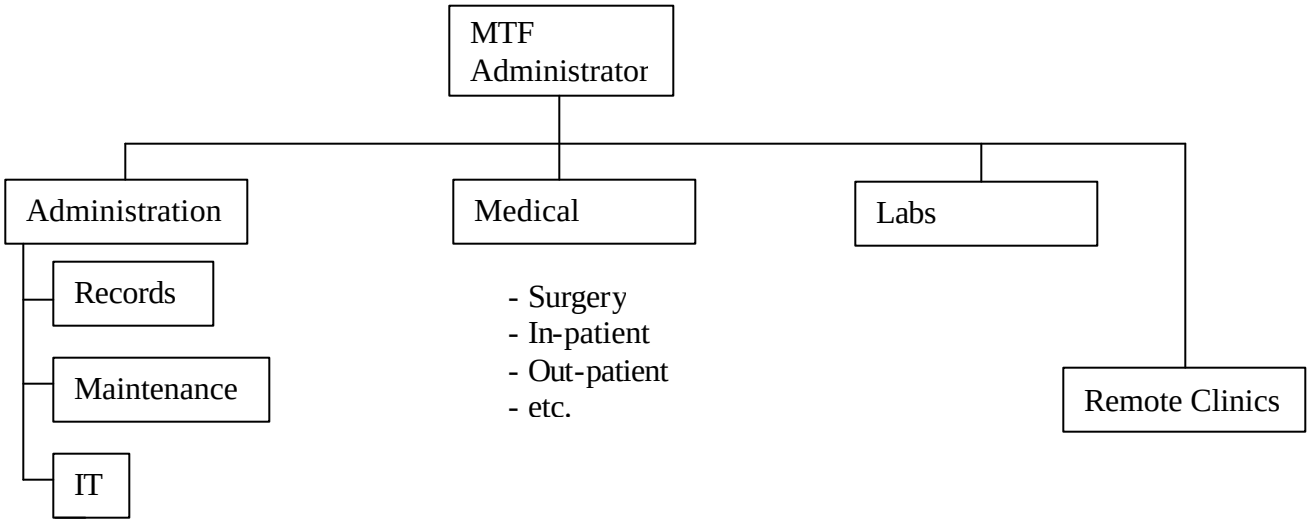
2 Medical Treatment Facility Background

These example results concern a fictitious medical treatment facility. The Medical Treatment Facility (MTF) is a hospital with several clinics and labs, some of which are distantly located. It has:

- a permanent administrative organization
- both permanent and temporary
  - physicians
  - surgeons
  - medical staff
  - facility staff
  - maintenance
- a small information technology (IT) department (three people) responsible for on-site computer and network maintenance and upgrades, and handling simple user help requests

Figure 1 shows a high-level view of the MTF organization.

Figure 1: MTF Organization Chart



One of the main systems is the Patient Information Data System (PIDS). PIDS includes the network, PCs, and applications to link and integrate another set of smaller, older, function-specific databases, which include patient care, lab results, and billing. Patient data can be entered into either PIDS or one of the other databases at any time from any workstation. Data can be entered by physicians, administrative clerks, lab technicians, or nursing staff. Workstations are located in all physicians' offices, treatment rooms (including emergency rooms), nursing stations, labs, and administrative

offices. Off-site access is also available from physicians' private computers and may eventually be available via personal digital assistants (PDAs). Support for PIDS, the network, and most of the other databases is provided by an independent contractor, ABC Systems. One or two databases are legacy systems built and maintained either internally or by another external contractor. MTF also has a small, internal IT staff to provide on-site help desk support and basic system maintenance for the hospital, all clinics, and the labs. Internal IT personnel were provided with limited training from ABC Systems.

In August 2000, MTF senior managers decided they wanted a comprehensive review of information security within their facility. Several new regulations would be coming out in the following year that would require documented information security risk assessments and proof of good security practices. After some discussion and consultation with other medical facility managers, they decided to use OCTAVE. They assigned the initial planning and preparation to the assistant administrator, E. Smith. Smith used the OCTAVE Preparation Guide to start the process and to determine what to do first.

3 MTF Preparation Results

Smith and other senior officials at MTF held an initial discussion to select an analysis team (Table 1). With the exception of the logistics coordinator, all analysis team members were assigned to this effort on a 50% time basis. An alternate IT member was identified as the work schedules of all IT staff were subject to emergency interrupts. The analysis team members (including the alternate) were trained in the OCTAVE Method in early September and worked with Smith to develop an overall schedule. This schedule was refined after some discussion with senior managers to discuss the process in more detail (using part of the Senior Management Briefing) and to select the operational areas to be evaluated and the senior managers who would be interviewed (Table 2).

Table 1: Analysis Team Members

Name of Core Analysis Team Member	Job Function in MTF
L. Pierce (analysis team leader)	an operational manager for Surgery A
J. Cutter (recorder)	a mid-level administrative clerk from Records
S. Nolan R. Green	IT staff member Alternate IT member
K. Brown for logistics (part-time)	Facilities assistant manager

Table 2: Senior Managers, Operational Areas, and Operational Area Managers

Senior Managers	Operational Areas	Operational Area Managers
P. Rollins (Hospital Administrator)	Information Technology	J. Donaldson
B. Houston (Director of Admissions)	Out-Patient Records	M. Davis
M. Samuelson (Director of Medical Operations)	In-Patient Treatment	L. Roland
R. Smith (Director of Pathology)	Lab 2	J. Livingston
C. Davidson (Manager, Clinic D)		

Once the operational area managers were identified, the analysis team met with them to select the staff participants. The IT staff will participate in a separate workshop from the remaining staff

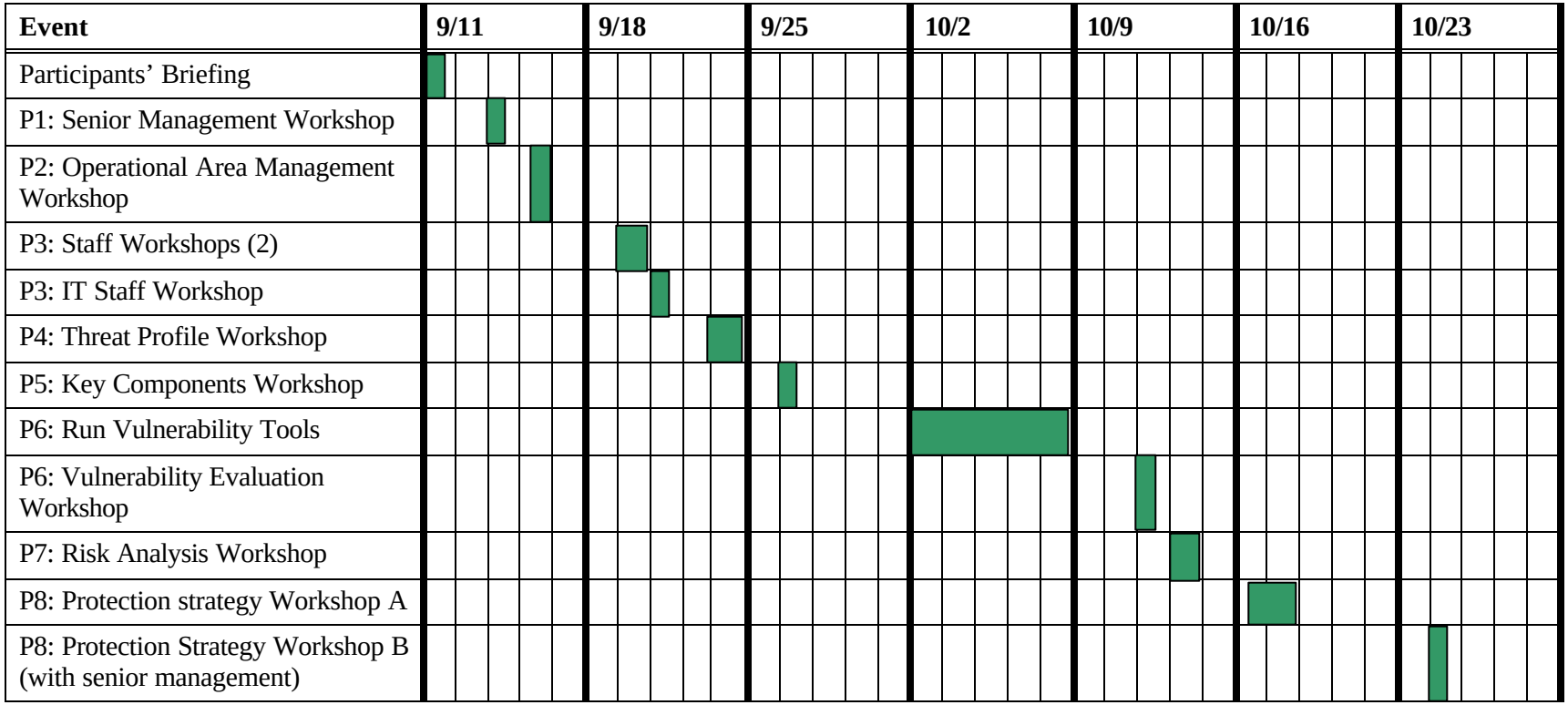
members. The analysis team decided to mix the representatives from the other operational areas into two workshops. (Table 3)

Table 3: General and IT Staff Members

Operational Areas	Name of Staff Member	Workshop
Information Technology	C. Jones	IT Staff Workshop
	L. Gunnar	
	S. Leeds	
Out-Patient Records	K. Ambrose	General Staff Workshop 1
	S. Woods	General Staff Workshop 2
	W. Goodman	General Staff Workshop 2
In-Patient Treatment	J. Simmons	General Staff Workshop 1
	S. Caller	General Staff Workshop 2
	M. Davidson	General Staff Workshop 2
	L. Madison	General Staff Workshop 1
Lab 2	J. Fleet	General Staff Workshop 1
	K. Harriman	General Staff Workshop 1
	S. Thomas	General Staff Workshop 2

Once the staff members were selected, the final schedule (Figure 2) was created and all participants were provided with an initial briefing (using the Participants' Briefing). The logistics coordinator, K. Brown, made sure all the necessary equipment and rooms were available and sent reminder email to all participants the day before their workshop. The participants were briefed on September 11, 2000, and the final workshop with senior management to review the proposed protection strategy and mitigation plans was held on October 27, 2000.

Figure 2: OCTAVE Schedule



Tailoring Guidelines

This section is for analysis teams and other OCTAVE users. It provides some suggestions for the overall tailoring and a summary of the tailoring guidance found in each process section for processes and artifacts**.** You should read this section before starting the evaluation to determine the extent of tailoring needed to suit your organization.

Contents

1 Overview of Tailoring

OCTAVE was designed as a generic evaluation that almost any organization in any domain could use. It should be tailored to your specific constraints, culture, and applicable regulations. OCTAVE can be tailored at multiple levels. The overall evaluation can be tailored, individual processes can be tailored, and the artifacts (e.g., worksheets or catalog of practices) can be tailored. These guidelines provide some suggestions (it is not an exhaustive list) for the overall tailoring and a summary of the tailoring guidance found in each process section for processes and artifacts**.**

The overall tailoring suggestions here have not been extensively tested, but we believe they are worth considering as you look for different ways to adapt OCTAVE to your needs and constraints. The summary of the process tailoring should help you decide, ahead of time, what you might want to consider before the first workshop. You can refer to the OCTAVE principles and characteristics [Alberts 2001] if you want to make sure you adhere to the basic concepts of what OCTAVE was intended to be.

2 Tailoring the Evaluation

There is a multitude of ways to tailor the overall evaluation. These are some, but by no means all, of them. In general, be cautious with tailoring anything new as you might eliminate an important aspect.

2.1 Order of Processes

The basic flow of events described in this Method Implementation Guide is sequential. To some extent, the processes depend upon the outputs of previous processes. For example, building an organizational strategy in Process 8 depends on information about current organizational vulnerabilities gathered in Processes 1 to 3. The vulnerability evaluations of Phase 2 need the critical assets identified in Process 4 to provide adequate focus. Some processes, however, can be moved around in order, depending upon your organization.

Processes 1-3 are set up in descending order among the organizational levels, from senior management to staff. This allows lower levels of the organization to see the opinions of others at the end of their own workshop. Some senior managers, however, are culturally attuned to reviewing and refining what has been recommended from others. The analysis team may consider running Processes 1-3 in reverse and letting the senior managers build on the opinions and information from operational area managers and staff.

If your organization already does routine vulnerability evaluations on your systems and components, then you may be able to simply review the results for applicable components as opposed to running the tools again. As the results of the surveys are not used until Process 8, they could be distributed, collected, and discussed with the participants at any time before Process 8.

2.2 Schedule

The example schedule provided in the Preparation Guide can be either condensed or expanded. With the possible exception of the vulnerability evaluations, most of OCTAVE can be accomplished within a tightly coordinated two-week span. Generally, the difficulties of coordinating different people's schedules, unexpected events, and critical projects will interfere with all of the processes. In addition, setting up and coordinating technological vulnerability evaluations can be time consuming for any organization that does not do this on a routine basis.

On the other end of the spectrum, the schedule can be lengthened to three months or more, although the risk of the analysis team working with stale data increases. If this needs to be done, schedule Processes 6, 7, and 8 as close as possible or be prepared to act upon the results of the vulnerability evaluations of Process 6 immediately. It could be disastrous to wait a month after Process 6 to begin thinking about technological vulnerability mitigation in Process 7.

2.3 Number of Workshops

Throughout Processes 1-3, it was stated that there was a maximum number of participants, usually five, depending upon the capabilities of the analysis team to manage a large number of people. Scheduling difficulties always arise, as do personality conflicts. So the number of workshops for any of these first three processes can increase as needed. It is not quite as useful to have only one participant in a workshop – a minimum of three is preferred. However, if a key senior manager is unable to make a session, he or she can be worked with separately.

If you are dealing with a dispersed or multi-site organization, you may find travel restrictions force the number of workshops to increase. The number of workshops is significant only in the amount of time it takes to conduct them.

2.4 Format of Workshops

The process guidelines set a specific format for the workshops and assume that it all takes place in one sequential chunk of time on one or, at most, two days. Processes 1-3 can be run across several days in small pieces, even during lunch. Assets and security requirements can be identified on one day, areas of concern on another, and the survey and survey discussion can be held on a third day. The surveys could also be completed prior to the workshop and then discussed. Processes 4 and 7 are longer, almost full-day workshops. These can be broken into pieces by asset, focusing on one critical asset per day as opposed to one long session. Any of these format changes can be made to decrease any negative impacts on the analysis team members' regular job duties.

2.5 Phase 2 and Outsourcing

Phase 2 is the one set of activities that is most likely to be outsourced by many organizations. Some organizations do not have the internal expertise to run vulnerability evaluation tools on all of their systems or they have a particular system that is not under their direct control. In the ideal case, the analysis team works with the other party during Process 5. The analysis team brings the information about what needs to be protected and the threats they see, and the third party brings their knowledge of what systems and components support those assets. Together, they identify the key components and determine the type of vulnerability evaluation that is needed. The third party runs the appropriate tools, collects the data, and returns to discuss the results with the analysis team during Process 6.

In some cases, the analysis team may find they have no easy way of working with the third party. Contracts may not permit this type of work or there may be restrictions on who can be contacted. In these cases, Phase 2 may have to wait until later. In the meantime, such problems call out for looking at the collaborative security management practice. (See the Catalog of Practices in Appendix A.)

2.6 Outsourcing in General

Some organizations outsource their entire IT infrastructure. In this case, you will need to work with that third party to acquire an IT-knowledgeable member for the analysis team for the duration of OCTAVE. Contractual arrangements or other managerial approvals may be needed to ensure this occurs and that you have the full support of the IT member.

2.7 Getting Senior Sponsorship

The Senior Management Briefing is one way to gain senior manager support and commitment. However, many managers prefer a much clearer idea of what they are going to get for their resources. Here are some suggestions for providing senior managers with the information the need to support the evaluation:

- You could use selected portions of the example results to show managers the type of data and information you will be producing with OCTAVE. This doesn't require a lot of time or effort.
- You could distribute the surveys (electronically or paper), collect and summarize the results, and use the results to help convince managers that you have considerable room for improvement and need the rest of the evaluation to focus your improvement efforts effectively.
- You could ask senior managers what the most important asset is, then spend a few hours on their own with the Asset Profile Workbook, documenting the risks to the asset and potential mitigation actions. This can be used to show managers useful results directly applicable to the organization. This does require, however, that the analysis team become familiar with Processes 4-8. This can be a part of their training or familiarization.
- You could find all of the applicable regulations, laws, documents, edicts, directives, and any other paperwork that directs organizations such as yours to do information security evaluations, e.g., [HIPAA[1] 98] and [Gramm 00]. This can be helpful in reminding managers that future audits, accreditation reviews, and other events are likely to look closely at the way you identify and manage information security risks.

2.8 Risk Probability

If you are familiar with risks and risk management, you will know that probability and impact are both considered the main aspects of risk. OCTAVE assumes the probability for all marked or active branches of the risk tree to be equal – one. The reasoning behind this is simple – that there is not enough current, validated data to make any kind of accurate, reliable predictions of probability. While some data have been gathered and made available on the general probabilities of certain types of attacks, translating that probability to the context of a specific company and a specific asset is far more difficult.

That being said, if you have a set of reliable information for your company showing the current probability for certain types of attacks with your current system configuration and organizational practices, then you might be able to assign a qualitative value of probability to some risk profile branches. We simply caution you to always consider the magnitude of the risk impact first. If, for example, human life is at risk from improperly modified data, you may be obligated to mitigate the risk, no matter how small the probability.

[1] Health Insurance Portability and Accountability Act

2.9 Independent Analysis Teams (Facilitated or Expert-Led)

Within very large organizations that have many sites or facilities (e.g., branches of the military, government, or large corporations), it can be more cost effective to train a set number of analysis teams and let them travel or move around as needed to conduct evaluations. Such site- or facility-independent teams would need to supplement their membership with local personnel, usually at least one staff member and one IT staff member. The local team members could be briefed (with the slides for each process) as a part of just-in-time "training". The local team members could then be used as a source of local information and for verification or correction of findings and recommendations. Some of the benefits of independent teams are their ability to see much larger patterns across the larger organization and the reduction in training and personnel costs.

2.10 Automation

A last evaluation-wide tailoring point is the use of automation to speed up the collection, consolidation, formatting, and review of information collected during OCTAVE. A simple tool could easily be constructed within a multi-layered spreadsheet, or a more complicated database program could be used. Either option could reduce the amount of data capture and integration as well as provide a more convenient historical record.

3 Tailoring Major Artifacts

A second way to tailor OCTAVE is to adapt the artifacts to suit your organization or the particular regulations, standards, or domain that you work with.

3.1 Catalog of Practices

The catalog of practices is deliberately divided into two main sets of practices – strategic and operational. Strategic practices focus on organizational issues at the policy level and contain good, general management practices. Strategic practices include business-related issues as well as issues that require organization-wide plans and participation. Operational practices focus on technology-related issues. They include issues related to how people use, interact with, and protect technology. Since strategic practices are based on good management practice, they should be fairly stable over time. Operational practices are more subject to changes as technology advances and new practices arise to deal with those changes.

Nonetheless, the catalog is a general catalog of good security-related practices; it is not specific to any domain, organization, or set of regulations. It can be modified to suit a particular domain's standard of due care or set of regulations (e.g., the medical community's security regulations [HIPPA 98]). It can also be extended to add organization-specific standards, modified to terminology suitable to a specific domain, or the thresholds for summarizing the results can be modified.

If the catalog of practices is modified, the surveys used in Processes1, 2, 3, and 8 more than likely must also be modified. You may also find that some areas are not applicable or only partly applicable.

3.2 Generic Threat Profile

The generic threat profile is a basic profile that covers a range of threats to critical assets. The threat profile can be tailored to meet your organization's needs. You can change the components on one of the trees or use the blank tree provided for this purpose. For example, if terrorism or corporate espionage is a real threat to your critical assets, you can modify the definition of human actors on the appropriate tree. You may also want to modify the threat profile if you have natural disasters unique to your area or if your site is located in an area with severe electric power or water supply issues.

Another possible tailoring of the threat profile is expanding it or decomposing one of the trees. For example, the *Human Actors Using Network Access* tree is a general tree for any network access. You may find you want a separate tree for each major type of system to help clarify your network access threats. For example, you may have a strictly internal network with corporate data accessed by your employees from work or home. Some of the same data are on an externally accessible server and network for customers and third parties. You may want two different threat trees for *Human Actors*

Using Network Access to distinguish between threats (and eventually mitigation plans) to the same information asset coming via two different systems. Another example is the *Human Actors Using Physical Access* tree, which could be decomposed for different buildings or different sites.

The caution here is not to get too complex and create more data than you can reasonably deal with. You can use the general profile, and, if the situation and the threats warrant it, decompose it later in a separate follow-on activity.

3.3 Asset Profile Workbook

This workbook was compiled from separate worksheets to put all of the information about a single asset in one place. Obviously, you can break it apart into separate worksheets. You could also reformat, reorganize it to suit corporate standards, or make it a standard report from a database tool. In addition, it could be condensed, eliminating some of the detailed information, and used as a summary for reporting results to other parts of the organization or for maintaining current status on a critical asset's risks.

3.4 Slides

Each process is accompanied by a set of slides and notes used to familiarize new team members with the process, its activities, and any specific concepts. If you do any tailoring of the overall process, artifacts, or terminology, don't forget to check the slides before you use them. These slides can also be combined together to make longer briefings for other parts of the organization, third parties, customers, or collaborators. Organization-specific information should also be added where appropriate.

3.5 Example Results

The example results are just that – an example. It may not be particularly relevant to your domain and you may want to create your own example results. You can tailor these results to suit the assets, threats, and risks that are applicable to your domain and organization. As each set of process results builds upon the previous set, care should be taken to maintain internal consistency across the example. Once you have a set of results from OCTAVE, you can sanitize your own data and use it as an example.

4 Summary of Individual Process Tailoring

The following tables summarize the types of tailoring, and why you might want to tailor, for each process in OCTAVE. Processes 1 to 3 are similar enough that there is only one table. Note that tailoring can ripple from one process to the next. For example, if you add a new type of security requirement to Processes 1-3, Activity 3, this ripples into Processes 4 and 7 for consolidated security requirements and threat profiles. Notes provided in the "Why Tailor?" column indicate tailoring ripples by referencing other rows in the tables with the relevant activity number (e.g., A1-3.2).

Table 1: Tailoring Processes 1 to 3

Processes 1-3: Knowledge Elicitation Workshops			
Activity Number	**Tailoring Item**	**Description**	**Why Tailor?**
A1-3.1	Asset categories	Change the list of basic asset categories.	• Include unique types of assets specific to your domain.
A1-3.1	Number of assets	Increase or decrease the number of important assets (from five) that participants select.	• Decrease if this is a new process and the analysis team needs to constrain the effort. • Increase for experienced teams or very large, complex organizations.
A1-3.2	Threat sources and outcomes	Add, delete, or change the classes of threat sources and outcomes.	• Include unique or common domain threats (e.g., terrorists or corporate espionage). • Remove irrelevant sources. • Add outcomes that you feel are crucial to identify (e.g., accuracy). • Add outcomes to reflect changes in security requirements. **Note**: See also A1-3.3.
A1-3.3	Security requirements list	Add, delete, or change the types of security requirements (integrity, availability, confidentiality).	• Add or expand to new types (e.g., add authenticity). • Reflect changes made to threat outcomes. **Note**: See also A1-3.2, A4.2, and A8A.3.

Table 1: Tailoring Processes 1 to 3 (cont.)

Processes 1-3: Knowledge Elicitation Workshops			
Activity Number	**Tailoring Item**	**Description**	**Why Tailor?**
A1-3.4	Catalog of practices	Add, delete or modify practices.	• Meet new or modified regulations, laws, or standards for due care. • Incorporate technological advances or different types of tools. • Incorporate changes or improvements in the state of management practices. **Note**: See also D8A.1 and A8A.2.
A1-3.4	Surveys	Modify surveys.	• Match changes to catalog of practices. • Simplify or expand the detail of the surveys. • Focus on different organizational level or group of people (e.g., third-party contractors). **Note**: See also D8A.1 and A8A.2.

Table 2: Tailoring Process 4

Process 4: Creating Threat Profiles			
Activity Number	**Tailoring Item**	**Description**	**Why Tailor?**
A4.2	Security requirements list	Add, delete, or change the types of security requirements (integrity, availability, confidentiality).	• Add or expand to new types (e.g., add authenticity). **Note**: See also A1-3.3.
A4.3	Modify threat profile	Add, delete or modify any of the threat components (actor, access, motive, outcome).	• Reflect changes in security requirement types. • Add threats unique to your domain. **Note**: See also A1-3.2, A1-3.3, and A8A.3.

Table 3: Tailoring Process 5

Process 5: Identify Key Components			
Activity Number	**Tailoring Item**	**Description**	**Why Tailor?**
A5.1	Classes of key components	Add, delete, abstract, decompose, or change the classes.	• Address new types of hardware or system components. • Address unique types of components included in your systems.
A5.1	Expand to physical access threats	Expand this process to identify classes of components relative to attacks on physical security.	• Identify classes of physical components as a precursor to doing a focused evaluation of physical security (e.g., buildings, rooms, doors).

Table 4: Tailoring Process 6

Process 6: Evaluate Selected Components			
Activity Number	**Tailoring Item**	**Description**	**Why Tailor?**
D6.1	Levels of severity	Expand the levels of vulnerability severity, (e.g., from three to five) or change the definition of the levels.	• Increase your ability to distinguish between different types of vulnerabilities and their impact on your organization. • Make the definitions more meaningful to your situation. • Be consistent with the organization's standard tools.

Table 5: Tailoring Process 7

Process 7: Conduct Risk Analysis			
Activity Number	**Tailoring Item**	**Description**	**Why Tailor?**
A7.2	Risk evaluation criteria	Expand the measures of impact (beyond high, medium, or low) or modify the impact areas (e.g., reputation).	• Prefer five or more levels (e.g., high, high/medium, medium, medium/low, and low) for greater clarification of impact. • Delete areas that don't apply to your organization or add unique areas (e.g., community safety).

Table 6: Tailoring Process 8

Process 8: Develop Protection Strategy			
Activity Number	**Tailoring Item**	**Description**	**Why Tailor?**
D8A.1	Survey summary thresholds	Change the thresholds from 75% to reflect your own preference for what constitutes a majority opinion.	• Prefer a tighter (or looser) threshold to indicate a practice is or is not generally performed in the organization.
D8A.1	Survey summary categories	Change the structure or categories on the summary worksheet.	• Reflect earlier changes made to the catalog of practices or surveys. **Note**: See also A1-3.4 and A8A.2.
A8A.2	Protection strategy	Change the categories on the worksheets.	• Reflect earlier changes made to the catalog of practices or surveys. • Reflect corporate standards for documenting strategies. **Note**: See also A1-3.4 and D8A.1.
A8A.3	Mitigation plans	Change the categories or structure of the mitigation plans.	• Reflect changes made to the threat profile. • Reflect corporate standards for documenting mitigation plans. **Note**: see also A1-3.2, A1-3.3, and A4.3.
A8B	All worksheets	Tailor format, content, and depth of detail for presentation to senior managers.	• Different senior managers prefer information presented in different ways – add or subtract detail, follow corporate standards, adapt to specific manager preferences.
A8B.1	Survey results	Tailor to eliminate all attribution, produce a concise format, or highlight key areas.	• Organization culture may require that all attribution be eliminated, even identification of which level thought a practice was or was not being done. • Senior managers may want only highlights of survey results.
A8B.1	Risk profile	Condense or change the format to a different type of graphic (e.g., color pie chart) or plain text.	• Suit the preferences or time constraints of senior managers. • Highlight significant aspects of the risks.
X8B.1	Protection strategy, mitigation plans, action list	Change the format or content.	• Meet corporate standards. • Suit management preference. • Enhance communication of the results with the rest of the organization.

